Carlos Gajero Grande

LA DESINFORMACIÓN COMO AMENAZA A LA SEGURIDAD COLECTIVA Y LA RESPUESTA DEL ESTADO DEMOCRÁTICO

COLECCIÓN

TESIS POLICIALES

Ediciones Universidad Salamanca

CARLOS GAJERO GRANDE

LA DESINFORMACIÓN COMO AMENAZA A LA SEGURIDAD COLECTIVA Y LA RESPUESTA DEL ESTADO DEMOCRÁTICO



Ediciones Universidad
Salamanca

COLECCIÓN TESIS POLICIALES
6

Ediciones Universidad de Salamanca
y Carlos Gajero Grande

1.ª edición: diciembre, 2025
ISBN: 978-84-1091-182-6
DOI: https://doi.org/10.14201/0TP0006

Ediciones Universidad de Salamanca
eusal.es

Hecho en UE-Made in EU

Usted es libre de: Compartir — copiar y redistribuir el material en cualquier medio o formato Ediciones Universidad de Salamanca no revocará mientras cumpla con los términos:

Reconocimiento — Debe reconocer adecuadamente la autoría, proporcionar un enlace a la licencia e indicar si se han realizado cambios. Puede hacerlo de cualquier manera razonable, pero no de una manera que sugiera que tiene el apoyo del licenciador o lo recibe por el uso que hace.

NoComercial — No puede utilizar el material para una finalidad comercial.

SinObraDerivada — Si remezcla, transforma o crea a partir del material, no puede difundir el material modificado.

♠

Ediciones Universidad de Salamanca es miembro de la UNE Unión de Editoriales Universitarias Españolas
www.une.es

A Mercedes, mi alma gemela, por su incondicional aliento, su permanente apoyo y por todo ese valioso tiempo que desinteresadamente me ha cedido para que yo pudiera dedicarlo a este proyecto personal.

A Rafa, mi director, por su visión, por su saber, por su paciencia, por su sentido del humor y por sus invariablemente acertados consejos.

A José María, aliado y amigo que siempre confía en mí, hasta el extremo de creerme capaz de hacer una tesis doctoral.

Y a mi familia y a todos aquellos a los que, durante los dos últimos años, les he dedicado algo menos del tiempo que se merecen.

Índice

Abreviaturas 11
RESUMEN 17
ABSTRACT 20
CAPÍTULO 1. SOBERANIA Y SEGURIDAD 23
1.1. La evolución de la soberanía desde el Estado moderno hasta la llegada del nuevo dominio digital 23
1.1.1. El Estado Moderno y su visión del poder soberano 24
1.1.2. La soberanía digital 31
1.2. La organización de la seguridad como faceta de la soberanía 39
1.2.1. La seguridad como principio básico de la vida social organizada 41
1.2.2. La seguridad como monopolio incontestable del Estado 45
1.3. De la garantía de seguridad a la seguridad como garantía: la seguridad humana 49
1.3.1. El concepto de *seguridad humana* 50
1.3.2. El valor agregado de la seguridad humana 56
1.3.3. La visión integral de la seguridad a través de la Agenda 2030 y los ODS 60
1.4. Conclusiones: el estado de salud de los conceptos de soberanía y seguridad en la Era Digital 63
CAPÍTULO 2. LA CONSTRUCCIÓN DEL CONCEPTO DE SEGURIDAD MULTIDIMENSIONAL: NACIONES UNIDAS Y LA ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE 69
2.1. La Organización de las Naciones Unidas 72
2.1.1. El periodo fundacional y la Guerra Fría (1945-1989) 72
2.1.2. El final de la Guerra Fría y la reordenación de los actores internacionales . 76
2.1.3. Balance y situación actual tras 75 años de Naciones Unidas: ¿realidad o ficción de su rol como árbitro de la seguridad internacional? 81
2.1.4. La aportación de Naciones Unidas a la ciberseguridad en el siglo XXI 92
2.2. La Organización del Tratado del Atlántico Norte 98
2.2.1. 1949-1990: el equilibrio de la Guerra Fría 98
2.2.2. 1990-2001: la evolución desde la defensa colectiva a la seguridad compartida 104
2.2.3. 2001-2014: la adaptación a las nuevas amenazas 106
2.2.4. 2014-2024: el resurgir del desafío ruso 108
2.2.5. El Concepto Estratégico de Madrid 118
2.2.6. Balance y situación actual tras 75 años de OTAN: ¿anacronismo o pilar del equilibrio de fuerzas? 122

Ediciones Universidad de Salamanca | CC BY-NC-ND

2.2.7. La aportación de la OTAN a la ciberseguridad en el siglo XXI 128
2.3. Conclusiones: la adaptación como parte del secreto para llegar a los 80 años de edad 131
CAPÍTULO 3. LA SEGURIDAD EUROPEA: REPLANTEAMIENTO DE LA ESTRATEGIA Y REAFIRMACIÓN DE VALORES EN EL CIBERESPACIO 136
3.1. El inopinado proceso constitutivo de la Unión Europea 138
3.2. La Política Exterior y de Seguridad Común: el camino hacia la deseada autonomía estratégica de la Unión 148
3.2.1. La Estrategia Europea de Seguridad: una Europa segura en un mundo mejor (2003 – 2008) 155
3.2.2. La Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea. Una visión común, una actuación conjunta: una Europa más fuerte (2016) 161
3.2.3. Reflexiones sobre la Política Exterior y de Seguridad Común: ¿cómo construir la imagen de una Unión creíble y cómo afecta a su seguridad? 166
3.3. La Política Común de Seguridad y Defensa: la determinación de Europa por alcanzar su propia alianza militar 170
3.3.1. La relación OTAN - UE: el Caballo de Troya 172
3.3.2. El nacimiento en Lisboa de la Política Común de Seguridad y Defensa de la UE 176
3.3.3. La cristalización de un nuevo enfoque: la Brújula Estratégica para la Seguridad y la Defensa (2022) 183
3.3.4. El Libro Blanco de la Defensa y el Plan ReArm Europe: la estrategia de defensa europea mirando al 2030 190
3.3.5. Reflexiones sobre la Política Común de Seguridad y Defensa: ¿herbívoros en un entorno de carnívoros? 194
3.4. La cooperación en el ámbito de la seguridad interior de la Unión Europea 198
3.4.1. Surgimiento y arraigo de la colaboración policial en la UE 199
3.4.2. El Tratado de Lisboa y la comunitarización del Tercer Pilar 206
3.4.3. La Red de Agencias de Justicia y Asuntos de Interior: Europol y Eurojust . 210
3.4.4. La Estrategia de Seguridad Interior de la UE: hacia un modelo europeo de seguridad (2010-2015) 221
3.4.5. La Agenda Europea de Seguridad (2015-2020) 223
3.4.6. La Estrategia de la UE para una Unión de la Seguridad (2020-2025) 225
3.4.7. Consideraciones sobre el modelo de seguridad interior de la Unión: ¿quién abre la caja de Pandora? 228
3.5. La estrategia europea en el ciberespacio: dominio digital con valores 230
CAPÍTULO 4. LA SEGURIDAD ESPAÑOLA: MODELO INTEGRAL E INTEGRADO DE RESPUESTA A LOS DESAFÍOS TRADICIONALES Y DEL CIBERESPACIO 241

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.1. La seguridad como concepto y la Policía como institución en el constitucionalismo histórico español 242
4.1.1. De la Constitución de Cádiz a la II República 243
4.1.2. La dictadura franquista 251
4.1.3. La democracia española de 1978 253
4.2. Los distintos planos conceptuales de la seguridad en la Constitución de 1978 260
4.2.1. El Título Preliminar de la Constitución Española de 1978 261
4.2.2. El Título I "De los derechos y deberes fundamentales" 262
4.2.3. El Título IV "Del Gobierno y la Administración" 267
4.2.4. El Título VIII "De la organización territorial del Estado" 269
4.3. La estructura de seguridad nacional española 271
4.3.1. La Ley de Seguridad Nacional de 2015 276
4.3.2. El marco colaborativo del Sistema de Seguridad Nacional 281
4.3.3. El Departamento de Seguridad Nacional 284
4.3.4. Los Comités Especializados 288
4.3.5. Conclusiones sobre el Sistema de Seguridad Nacional 301
4.4. El desarrollo del modelo de Estrategia de Seguridad Nacional como elemento integrador y de consenso frente a la amenaza 303
4.4.1. Estrategia Española de Seguridad: una responsabilidad de todos (2011) . 305
4.4.2. Estrategia de Seguridad Nacional: un proyecto compartido (2013) 308
4.4.3. Estrategia de Seguridad Nacional: un proyecto compartido de todos y para todos (2017) 311
4.4.4. Estrategia de Seguridad Nacional: un proyecto compartido (2021) 316
4.5. Los ámbitos de interés de la Seguridad Nacional y su desarrollo normativo de segundo nivel 324
4.5.1. La Estrategia de Seguridad Marítima Nacional 327
4.5.2. La Estrategia de Seguridad Energética Nacional 329
4.5.3. La Estrategia de Seguridad Aeroespacial Nacional 330
4.5.4. La Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 332
4.5.5. La Estrategia Nacional de Protección Civil 334
4.5.6. La Estrategia Nacional Contra el Terrorismo 335
4.5.7. La Estrategia Nacional de Ciberseguridad 339
4.5.8. La Estrategia Nacional contra las Campañas de Desinformación 340
4.6. El Modelo de Seguridad 2030 en España 342
4.6.1. La ampliación del concepto de seguridad en el marco normativo español342

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.6.2. El Modelo de Seguridad 2030 del Ministerio del Interior 346
4.7. Reflexiones sobre la seguridad española: la integración de la ciberamenaza como nuevo horizonte de riesgo 351
CAPÍTULO 5. EVOLUCIÓN DE LAS AMENAZAS A LA SEGURIDAD Y SU VINCULACIÓN CON LA SINGULARIDAD DEL CIBERESPACIO 356
5.1. La guerra: evolución desde el entorno físico al virtual 357
5.1.1. La guerra clásica o convencional 358
5.1.2. La guerra híbrida 364
5.1.3. El nuevo modelo de confrontación: la simbiosis entre el pasado y el futuro 367
5.2. El terrorismo 377
5.2.1. El reto de la conceptualización del terrorismo 377
5.2.2. El fenómeno terrorista en Europa 383
5.2.3. El ciberterrorismo: el Estado Islámico y la vertebración de la amenaza a través de la yihad digital 389
5.3. Las operaciones en el ciberespacio 398
5.3.1. El ciberespacio como nuevo escenario de confrontación y la cuestión de la aplicabilidad del Derecho Internacional 398
5.3.2. El uso de operaciones cibernéticas maliciosas en las relaciones entre Estados: posicionamiento de la Unión Europea y de la Federación de Rusia 407
5.3.3. Reflexiones sobre la aplicabilidad del Derecho Internacional al ciberespacio 428
5.4. Conclusiones: el impulso de la amenaza con el salto del mundo físico al plano digital 430
CAPÍTULO 6. EL DESAFÍO DE SEGURIDAD EN LA ZONA GRIS 433
6.1. La ambigüedad entre la paz y la guerra: la Zona Gris 433
6.1.1. Definición de Zona Gris 435
6.1.2. Actores, escalada y estrategias en la Zona Gris 439
6.1.3. Disuasión y respuesta frente a la amenaza híbrida en la Zona Gris 448
6.2. La desinformación como nueva dimensión de la amenaza 455
6.2.1. Marco conceptual de la desinformación 459
6.2.2. Contexto y causas principales de la desinformación 464
6.2.3. La categorización y la medición del impacto de las operaciones de influencia y desinformación desde la perspectiva europea 470
6.2.3.1. El ciclo de análisis FIMI: buscando un marco común de defensa 471
6.2.3.2. La aplicabilidad del Derecho Internacional a la FIMI 478
6.3. Conclusiones: la Zona Gris en expansión 482

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 7. LA ESTRATEGIA DE LA UNIÓN EUROPEA FRENTE A LA AMENAZA DESINFORMATIVA 485
7.1. La movilización de políticas e instrumentos de colaboración internacionales y europeos contra las amenazas híbridas 486
7.1.1. Las Naciones Unidas frente al desafío híbrido 487
7.1.2. La respuesta a la amenaza híbrida de la OTAN 491
7.1.3. La estrategia de respuesta europea frente a la amenaza híbrida..... 495
7.2. La lucha contra la desinformación en el marco de la Unión Europea..... 501
7.2.1. La concienciación sobre la gravedad de la amenaza y el señalamiento de prioridades para contrarrestarla (2015-2018) 504
7.2.1.1. El Grupo de Trabajo East StratCom y la Comunicación Conjunta sobre la lucha contra las amenazas híbridas 505
7.2.1.2. El desarrollo de las capacidades frente a la amenaza híbrida y el primer Código de Buenas Prácticas en materia de desinformación 508
7.2.1.3. El Plan de Acción contra la Desinformación 510
7.2.2. Las evaluaciones de impacto, la definición del marco normativo y la elaboración de herramientas específicas (2019-2024) 513
7.2.2.1. La Agenda Estratégica de la UE y la infodemia de la COVID-19.... 513
7.2.2.2. El Plan de Acción para la Democracia Europea 515
7.2.2.3. La evaluación del Plan de Acción contra la Desinformación 517
7.2.2.4. La Caja de Herramientas Híbrida de la Brújula Estratégica 519
7.2.2.5. El Código Reforzado de Buenas Prácticas contra la Desinformación 521
7.2.3. La recuperación del tiempo perdido: la Ley de Servicios Digitales 523
7.3. La injerencia extranjera en las democracias europeas 527
7.3.1. Una respuesta conjunta ante una amenaza diversificada 528
7.3.2. La estrategia de defensa común europea frente a la desinformación aplicada a los pilares de la democracia: la vulnerabilidad de los procesos electorales 539
7.4. Conclusiones..... 550
CAPÍTULO 8. LA RESPUESTA ESPAÑOLA FRENTE A LA AMENAZA DESINFORMATIVA CON AFECTACIÓN A LA SEGURIDAD NACIONAL..... 552
8.1. El reto: la identificación de la amenaza desinformativa como ámbito de interés para la seguridad nacional española 554
8.1.1. El señalamiento de la desinformación como amenaza y el inicio de la configuración de la respuesta 556

Ediciones Universidad de Salamanca | CC BY-NC-ND

8.1.2. El compromiso español a través del Procedimiento de actuación contra la desinformación y la puerta de entrada de la sociedad civil 558
8.1.3. El desarrollo del eje de colaboración público-privado: el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional 562
8.1.4. El Plan de Acción por la Democracia 567
8.2. El marco de respuesta español frente a la desinformación con afectación a la seguridad nacional 570
8.2.1. El ámbito legal de la respuesta 570
8.2.2. La articulación operativa de la respuesta 576
8.3. El desafío pendiente: la proyección de la resiliencia en el contexto de la seguridad nacional 584
8.3.1. La incorporación de la resiliencia en las Estrategias de Seguridad españolas 585
8.3.2. El tratamiento de la resiliencia en las estrategias de segundo nivel ... 586
8.3.3. La resiliencia en el marco de la seguridad nacional 588
8.4. Conclusiones: la estrecha relación entre desinformación y seguridad nacional 590
CONCLUSIONES FINALES 592
1. La evolución de los conceptos de soberanía y seguridad 592
2. La perspectiva multidimensional de la seguridad a través de las Naciones Unidas y la Organización del Tratado del Atlántico Norte 593
3. El replanteamiento de la estrategia de seguridad y los principios europeos en el ciberespacio 596
4. El modelo de seguridad español frente a los desafíos de seguridad tradicionales y emergentes 598
5. La evolución de las amenazas a la seguridad y su vinculación con el ciberespacio 601
6. El desafío de seguridad en la Zona Gris 602
7. La estrategia de la Unión Europea frente a la amenaza desinformativa 603
8. La respuesta española frente a la desinformación con afectación a la seguridad nacional 605
Bibliografía 608
Webgrafía: normativa, informes y documentos oficiales 631
Normativa, informes y documentos oficiales internacionales 631
Normativa, informes y documentos oficiales supranacionales-europeos 639
Normativa, informes y documentos oficiales nacionales 659
Normativa 659
Diarios de Sesiones 665

Ediciones Universidad de Salamanca | CC BY-NC-ND

Informes, Instrucciones y otros documentos 665
Jurisprudencia 668
Internacional 668
Tribunal de la Haya 668
Supranacional Europea 668
Tribunal de Justicia de la Unión Europea 668
Jurisprudencia nacional 669
Tribunal Constitucional 669
Otras sentencias y autos 670
Otras referencias web 670

Ediciones Universidad de Salamanca | CC BY-NC-ND

Abreviaturas

ACNUDH: Alto Comisionado de las Naciones Unidas para los Derechos Humanos
AQI: Al Qaeda en Irak
APPF: Authority for European Political Parties and European Political Foundations (Autoridad para los Partidos Políticos Europeos y las Fundaciones Políticas Europeas)
AR/VP: Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad
ASEAN: Asociación de Naciones del Asia Sudoriental

BESD: Brújula Estratégica para la Seguridad y la Defensa (Strategic Compass for Security and Defence)

CARD: Coordinated Annual Review on Defence (Revisión Anual Coordinada de la Defensa)
CBP: Customs and Border Protection (Aduanas y Protección de Fronteras de los EE.UU.)
CCDCOE: NATO Cooperative Cyber Defence Centre of Excellence (Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN)
CCN: Centro Criptológico Nacional (España)
CE: Constitución Española de 1978
CEE: Comunidad Económica Europea
CECA: Comunidad Europea del Carbón y del Acero
CED: Comunidad Europea de Defensa
CELA: Comité Europeo de Lucha contra la Droga
CelCor: Célula de Coordinación del Comité de Situación del Sistema de Seguridad Nacional (España)
CEPOL: European Union Agency for Law Enforcement Training (Agencia Europea para la Formación Policial)
CEPS: Centre For European Police Studies (Centro de Estudios Policiales Europeos)
CERT: Computer Emergency Response Team (Equipo de Respuesta a Emergencias Informáticas)
CGI: Comisaría General de Información de la Policía Nacional (España)
CHST: Contra-Hybrid Specialist Team (Equipo de Apoyo Contra Híbridos de la OTAN)
CICR: Comité Internacional de la Cruz Roja
CITCO: Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (España)
CJTF: Combined Joint Task Force (Fuerza Operativa Conjunta Combinada)
CNI: Centro Nacional de Inteligencia (España)
CNPIC: Centro Nacional de Protección de Infraestructuras Críticas (España)
COPS: Comité Político y de Seguridad de la UE
COREPER: Comité de Representantes Permanentes de los Gobiernos de los Estados miembros de la UE
COSI: Comité Permanente de Cooperación Operativa en Materia de Seguridad Interior de la UE
CPCC: Civilian Planning and Conduction Capacity (Capacidad Civil de Planeamiento y Ejecución de misiones civiles de la UE)
CSCE: Conferencia sobre la Seguridad y la Cooperación en Europa

Ediciones Universidad de Salamanca | CC BY-NC-ND

CSIRT: Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática)
CSN: Consejo de Seguridad Nacional (España)

DEA: Drug Enforcement Administration (Administración Antidroga de EE.UU.)
DGCE: Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad, del Ministerio del Interior (España)
DIH: Derecho Internacional humanitario
DISSC: Departamento de Infraestructura y Seguimiento de Situaciones de Crisis (España)
DMA: Digital Market Act (Ley del Mercado Digital)
DSA: Digital Services Act (Ley de Servicios Digitales)
DSN: Departamento de Seguridad Nacional (España)

EAS: Europol Analysis System (Sistema de Análisis de Europol)
EASO: European Asylum Support Office (Oficina Europea de Soporte al Asilo)
EC3: European Cybersecurity Competence Centre and Network (Centro Europeo de Competencia en Ciberseguridad)
ECI: Equipo Conjunto de Investigación
ECOSOC: Consejo Económico y Social de las Naciones Unidas
EDA/AED: European Defense Agency (Agencia Europea de Defensa)
EDAP: European Defense Action Plan (Plan de Acción Europeo de Defensa)
EDF/FED: European Defence Fund (Fondo Europeo de Defensa)
EDIP: European Defence Investment Programme (Programa Europeo de Inversión en Defensa)
EDMO: European Digital Media Observatory (Observatorio Europeo de Medios Digitales)
EDT: Emerging and Disruptive Technologies (Tecnologías Emergentes y Disruptivas)
EDTIB: European Defence Tecnological and Industrial Base (Base Industrial y Tecnológica de Defensa Europea).
EDPS: European Data Protection Supervisor (Supervisor Europeo de Protección de Datos)
EEAS: European Union External Action (Servicio Europeo de Acción Exterior)
EEMM: Estados Miembros de la Unión Europea
EES: Estrategia Europea de Seguridad (2003)
EES 2011: Estrategia Española de Seguridad: una responsabilidad de todos (2011)
EEUS: Estrategia de la UE para una Unión de la Seguridad (2020-2025)
EE.UU.: Estados Unidos
EFCSN: European Fact-Checking Standards Network (Red Europea de Estándares de Verificación)
EGPGC: Exército Guerrillheiro do Pobo Galego Ceive
EIGE: European Institute for Gender Equality (Instituto Europeo para la Igualdad de Género)
EIIL: Estado Islámico de Irak y Levante
ELSJ: Espacio de Libertad, Seguridad y Justicia de la UE
EMAD: Estado Mayor de la Defensa (España)
EMUE: Estado Mayor de la UE
EMCDDA: European Monitoring Centre for Drugs and Drug Addiction (Centro Europeo de Monitorización de Drogas y Toxicomanías)

Ediciones Universidad de Salamanca | CC BY-NC-ND

EMPACT: European Multidisciplinary Platform Against Criminal Threats (Plataforma Multidisciplinar Europea contra las Amenazas Criminales)
ENC: Estrategia Nacional de Ciberseguridad (España)
ENCCD: Estrategia Nacional contra las Campañas de Desinformación
ENCODG: Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (España)
ENCOT: Estrategia Nacional contra el Terrorismo (España)
ENFSI: European Network Of Forensic Science Institutes (Red Europea de Institutos de Ciencia Forense / Espacio Forense Europeo)
ENISA: European Union Agency for Cybersecurity (Agencia de la Unión Europea para la Ciberseguridad)
ENPC: Estrategia Nacional de Protección Civil (España)
EPPO: European Public Prosecutor´s Office (Fiscalía Europea)
ESAN: Estrategia de Seguridad Aeroespacial Nacional (España)
ESEN: Estrategia de Seguridad Energética Nacional (España)
ESI-UE: Estrategia de Seguridad Interior de la Unión Europea 2010-2015
ESMN: Estrategia de Seguridad Marítima Nacional (España)
ESN: Estrategia de Seguridad Nacional (España)
ETA: Euskadi Ta Askatasuna
EUAA: European Union Agency for Asylum (Agencia Europea para el Asilo)
EUBG: European Union Battlegroups (Grupos de Combate de la UE)
EUCS: European Union´s Cybersecurity Strategy for the Digital Decade (Estrategia Europea de Ciberseguridad para la Década Digital)
EU-CyCLONe: European Cyber Crises Liaison Organisation Network (Red Europea de Organizaciones de Enlace para la Cibercrisis).
EUDIS: European Union Defence Innovation Scheme (Programa Europeo de Innovación en Defensa)
EUGS: European Union Global Strategy (Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea, 2016)
EUHT: European Union Hybrid Toolbox (Caja de Herramientas Híbridas de la UE)
EU INTCEN: European Union Intelligence and Situation Centre (Centro de Inteligencia y de Situación de la UE)
EUISS: European Union Institute for Security Studies (Instituto de Estudios de Seguridad de la UE)
eu-LISA: European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (Agencia de la UE para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud)
EURATOM: Comunidad Europea de la Energía Atómica
EURDC: European Union Rapid Deployment Capacity (Capacidad de Despliegue Rápido)
EUROJUST: European Union Agency for Criminal Justice Cooperation (Agencia de la Unión Europea para la Cooperación Judicial Penal)
EUROPOL: European Union Agency for Law Enforcement Cooperation (Agencia de la Unión Europea para la Cooperación Policial)

FAMI: Fondo de Asilo, Migración e Integración de la UE
FBI: Federal Bureau of Investigation (Oficina Federal de Investigación de EE.UU.)
FCS: Fuerzas y Cuerpos de Seguridad

Ediciones Universidad de Salamanca | CC BY-NC-ND

FCSE: Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional y Guardia Civil)
FIMI: Foreign Information Manipulation and Interference (Manipulación e Interferencia de Información Extranjera)
FRA: Fundamental Rights Agency (Agencia Europea de Derechos Fundamentales)
FRAP: Frente Revolucionario Antifascista y Patriota
FRONTEX: European Border and Coast Guard Agency (Agencia Europea de la Guardia de Fronteras y Costas)
FSI: Fondo de Seguridad Interior de la UE

GAM: Grupo de Ayuda Mutua para cuestiones aduaneras de la UE
GEG: Grupos de Expertos Gubernamentales (Naciones Unidas)
GRAPO: Grupos de Resistencia Antifascista Primero de Octubre
GTCA: Grupo de Trabajo de Composición Abierta (Naciones Unidas)
GRU: Servicio de Inteligencia Militar de las Fuerzas Armadas de la Federación de Rusia

HII: Hecho internacionalmente ilícito
Hybrid CoE: European Centre of Excellence for Countering Hybrid Threats (Centro Europeo de Excelencia Contra las Amenazas Híbridas)
HVT/OTF: High Value Targets and Operational Task Forces (Objetivos de Alto Valor y Grupos de Acción Operativa)

IA: Inteligencia artificial
IApEES: Informe sobre la Aplicación de la Estrategia Europea de Seguridad (2008)
IFCN: International Fact-Checking Network (Red Internacional de Verificación de Datos)
INCIBE: Instituto Nacional de Ciberseguridad de España
IOCTA: Internet Organised Crime Threat Assesment (Informe de la amenaza de la delincuencia organizada en Internet de Europol)
IoT: Internet of Things (Internet de las cosas)

JAI: Consejo de Justicia y Asuntos de Interior de la Unión Europea
JIGC: Jefatura de Información de la Guardia Civil (España)
JISD: Joint Intelligence and Security División (División Conjunta de Inteligencia y Seguridad de la OTAN)

LAG: Loita Armada Galega
LOFCS: Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.
LSN: Ley 36/2015, de 28 de septiembre, de Seguridad Nacional

MAEC: Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (España)
MCCE: Mando Conjunto del Ciberespacio (España)
MCDC: Multinational Capability Development Campaign (Campaña Multinacional de Desarrollo de Capacidades)
MDO: Operaciones multidominio
MPAIAC: Movimiento para la Autodeterminación e Independencia del Archipiélago Canario.
MPCC: Military Planning and Conduction Capacity (Capacidad Militar de Planeamiento y Conducción de operaciones de la UE)

Ediciones Universidad de Salamanca | CC BY-NC-ND

NATO CCDCOE: NATO Cooperative Cyber Defense Centre of Excellence (Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN)
NCI Agency: NATO Communications and Information Agency (Agencia de Información y Comunicaciones de la OTAN)
NCS: NATO Command Structure (Estructura de Mando de la OTAN)
NIFC: NATO Intelligence Fusion Centre (Centro de Fusión de Inteligencia de la OTAN)
NIMSC: NATO Integrated Mobil Services Centre (Centro de Servicios Móviles Integrado de la OTAN)
NNUU: Naciones Unidas
NRBQ: Nuclear, radiológica, biológica y química
NSA: Agencia Nacional de Seguridad (EE.UU.)

OCC: Oficina de Coordinación de Ciberseguridad de la Secretaría de Estado de Seguridad, del Ministerio del Interior (España)
OCN: Oficina Central Nacional
ODM: Objetivos de Desarrollo del Milenio
ODS: Objetivos de Desarrollo Sostenible
OLAF: European Anti-Fraud Office (Oficina Europea de Lucha contra el Fraude)
OLCT: Oficina de Lucha contra el Terrorismo de Naciones Unidas
ONG: Organización no gubernamental
OSC: Organizaciones de la sociedad civil
OSCE: Organización para la Seguridad y Cooperación en Europa
OTAN/NATO: Organización del Tratado del Atlántico Norte
OTF: Operational Task Force (Grupo de Acción Operativa - Europol)

PCSD: Política Común de Seguridad y Defensa de la Unión Europea
PENCFIT: Plan Estratégico Nacional contra la Financiación del Terrorismo (España)
PENCRAV: Plan Estratégico Nacional de Prevención y Lucha contra la Radicalización Violenta (España)
PESC: Política Exterior y de Seguridad Común de la Unión Europea
PESCO: Permanent Structured Cooperation (Cooperación Estructurada Permanente)
PESD: Política Europea de Seguridad y Defensa (posteriormente pasa a denominarse PCSD).
PEV: Política Europea de Vecindad
PIDCP: Pacto Internacional de Derechos Civiles y Políticos
PPPRA: Plan de Prevención, Protección y Respuesta Antiterrorista (España)
PNR: Passenger Name Record (Registro de Nombres de Pasajeros)
PNUD: Programa de las Naciones Unidas para el Desarrollo

RAE: Real Academia Española
RAS: Rapid Alert System (Sistema de Alerta Rápida de la UE)
RG: Resistencia Galega
RGPD: Reglamento General de Protección de Datos (UE)
RMA: Revolución de Asuntos Militares

Ediciones Universidad de Salamanca | CC BY-NC-ND

SACEUR: Supreme Allied Commander Europe (Comandante Supremo Aliado de la OTAN en Europa)
SACLANT: Supreme Allied Commander Atlantic (Comandante Supremo Aliado del Atlántico)
SACT: Allied Command Transformation (Mando Aliado de Transformación OTAN)
SDN: Sociedad de las Naciones
SES: Secretaría de Estado de Seguridad del Ministerio del Interior (España)
SGPGIMS: Subdirección General de Planificación y Gestión de Infraestructuras y Medios para la Seguridad (España)
SIAC: Single Intelligence Analysis Capacity (Capacidad Única de Análisis de Inteligencia)
SIENA: Secure Information Exchange Network Application (Aplicación de la Red de Intercambio Seguro de Información - SIENA)
SIRENE: Supplementary Information Request at the National Entries (solicitud de información complementaria a la entrada nacional)
SIS: Sistema de Información Schengen
SOC: Security Operations Centre (Centro de Operaciones de Seguridad)
SOCTA: Serious and Organised Crime Threat Assesment (Informe de Amenaza de Crimen Organizado de Europol)
SSN: Sistema de Seguridad Nacional (España)
STC: Sentencia del Tribunal Constitucional
StratCom COE - NATO: NATO Strategic Communications Centre of Excellence (Centro de Excelencia de Comunicaciones Estratégicas de la OTAN)
STS: Sentencia del Tribunal Supremo

TCE: Tratado Constitutivo de la Comunidad Europea
TE-SAT: Terrorism Situation and Trend Report (Informe de Situación y Tendencias del Terrorismo de Europol)
TFUE: Tratado de Funcionamiento de la Unión Europea
TIC: Tecnologías de la Información y las Comunicaciones
TTP: Tácticas, Técnicas y Procedimientos
TUE: Tratado de la Unión Europea

UAS: Unmanned Aircraft System (sistema de aviones no tripulados)
UE: Unión Europea
UEO: Unión Europea Occidental
UNIP: Unidad Nacional de Información sobre Pasajeros (española)
UNODC: United Nations Office on Drugs and Crime
UO: Unión Occidental
URSS: Unión de Repúblicas Socialistas Soviéticas
USSS: United States Secret Service (Servicio Secreto de los Estados Unidos)

ZG: Zona Gris

Ediciones Universidad de Salamanca | CC BY-NC-ND

RESUMEN

Las formas de relacionarse los ciudadanos en todo el mundo han experimentado profundos cambios con el inicio del siglo XXI las cuales, entre otras, derivan de la generalización del uso de las conocidas como tecnologías de la información y las comunicaciones y el impulso experimentado por el ciberespacio como nuevo entorno global.

Sin embargo, el consiguiente proceso de *transformación digital* ofrece una doble perspectiva referida, por un lado, a los beneficios y, por otro, a los riesgos que ofrece a los usuarios. Así, la posibilidad de estar permanentemente informados y conectados a nuestras redes sociales nos hace pagar un peaje, que se cifra en la pérdida de intimidad y la monetización de nuestros datos personales por parte de empresas que, mediante complejos algoritmos, definen las preferencias de los usuarios. Estos son el anverso y el reverso de una misma moneda que ya no puede acuñarse de otra manera.

La propia evolución de la amenaza, ayudada por el proceso de tecnificación y digitalización, ha consolidado el indefinido ámbito de actuación entre la paz y la guerra que se conoce como *Zona Gris*, donde el ciberespacio ocupa un lugar preferente por derecho propio como escenario en el que se representa la *confrontación informativa* entre Estados, y respecto del que aún no hay acuerdo sobre si las actividades que en él se desarrollan están bajo el arbitrio del Derecho Internacional.

Fruto de este contexto y, también, de la propia permeabilidad de las democracias a la incorporación de tecnologías que contribuyan a mejorar la interacción entre personas e ideas, las nuevas *amenazas híbridas* suponen para aquellas un permanente foco de atención por cuanto las *injerencias extranjeras* y las *campañas de desinformación*, articuladas principalmente a través de los medios de comunicación digitales y las redes sociales, buscan socavar sus instituciones y generar dudas sobre la legitimidad de sus procesos, polarizando el debate social y político interno como vía de entrada para los extremismos, el odio y la radicalización.

La solución al problema se torna compleja porque la base de esta estrategia es el recurso a las emociones, a través de las que se busca captar la atención del público que, por lo general, carece de una adecuada *alfabetización digital y mediática* que le ayude a integrar toda esa información manipulada que le abruma y de la que no es plenamente consciente. La desafección ciudadana es el primer paso hacia la decadencia de los procesos democráticos, el abrazo social a las teorías conspirativas y la retroalimentación de las propias convicciones que beben de fuentes informativas contaminadas.

Por esta razón, nuestro estudio pretende recorrer el camino que transcurre desde las amenazas híbridas y, en concreto, la desinformación, hasta las graves consecuencias para la seguridad nacional de un Estado democrático y de derecho, a través del análisis de conceptos tradicionalmente vinculados al entorno físico como los de soberanía, seguridad, amenaza, guerra o terrorismo que hoy día, indefectiblemente, tienen sus *gemelos digitales* en el dominio del ciberespacio. En este sentido, la base conceptual y

Ediciones Universidad de Salamanca | CC BY-NC-ND

normativa del orden internacional debe ser profundamente revisada para, desde el acuerdo de todos los actores involucrados, integrar en ella la nueva dimensión de la soberanía digital, la ciberseguridad, la ciberamenaza, la ciberguerra o el ciberterrorismo.

Por ello, la presente investigación tiene como objeto final estudiar la seguridad nacional española y analizar la afectación que para ella supone la actual amenaza desinformativa, materializada a través de la manipulación de la opinión y los actos de los ciudadanos.

En cuanto a la metodología utilizada, este estudio se ha vertebrado desde el Derecho Constitucional por su carácter central frente a otras disciplinas jurídicas, como el Derecho Internacional, apoyándose de forma instrumental en otras ciencias como la Sociología, la Politología, las Ciencias Policiales y las Tecnológicas, lo cual nos puede ayudar a comprender mejor las afirmaciones expuestas y las preocupaciones subyacentes en esta investigación. De esta manera, son el sincretismo y la interdisciplinariedad las bases metodológicas.

Partiendo de este presupuesto, hemos planteado nuestra investigación desde una perspectiva inductiva-deductiva, lo cual nos permite generar nuevas ideas a partir del análisis de los marcos normativos y teóricos existentes para, posteriormente, verificar las premisas con las que operan e ir comprobando nuestra hipótesis de trabajo.

Esta investigación se desarrolla a través de ocho capítulos, siendo el primero de ellos el dedicado a los conceptos de *soberanía y seguridad*, claves para entender el contexto en el que se sustancia el análisis del resto de materias. En el segundo capítulo estudiamos la construcción del concepto de *seguridad multidimensional* a través de las dos principales estructuras de cooperación internacionales: las Naciones Unidas y la Organización del Tratado del Atlántico Norte. El tercer capítulo propone una revisión de la *estrategia de seguridad europea* a tenor de la cada vez mayor relevancia del ciberespacio como quinto dominio en el que se desenvuelven las relaciones entre los Estados. El cuarto capítulo presenta el *modelo de respuesta español* a los desafíos de seguridad tradicionales y emergentes, haciendo referencia al carácter innovador de su Ley de Seguridad Nacional. En el quinto se analiza la *evolución de las amenazas a la seguridad y su vinculación con la singularidad del ciberespacio*, centrándonos en las tres principales actualmente: la guerra, el terrorismo y las ciberoperaciones. El capítulo sexto explica *el desafío de seguridad en la Zona Gris*, y presenta la desinformación como principal exponente de las amenazas híbridas con las que se desgasta a las democracias. El séptimo capítulo presenta *la estrategia de la Unión Europea frente a la amenaza desinformativa*, con especial atención a la injerencia extranjera en sus procesos electorales. Finalmente, el capítulo octavo estudia *la respuesta española frente a la amenaza desinformativa con afectación a la seguridad nacional*, a través del repaso de los instrumentos normativos y técnicos de que se dispone en el marco de nuestra democracia constitucional.

Respecto a la bibliografía utilizada y resto de soporte documental, no solo se han tomado en consideración fuentes directas como monografías, manuales y artículos científicos, que muestran el aspecto más específico de la materia, sino que también hemos utilizado fuentes primarias tanto internacionales como comunitarias y

Ediciones Universidad de Salamanca | CC BY-NC-ND

nacionales. De igual modo, hemos ampliado el conocimiento de la materia acudiendo a páginas webs y otros recursos digitales sin los cuales no hubiera sido posible acceder a la variedad de documentación que sustenta esta investigación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

ABSTRACT

The ways in which citizens relate to each other around the world have undergone profound changes at the beginning of the twenty-first century, which, among others, derive from the generalization of the use of what are known as information and communication technologies and the impulse experienced by cyberspace as a new global environment.

However, the ensuing process of digital transformation offers a double perspective referring, on the one hand, to the benefits and, on the other, to the risks it offers to users. Thus, the possibility of being permanently informed and connected to our social networks makes us pay a toll, which is the loss of privacy and the monetization of our personal data by companies that, through complex algorithms, define the preferences of users. These are the obverse and reverse of the same coin that can no longer be minted in any other way.

The evolution of the threat itself, aided by the process of technification and digitalization, has consolidated the undefined scope of action between peace and war known as the *Grey Zone*, where cyberspace occupies a preferential place in its own right as a scenario in which the *confrontation of information* between States is represented, and on which there is still no agreement on whether the activities carried out in it are under the control of the arbitrariness of International Law.

As a result of this context and also of the very permeability of democracies to the incorporation of technologies that contribute to improving the interaction between people and ideas, the new *hybrid threats* are a permanent focus of attention for them as *foreign interference* and *disinformation campaigns*, mainly articulated through digital media and social networks, They seek to undermine its institutions and generate doubts about the legitimacy of its processes, polarizing the internal social and political debate as a gateway for extremism, hatred and radicalization.

The solution to the problem becomes complex because the basis of this strategy is the use of emotions, through which it seeks to capture the attention of the public who, in addition, lacks adequate *digital and media literacy* to help them integrate all that manipulated information that overwhelms them and of which they are not fully aware. Citizen disaffection is the first step towards the decay of democratic processes, the social embrace of conspiracy theories and the feedback of one's own convictions that drink from contaminated information sources.

For this reason, our study aims to trace the path that runs from the hybrid threat and, specifically, disinformation, to the serious consequences for national security of a democratic State governed by the rule of law, through the analysis of concepts traditionally linked to the physical environment such as those of sovereignty, security, threat, war, or terrorism that today, Unfailingly, they have their *digital twins* in the domain of cyberspace. For this reason, the conceptual and normative basis of the international order must be thoroughly reviewed in order to, with the agreement of all

Ediciones Universidad de Salamanca | CC BY-NC-ND

the actors involved, integrate into it the new dimension of digital sovereignty, cybersecurity, cyber threat, cyberwar or cyberterrorism.

Therefore, the final objective of this research is to study Spanish national security and analyse the impact that the current disinformation threat represents for it, materialised through the manipulation of the opinion and actions of citizens.

Regarding the methodology used, it should be noted that this study has been structured from Constitutional Law due to its interconnection with other legal disciplines, such as International Law, and other non-legal disciplines, such as Sociology, Politics, Police and Technological Sciences, which can help us to better understand the statements made and the underlying concerns in this research. In this way, syncretism and interdisciplinarity are the methodological bases.

Based on this assumption, we have approached our research from an inductive-deductive perspective, which allows us to generate new ideas from the analysis of the existing normative and theoretical frameworks in order to subsequently verify the premises with which they operate and to verify our working hypothesis.

This research is developed through eight chapters, the first of which is dedicated to the concepts of *sovereignty and security*, key to understanding the context in which the analysis of the rest of the subjects is substantiated. In the second chapter, we study the construction of the concept of *multidimensional security* through the two main structures of international cooperation: the United Nations and the North Atlantic Treaty Organization. The third chapter proposes a review of the *European security strategy* in light of the growing importance of cyberspace as the fifth domain in which relations between States develop. The fourth chapter presents the *Spanish response model* to traditional and emerging security challenges, referring to the innovative nature of its National Security Law. The fifth analyses the *evolution of security threats and their link with the uniqueness of cyberspace*, focusing on the three main ones today: war, terrorism and cyber operations. The sixth chapter explains *the security challenge in the Grey Zone*, and presents disinformation as the main exponent of the hybrid threats with which democracies are worn down. The seventh chapter presents the *European Union's strategy in the face of the disinformation threat*, with special attention to foreign interference in its electoral processes. Finally, the eighth chapter studies *the Spanish response to the disinformation threat affecting national security*, through a review of the regulatory and technical instruments available within the framework of our constitutional democracy.

With regard to the bibliography used and the rest of the documentary support, not only have direct sources such as monographs, manuals and scientific articles been taken into consideration, which show the most specific aspect of the subject, but we have also used international, EU and national primary sources. In the same way, we have expanded our knowledge of the subject by going to websites and other digital resources without which it would not have been possible to access the variety of documentation that supports this research.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 1. SOBERANIA Y SEGURIDAD

La necesidad del ser humano de conseguir un entorno de seguridad ha sido uno de los motores de la vida social organizada a lo largo de los tiempos. La garantía de la seguridad se ha interpretado como una necesidad humana desde los orígenes de la sociedad, dotándose para ello de fuerzas a las que confiar esta misión desde muy antiguo (RIDAURA MARTÍNEZ, 2014, pág. 320). Estas pretéritas formas de organización social de carácter preestatal, como por ejemplo las *polis* griegas o las *civitas* romanas, comparten como elemento común una perspectiva personal de la seguridad basada en la vinculación personal con un tercero que la provee, pero sin una base de autoridad o legitimidad sustentada en un poder jurídico-político y coactivo, que serán definitivos posteriormente para la concepción estatocéntrica de la seguridad.

Abraham Maslow, en su pirámide de motivación de la conducta humana, sitúa las necesidades de seguridad en el segundo nivel, justo después de las necesidades más básicas de soporte vital y por delante del resto de necesidades sociales, de estima y autorrealización, señalando además que aquellas "sólo pueden ser satisfechas por los demás, es decir, desde fuera de la persona. Esto implica una considerable dependencia del exterior" (MASLOW, 2007, págs. 60-61), que se traduce en que una persona, por sí sola, no controla o gobierna plenamente su seguridad.

Es por ello que la seguridad, en su concepción clásica vinculada al Estado como estructura política y único gestor del ejercicio de la jurisdicción y de la fuerza legítima dentro de su territorio, se entiende como la protección de los ciudadanos y de la riqueza del Estado, que se garantiza a través del ejercicio del poder soberano. Esta es la base del acuerdo por el que el príncipe absolutista se obliga a garantizar la seguridad de sus súbditos frente a la amenaza externa y a mantenerles satisfechos con una paz interna auspiciada por el equilibrio en sus acciones, a cambio de la lealtad de aquellos que habrá de mantenerle en el poder soberano (MAQUIAVELO, 1994, pág. 124). Es así como se da forma al contrato que vincula la soberanía con la seguridad en el marco del Estado.

La cada vez mayor complejidad del entramado de relaciones inter, supra e intranacionales han impulsado la evolución de estos dos conceptos tan íntimamente relacionados hasta llegar al siglo XXI donde la seguridad, en una interpretación extensiva, se concibe no ya como propia del individuo sino del conjunto de la especie humana, mientras que la soberanía trasciende el plano físico del territorio y las aguas territoriales correspondientes para alcanzar el espacio aéreo ultraterrestre e, incluso, las distintas capas del ciberespacio asociadas al Estado.

1.1. La evolución de la soberanía desde el Estado moderno hasta la llegada del nuevo dominio digital

El Estado moderno derivado de las revoluciones constitucionales del siglo XVIII marca un punto de inflexión en la teorización del concepto de soberanía por cuanto, hasta ese momento, se asimila al rey y éste, a su vez, al Estado. Será por efecto de estas revoluciones –principalmente la americana y la francesa- que la noción de soberanía

Ediciones Universidad de Salamanca | CC BY-NC-ND

comienza a expandirse para dar cobijo a una serie de nuevas instituciones, como el Parlamento, que contrarias a la concentración del poder en el rey tratan de acercarlo a los ciudadanos e incidir en el carácter nacional de dicha soberanía, sobre la que ya en el siglo XIX se articulará el concepto de soberanía popular como base del Estado. Posteriormente, tras un siglo XX castigado por dos Guerras Mundiales, la propia evolución geopolítica internacional y el paso, a través de la globalización, a la Era Digital con nuevos dominios *no físicos*, harán necesaria la revisión conceptual de la soberanía, de la seguridad e, incluso, del elemento territorial del Estado.

Define el diccionario de la Real Academia Española la *soberanía* como "cualidad de soberano", sinónimo de autoridad, poder e independencia, y en su segunda acepción como "poder político supremo que corresponde a un Estado independiente". Es evidente que al proceder a la fijación del concepto de soberanía tenía la Academia en mente el modelo del Estado moderno, caracterizado por su poder independiente y su autoridad incontestada dentro del territorio que gobierna.

Pero el nacimiento en 1989 de la World Wide Web, casualmente el mismo año de la caída del Muro de Berlín, supone el pistoletazo de salida para el fenómeno de la globalización y, con ella, de nuevos retos ligados a la evolución de la tecnología y su afectación al ámbito de las relaciones humanas a todos los niveles, incluidas lógicamente las derivadas de la soberanía que los Estados ejercen dentro de sus fronteras, de manera autónoma y aceptada por sus iguales, desde el siglo XVI.

1.1.1. El Estado Moderno y su visión del poder soberano

El concepto de soberanía como poder final e ilimitado ejercido en el interior del territorio y proyectado hacia el exterior está unido al surgimiento del Estado moderno (GÖRLITZ, 1980, pág. 589), forma política prevalente hasta la Segunda Guerra Mundial en la que la sacrosanta soberanía y las fronteras son sus baluartes principales (BARBÉ IZUEL, 2004, pág. 22).

Previamente, en las comunidades políticas medievales no existía un poder central y único facultado para tomar decisiones finales y con el monopolio de la coacción física legítima para llevarlas a efecto, sino que la pirámide feudal del poder se cimentaba sobre una base multijurisdiccional de señores, municipios y estamentos dotados de derecho propio que, en régimen de vasallaje, se relacionaban con el emperador en la cúspide para, a cambio de la servidumbre, poder mantener y ejercer la jurisdicción sobre la tierra y la población sobre ella asentada. Este mismo constructo se articulaba de forma paralela en torno al Papa, autoridad espiritual que convivía en dualidad con el poder temporal del emperador. Esta construcción poliárquica medieval se soportaba en las obligaciones que vinculaban a ambas partes y la lealtad en el mantenimiento del equilibrio que les daba soporte. Será la evolución de estas dos potestades, civil y religiosa, la que prepare el terreno para que, más tarde, se construya el concepto de soberanía unida al Estado nación moderno (ALZAGA VILLAAMIL & ÁLVAREZ RODRÍGUEZ, 2021, pág. 111).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Una línea de pensamiento diferente se abre paso en 1513 con Nicolás Maquiavelo y su original obra *El Príncipe*, que rompe con los tratados humanísticos y medievales anteriores para presentar un orden político regenerado a través de un príncipe nuevo que, aunque bajo diferentes formas y modelos, en todo caso "tiene que tener al pueblo de su parte, o de lo contrario no tendrá salvación en los momentos de peligro" (MAQUIAVELO, 1994, pág. 79). Para ello el príncipe habrá de perseguir en sus designios el bien común, que abarca el de los individuos que conforman el pueblo y el de la totalidad del colectivo -que es más que la simple suma de sus componentes-, al que hay que añadir también el del Estado como "personalidad colectiva incluso mucho más organizada, que podía imponer su voluntad en todo momento. La ley de esta voluntad era la razón de Estado: éste fue el gran descubrimiento de Maquiavelo" (MEINECKE, 2014, pág. 352)

Un paso más avanza Jean Bodin[1] en 1576, con su teoría de la soberanía únicamente limitada por la ley natural, donde se marca el inicio de la teoría política moderna. A partir de ahora el príncipe ostenta un poder perpetuo e inmutable, absoluto, que solo responde ante Dios -a quien representa en la tierra- y que le permite dictar leyes bajo la premisa del *solutus legibus*. En el soberano, que debe ser un rey, no una nación, se encuentra la cúspide el Estado y de él deriva la base jurídica que sustenta los derechos, poderes y privilegios del resto de estamentos, corporaciones, ciudades y colectivos de funcionarios (ALZAGA VILLAAMIL & ÁLVAREZ RODRÍGUEZ, 2021, pág. 112). Solo la ley natural, como manifestación de la ley divina, limita el poder del soberano que, a su vez, encuentra en la religión una aliada para mantener su autoridad y garantizar la obediencia y sometimiento de los súbditos (JURI, 2019, págs. 69-86).

En 1651, apenas dos años después de que el Parlamento inglés cortara la cabeza a su rey Carlos I y se constituyera bajo el liderazgo de Cromwell en la *Commonwealth*, Thomas Hobbes publica su *Leviathan o la materia, forma y poder de una República eclesiástica y civil,* en el que defiende un poder soberano absoluto e indivisible, que obtiene su legitimación del contrato entendido como "mutua transferencia de derechos" que acuerdan sus súbditos para garantizarse la paz que necesitan (HOBBES, 2013, págs. 174-175). Totalmente opuesto a la visión aristoteliana del hombre sociable *per se*, el positivismo de Hobbes le lleva a considerar que el estado natural del hombre es la guerra perpetua de todos contra todos -*homo homini lupus*-, donde cada uno toma lo que puede y lo mantiene solo durante el tiempo que su fuerza y su astucia le permitan conservarlo, por cuanto "hallamos en la naturaleza del hombre tres causas principales de discordia: la competencia, la desconfianza y la gloria" (HOBBES, 2013, pág. 166). Para liberarse de ese designio y alcanzar la organización política de un Estado, los hombres deben acordar renunciar al derecho natural absoluto que poseen sobre toda cosa en favor de un tercero, ajeno a dicho contrato, que sustituirá la voluntad de todos ellos y, al mismo tiempo, los representará y protegerá garantizando su seguridad. El soberano, sea persona o asamblea, exhibe un poder absoluto e indivisible, por encima de ese pacto entre los súbditos y, como tal, *solutus legibus* por cuanto es el único poder legislativo.

[1] Los *Seis libros de la República* es la obra clave de ciencia política de Jean Bodin (1530-1596), que publica en francés ya con cuarenta y seis años y que sin duda es la cima de su propuesta intelectual, por cuanto vertebra el concepto de soberanía en torno a la potestad del príncipe para dictar ley exigible a todos y a cada uno de sus súbditos *sin el consentimiento de más grande ni de igual ni de menor que él.*

Ediciones Universidad de Salamanca | CC BY-NC-ND

De esta manera, el Estado que se acuerda sobre la base de las voluntades individuales de los hombres puede definirse como:

> "Una persona de cuyos actos una gran multitud, por pactos mutuos realizados entre sí, ha sido instituida por cada uno como autor, al objeto de que pueda utilizar la fortaleza y medios de todos como lo juzgue oportuno para asegurar la paz y defensa común. El titular de esta persona se denomina soberano, y se dice que tiene poder soberano; cada uno de los que lo rodean es súbdito suyo" (HOBBES, 2013, pág. 193).

Habrá de ser John Locke quien, apoyándose en su *Ensayo sobre el gobierno civil* (1660), cuestione el paradigma del absolutismo y resquebraje la escuela del derecho divino. El filósofo y pensador inglés sostiene que los hombres están razonablemente bien en el estado de naturaleza, donde el ejercicio de la libertad, la igualdad y la propiedad se regulan por la ley natural, pero que en su ánimo de mejorar consienten en depositar en el estado de sociedad el poder de gobierno y que sea éste quien garantice el bien público. Son los ciudadanos los que tienen el auténtico poder soberano que se entrega, a través de ese contrato de depósito, a los gobernantes –sean reyes o parlamentos- quienes tendrán que ejercerlo dentro del marco de lo que el bien público exige y, para que no sea ni absoluto ni arbitrario, separando el legislativo –poder supremo al que corresponde la última palabra- del ejecutivo –poder subordinado que siempre debe estar dispuesto a hacer ejecutar la ley-. En este equilibrado arco político la clave de bóveda es el *derecho de insurrección del pueblo*, cuyo uso servirá para recobrar la soberanía en caso de que los gobernantes obren de manera contraria al fin para el que recibieron dicha autoridad.

En *El contrato social* (1762), Rousseau va más allá señalando que la fundamentación de la obligación social no es tanto la fuerza como la libre convención de los ciudadanos, cada uno de los cuales se compromete bajo las mismas condiciones para gozar de los mismos derechos. El soberano es el pueblo tomado en corporación, cuya voluntad general no es la simple suma de la voluntad de todos, ni siquiera la del mayor número, sino la que quiere el interés general en cuanto provecho del grupo. Por esto, obedecer al pueblo soberano es muestra de la libertad del ciudadano, que libremente decide someter su voluntad particular a la voluntad general, con la que se conforma una soberanía inalienable, indivisible, infalible y absoluta[2].

Hasta aquí podemos concluir que la soberanía supone en el periodo del absolutismo un poder igualmente absoluto e ilimitado, que ejerce directamente el monarca y cuya legitimidad deriva de su compromiso como Estado para garantizar el interés general y la paz del pueblo que ocupa su territorio. Sus únicos límites los marca el Derecho natural y la conveniencia de intereses con la Iglesia y otros poderes fácticos económicos. La

[2] En la teoría política de Rousseau la soberanía se empareja con la voluntad general, con la que comparte los rasgos distintivos de *inalienable* –por cuanto no puede ser representada dado que la voluntad del pueblo no puede transmitirse-, *indivisible* –ya que la voluntad general es la voluntad del pueblo soberano, no de una parte más o menos numerosa, que no dejaría de ser una voluntad particular-, *infalible* –puesto que la voluntad general es siempre acertada en su búsqueda de la utilidad pública-, y *absoluta* –el pacto social le entrega al pueblo soberano un poder absoluto sobre todos los ciudadanos libremente constituidos en corporación-.

Ediciones Universidad de Salamanca | CC BY-NC-ND

revolución liberal supone un factor disruptivo por cuanto traslada la titularidad de la soberanía a la nación que, a partir de entonces, ostenta el poder constituyente para establecer las reglas de convivencia y los principios fundamentales del sistema político, delegando en la Asamblea representativa el ejercicio diario de ese poder limitado por el marco jurídico y político definido por la nación (ALZAGA VILLAAMIL & ÁLVAREZ RODRÍGUEZ, 2021, pág. 117).

Evidentemente, conforme avanza el desarrollo de las estructuras sociales y se complican las relaciones humanas, más ardua es la tarea de gobernar. La convulsa Europa del siglo XIX obliga a los pensadores dedicados al estudio del gobierno y la sociedad a mirar hacia otro lado buscando modelos pacíficos y exitosos. La revolución liberal deja atrás el modelo del Antiguo Régimen enterrando el poder absoluto del monarca y, con ello, la sumisión del Estado al Derecho (RIDAURA MARTÍNEZ, 2014, pág. 322).

En este contexto de búsqueda de nuevos horizontes, viaja Alexis de Tocqueville a Estados Unidos para, con el pretexto de analizar su sistema penitenciario, sacar conclusiones de la democracia como sociedad igualitaria que serán reflejadas en su obra *La democracia en América* (1835). Para el aristócrata y autor francés es la igualdad la que, de forma natural, lleva a los hombres a la confianza en las instituciones libres, puesto que:

> "[…] en América, el principio de la soberanía del pueblo no es cosa oculta o estéril, como en ciertas naciones, sino que se le reconoce en las costumbres y se le proclama en las leyes, se extiende con libertad y llega sin obstáculos a sus últimas consecuencias" (TOCQUEVILLE, 1980, pág. 55).

Es así que la igualdad social conduce a la igualdad política, la cual se perfecciona en el pueblo soberano que actúa por sí mismo, con un poder absoluto justificado en las decisiones de la mayoría que, de igual manera, no reconoce poder externo alguno, concluyendo que "el pueblo reina sobre el mundo político americano como Dios sobre el universo. Él es la causa y el fin de todas las cosas; todo sale de él y todo se incorpora de nuevo a él" (TOCQUEVILLE, 1980, pág. 57).

Sin embargo, la visión alemana de la soberanía, encabezada por el modelo de monarquía constitucional de Hegel, se construye desde la función que aquella tiene de garantizar la unidad y la identidad del Estado, tanto hacia el interior como hacia el exterior, que representa un bien superior y que tiene en la *constitución* la clave del equilibrio de poderes que lo conforman. La soberanía interior del Estado reside en el pueblo y se realiza en el interés universal que determina las decisiones del monarca, que son aplicadas por el cuerpo de funcionarios especializados que conforman la administración centralizada que caracteriza al estado hegeliano (BAVARESCO, 2003, págs. 55-80). Frente al exterior, la individualidad y legitimación del Estado se articula a través del proceso de reconocimiento por parte de otros Estados igualmente independientes, y se manifiesta en el derecho a firmar acuerdos con ellos (*ius foedus*), así como en el derecho a proclamar la guerra (*ius ad bellum*) como remedio para la natural contingencia de los tratados firmados. Por encima de los Estados soberanos no existe ninguna autoridad superior con capacidad jurídica reconocida por todos para dictar solución a los conflictos entre sus intereses vitales, de manera que queda libre así el camino a la violencia en sus

Ediciones Universidad de Salamanca | CC BY-NC-ND

relaciones y se abre la puerta a las tentaciones consustanciales a la ambición de poder. Sin embargo, "la razón de Estado pone de manifiesto, empero, de nuevo en esta situación su escisión y ambivalencia íntimas, porque tiene que temer justamente aquellas potencias elementales que ella misma pone en juego" (MEINECKE, 2014, pág. 16), obligándole al Estado a autolimitarse poniéndose al servicio de los intereses generales que, a través del equilibrio de fuerzas y la equidistancia entre la amistad y la hostilidad, la paz y la guerra, procuran la tranquilidad y la continuidad en las relaciones de poder entre aquellos, generando un entorno de precaria estabilidad.

La creación del Tribunal Permanente de Arbitraje en la Conferencia de La Haya de 1899, materializa el esfuerzo de la sociedad internacional –por entonces mayormente referida a Europa- por encontrar un modelo de relación entre Estados que, sobre el ideal de un nuevo marco normativo garante de un interés superior al hasta entonces definido por el egoísmo de las naciones, asegure la paz y el ordenamiento jurídico internacional como escenario para el desarrollo económico y el funcionamiento de estos, rechazando el recurso a la guerra como forma de solución de conflictos. El Derecho Internacional se construye sobre la tesis de que los Estados son soberanos, puesto que se parte de que en la comunidad internacional no existe una autoridad superior a ellos. De aquí se derivan tres rasgos tradicionalmente aceptados: la igualdad entre los Estados, su independencia y consiguiente prohibición de que otro Estado intervenga en sus asuntos, y la propia soberanía del Estado como base del ordenamiento jurídico internacional. De ahí que se considere que "el Estado, en el plano del Derecho Internacional, es soberano cada día del año" (ALZAGA VILLAAMIL & ÁLVAREZ RODRÍGUEZ, 2021, págs. 117-118).

De esta manera, la mediación y el arbitraje van forjándose como auténticos mecanismos de regulación de las diferencias internacionales (LÓPEZ CORDÓN, 1982, págs. 703-708), aunque aún dependiente del libre sometimiento de los Estados soberanos, pues no existe un órgano superior dotado del poder de obligar al cumplimiento y sancionar las infracciones. Es en este contexto en el que, en 1928, el citado Tribunal Permanente dicta el laudo arbitral de la Isla de Palmas[3], en razón a una disputa territorial entre Estados Unidos y Países Bajos, en el que fija una definición de soberanía que fue bien recibida en el ámbito internacional y que, posteriormente, se recoge por el Grupo Internacional de Expertos de Tallin, que dispone[4]:

> "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State" (SCHMITT, 2017, p. 11).

[3] Laudo arbitral de la Corte Permanente de Arbitraje. Asunto de la Isla de Palmas, Estados Unidos de América vs. Países Bajos. Abril de 1928.
Se trata de un litigio entre Estados Unidos y Países Bajos en relación con la soberanía de la citada isla, que había sido cedida por España al primero mediante el Tratado de París de 1898, pero que reclamaba el segundo de los países litigantes. Disponible en: https://es.scribd.com/document/440736120/Fallo-Isla-de-Palmas (20/04/2023).

[4] "La soberanía en las relaciones entre Estados significa independencia. La independencia respecto a una porción del globo es el derecho a ejercer en ella, con exclusión de cualquier otro Estado, las funciones propias de un Estado" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Sin embargo, la decisiva influencia que a principios del siglo XX ejerce sobre el estudio sustantivo del Estado el pensamiento de Georg Jellinek, soportado en el territorio como escenario del poder, en la población como sujeto y objeto de su actividad[5] y, en tercer lugar, en la soberanía como ejercicio autónomo de sus competencias (JELLINEK, 2000, págs. 368-400), comienza a cuestionarse a raíz de la fundación en Europa a mediados de siglo de estructuras de poder supranacionales, que asumen gran parte de los designios políticos, económicos y normativos antes reservados a la decisión de los Estados, como por ejemplo el proceso de integración de la Unión Europea que conlleva una cierta *mutación* de la soberanía de sus Estados miembros:

> "Claro es que una de las principales características de la integración europea es la de avanzar progresivamente en sus lazos confederativos, y ello significa que la soberanía de los Estados miembros subsiste, pero con progresivas limitaciones prácticas […]. Y es que el poder de los Estados soberanos miembros de la Unión Europea ya no es absolute en el grado en que concebían los clásicos al soberano como *legibus solutus*" (ALZAGA VILLAAMIL & ÁLVAREZ RODRÍGUEZ, 2021, págs. 119-120).

En esta nueva configuración del orden mundial, los países se asocian y acuerdan el traspaso de competencias a esas agrupaciones políticas y organismos internacionales de cuyas decisiones ahora dependen y que, por ello, condicionan y limitan su soberanía, tanto interior como exterior, hasta entonces ejercida de forma individual y plena, buscando beneficios económicos, políticos y culturales que conlleven prosperidad y seguridad para ellos. Puede hablarse así del Estado posmoderno como especie nueva que evoluciona y va más allá de su ancestro, el Estado westfaliano, al aceptar la injerencia externa en los asuntos domésticos en cuanto "democracias avanzadas y economías altamente desarrolladas, en las que el poder es más difuso, con diferentes tipos de recursos, de actores y a diferentes niveles (supranacionales, subestatales)" (BARBÉ IZUEL, 2004, págs. 24-25).

Al tiempo que esto ocurre, consecuencia del resultado de la Segunda Guerra Mundial, se configura un nuevo esquema mundial bipolar y enfrentado que, liderado por Estados Unidos (EE.UU.) y la Unión de Repúblicas Socialistas Soviética (URSS), obliga al resto de países a posicionarse política e ideológicamente bajo su supremacía económica y militar. La Guerra Fría confronta directamente a las dos superpotencias y sus respectivas zonas de influencia, de manera que si cualquiera de ellos inicia acciones en el entorno geográfico del otro, podría suponer el inicio de la guerra. Esos fuertes lazos de dependencia vinculados a la alianza estratégica con uno de los bandos tienen profundas repercusiones políticas, económicas y culturales que, lógicamente, debilitan el ámbito de decisión soberana de los Estados afectados que, alineados con su líder, *tendrán que* optar por lo que convenga al bloque para mantener ese complicado equilibrio metaestable entre ellos. Podríamos así hablar de una especie de *federalismo ideológico encubierto*, con las implicaciones derivadas.

[5] Para Jellinek la soberanía pertenece no a la nación sino al Estado como tal, y aquella es un órgano de este.

Ediciones Universidad de Salamanca | CC BY-NC-ND

A partir de la disolución de la URSS en 1991, se configura un orden internacional *unipolar y multinivel* dominado en solitario por EE.UU. que, aun asumiendo el rol de superpotencia y queriendo ejercerlo, necesita apoyar sus políticas en organizaciones internacionales como la Organización de Naciones Unidas (NNUU) y la Organización del Tratado del Atlántico Norte (OTAN) para poderlas llevar a la práctica (ZURITA, 2007, pág. 5), toda vez que comienzan a surgir nuevas amenazas como el terrorismo de carácter internacional, el crimen organizado transnacional o la instrumentalización de los flujos migratorios irregulares como elemento de presión en frontera, que desdibujan la clásica distinción entre seguridad interior y seguridad exterior, vistas a partir de ahora como parte de un continuo en el que el Estado y sus elementos diferenciadores –territorio, población y soberanía- deben adaptarse para sobrevivir en ese contexto donde el poder ya no se identifica con la fuerza, y que hace de la cooperación internacional y las estructuras de poder supranacionales la clave de subsistencia.

Este mundo global y posmoderno que se vislumbra a finales del siglo XX, enfocado hacia la integración voluntaria de naciones como respuesta más viable ante los nuevos desafíos que se plantean, tiene un precio que los Estados de la Unión Europea han podido comprobar de primera mano: la *autolimitación de la soberanía* entendida como la transferencia de competencias y la sumisión al órgano superior jerárquico, con el compromiso de los Estados miembros de ejecutar la decisiones que aquel adopte (ÁLVAREZ ROBLES, 2024). Esta cesión en el caso europeo conlleva que el Derecho nacional no sea único ni supremo en su territorio, que su máximo Tribunal no ejerza jurisdicción superior en el Estado, que se pierda la competencia para regir la política monetaria o que las fronteras se relativicen, entre otras cuestiones. Todo ello parece apuntar hacia una crisis del concepto estricto de soberanía definida como:

> "[…] potencia absoluta y perpetua bodiniana y hobbesiana; poder absoluto, ilimitado, indivisible, inapelable, incontrolable, independiente ad extra y supremo ad intra. Esa potestad absoluta puede desplazarse del monarca absoluto al pueblo, a un órgano o a tres, o al estado en abstracto, pues siempre será mejor que el poder se institucionalice y no se concentre en una persona. Pero mientras siga teniendo aquellas características, que no excluyen cierta crudeza si llega el caso, seguirá siendo soberanía" (PEREIRA MENAUT, 2001, pág. 62).

En este sentido, se asiste a una relativa difusión de la competencia en la toma de decisiones políticas desde los gobiernos nacionales hacia organizaciones internacionales funcionales, en lo que parece una pérdida de terreno de las nunca antes cuestionadas atribuciones del Estado nación moderno en el plano de la política mundial (STEFFEK, 2007, págs. 109-129). Pero eso no significa, a nuestro modo de ver, que la estructura política, social, cultural y económica que sustenta al Estado y, con ello, su soberanía, se diluya por completo sino que, al contrario, se adapta convenientemente al nuevo contexto situacional en el que el Estado pasa a ser un actor cualificado que dirige sus políticas en un modelo de gobernanza multipolar, junto con otros actores de variada naturaleza y con intereses legítimos, donde la separación entre el ámbito interno y externo de su política se confunde por la complejidad de las nuevas relaciones y equilibrios de poder entre Estados, y en el que la cooperación internacional pasa a ser un elemento fundamental de seguridad ante la nueva dimensión de las amenazas, que trascienden la capacidad de respuesta individual de cada uno de ellos y exigen el

Ediciones Universidad de Salamanca | CC BY-NC-ND

concierto de voluntades de otros Estados soberanos. Por ello, lejos de desaparecer, "en el siglo XXI, más que nunca, la soberanía implica responsabilidad"[6].

1.1.2. La soberanía digital

La evolución del concepto de soberanía vinculado al mundo físico tradicional, que hemos analizado en el apartado precedente, se caracteriza de manera destacada por el ejercicio supremo e independiente de la autoridad del Estado dentro de su territorio, aún incluso en el contexto de las relaciones internacionales. No obstante, la aparición en el siglo XXI de nuevos escenarios de actividad humana, como el espacio ultraterrestre, el ciberespacio o el ámbito cognitivo, traen consigo prometedoras ventajas y complejas amenazas que cuestionan la relación de la soberanía con el Estado.

En este complejo sistema en continua evolución, los cinco dominios reconocidos -terrestre, marítimo, aéreo, espacial y cibernético- se relacionan con las tres dimensiones de sus efectos -físicos, virtuales y cognitivos- y los diferentes ámbitos en que actúan -político, militar, económico, social, e informativo-, conformando una serie de interrelaciones que trascienden ampliamente la dimensión física para dar relevancia a la intangible, en la que predominan las ideologías, los valores y las narrativas de opinión que tratan de condicionar el comportamiento humano. Las fronteras territoriales y la distinción de su vertiente interna y externa quedan no ya superadas sino, directamente, anuladas en este *sistema multidominio* en el que se desempeñan tanto las relaciones internacionales como las humanas.

En este contexto, el ciberespacio o *quinto dominio* se entiende como:

> "[…] una dimensionalidad añadida a las que han modelado nuestra experiencia vital como seres humanos. Las 4 dimensiones espacio-temporales que han servido para configurar toda nuestra cultura y nuestro desarrollo como especie se han visto ampliadas, por efecto de la tecnología, con una nueva dimensión específica: la del Ciberespacio" (ÁVILA, 2018).

De esta manera, la principal diferencia del ciberespacio respecto al entorno físico que conforman la tierra, el mar, el aire y el espacio es, precisamente, su *carácter virtual*, es decir, que es producto del desarrollo de capacidades tecnológicas propias del ser humano.

El ciberespacio, conforme lo define la Estrategia Nacional de Seguridad española de 2019[7], "es un espacio común global caracterizado por su apertura funcional y su

[6] Conclusión con la que se cierra el *Informe sobre la Aplicación de la Estrategia Europea de Seguridad: ofrecer seguridad en un mundo en evolución*, presentado por el Secretario General del Consejo de la UE/Alto Representante de la Política Exterior y de Seguridad Común, de 11 de diciembre de 2008. Disponible en: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/ES/reports/104637.pdf (20/04/2023).

[7] Orden PCI/487/2019, de 26 de abril, por la que se publica la *Estrategia Nacional de Ciberseguridad 2019*, aprobada por el Consejo de Seguridad Nacional. BOE núm. 103, de martes 30 de abril de 2019. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-6347 (20/04/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

dinamismo", por su flexibilidad digital, universalidad y velocidad. Frente a estas notas definitorias "la ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad"[8].

Entonces, ¿debemos entender que este *quinto dominio*, inédito hasta ahora, queda fuera del alcance del principio de soberanía, de forma que los Estados no pueden ejercer su autoridad en el ciberespacio, conviniendo así que se trata de un lugar independiente donde no son bienvenidos aquellos?

En este contexto, en el año 1996, John Perry Barlow[9] resuelve en su conocida Declaración que el ciberespacio es una *nueva creación independiente de la autoridad de los Estados*:

> "Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos"[10].

En esta línea de desafío a la soberanía del Estado debemos referimos a varias teorías y posturas ideológicas.

En primer lugar, la *teoría del excepcionalismo cibernético*, que parte del presupuesto de que el conglomerado de tecnologías que sostienen Internet y lo configuran como una red descentralizada, de complejas relaciones que superan el marco jurisdiccional de cualquier Estado, sin un cuerpo legislativo que pueda responder en tiempo oportuno a la velocidad de los cambios que comporta la innovación continua, y con la dificultad de atribución de responsabilidad consustancial a la anonimización que procura la red, hacen del ciberespacio un nuevo reino virtual y autónomo, independiente de la soberanía de los Estados, replicando así los postulados de Barlow. Este tipo de *teorías ciberlibertarias* quedan superadas por el volumen de crecimiento de Internet y su economización, cuestiones que avanzan acompañadas de todo tipo de conflictos de intereses entre particulares y empresas que, en conjunto, harán que aquellos *postulados libertarios* cedan ante la necesidad de la presencia estatal reguladora de la red para garantizar los derechos digitales de los usuarios, de forma que la intervención del Estado como tal se acepte y únicamente se discuta el grado de profundidad de la misma (ÁLVAREZ ROBLES, 2023, págs. 17-56).

---

[8] IBIDEM, Capítulo 1, página 17.

[9] El ciberactivista estadounidense John Perry Barlow presenta en Davos, el 8 de febrero de 1996, la *Declaración de Independencia del Ciberespacio*, como respuesta a la aprobación de la *Telecommunications Act* del Gobierno de los EE.UU., y sosteniendo que el ciberespacio es ajeno a la soberanía de los Estados y sus fronteras.

[10] *Declaración de independencia del ciberespacio* de John Perry Barlow, presentado en Davos el 8 de febrero de 1996. Disponible en: https://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf (26/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

En segundo lugar, debemos mencionar la *tesis de la gobernanza multiactor de Internet*, que pone en tela de juicio la necesidad de una autoridad central estatalizada que organice y decida cuestiones referidas al funcionamiento de la red, cuya administración debe corresponder en exclusiva a quienes operan en ella y donde el Estado desempeña distintos roles, en ningún caso vinculados a la soberanía (POHLE & THIEL, 2020, págs. 7-8).

La tercera de estas distintas consideraciones sobre la soberanía digital parte de su definición como "el *control* de nuestro presente y destino tal como se manifiesta y guía por el uso de la tecnología y las redes informáticas" (GUEHAM, 2017, pág. 3), para conectarla directamente con el control del *procesamiento de los datos* y el *dominio del lugar* donde se ubiquen las infraestructuras que los alojan. Esta línea de pensamiento entiende que, dado que el interés por la propiedad de los datos es compartido por los gobiernos, las empresas y los propios ciudadanos, es esencial para el Estado conseguir una soberanía digital fuerte frente a esos múltiples actores a través de herramientas como el desarrollo de un marco legal adecuado para la protección de datos, la implantación de infraestructuras informáticas seguras y accesibles, o el sostenimiento de una *cloud* soberana que consiga la autonomía tecnológica necesaria para proteger los datos de sus nacionales. Pero esta respuesta del Estado que, ante el conflicto de intereses por la posesión del dato, ejerce su autoridad para imponer la supervisión técnica y jurídica en el ciberespacio, fricciona con las aspiraciones de los otros grupos de poder, siendo interpretado como una confrontación al modelo de gobernanza de la Internet global, abierta y descentralizada y, por lo tanto, que enfrenta a la soberanía digital del Estado con la libertad en la red (GUEHAM, 2017, págs. 4-7).

En verdad el ciberespacio es un dominio de naturaleza *no física*, o al menos en la forma tradicional, altamente tecnificado, común y global, donde la propia personalidad de los que en él se relacionan puede enmascararse o, simplemente, anonimizarse, y en el que la capacidad de influencia de los actores no se mide por su fuerza o implantación territorial, sino por *likes* y el número de seguidores. Es por ello que todo parezca indicar que, en esta dimensión digital, la soberanía pierda parte de esos atributos que, hasta ahora, le habían conferido el carácter de medida de poder y fundamento del Estado como base de la vinculación jurídica entre personas y entidades, tanto públicas como privadas, que encuentran en el ecosistema digital nuevas formas de relacionarse entre sí al margen de las clásicas vías económicas, políticas o culturales comprendidas en el rígido marco westfaliano.

Otro reto añadido al que se enfrenta la soberanía es la cuestión geopolítica, referida a las tensiones y conflictos entre los Estados en su lucha por la supremacía mundial, con la inevitable influencia que sobre ella ejerce la geografía en sus dimensiones física, política y humana (BAQUÉS QUESADA & FOJÓN LAGOA, 2023, pág. 12). En el actual contexto internacional, de máxima pugna entre actores sistémicos por la supremacía tecnológica, el concepto de soberanía resurge porque los Estados no están dispuestos a asumir los riesgos derivados de una pérdida completa de autoridad en el nuevo dominio y, para ello, se enfrentan a las corrientes de pensamiento que cuestionan su jurisdicción en el ámbito digital.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Nuevamente nos surge la duda de si estamos ante la crisis definitiva de la soberanía o si, una vez más, será cuestión de flexibilizar el marco de referencia para adaptar su significado a la compleja realidad social, tecnológica, económica y geopolítica del siglo XXI.

Si bien unas líneas más arriba definimos el ciberespacio como un ecosistema digital y aterritorial, ahora debemos precisar que su naturaleza virtual no implica la inmaterialidad e ineludibilidad del mundo físico newtoniano, por cuanto los servicios prestados, las aplicaciones informáticas utilizadas, los efectos de las interacciones desempeñadas y los resultados de los contratos perfeccionados en el ciberespacio tienen detrás unas infraestructuras y dispositivos físicos de soporte que los posibilitan y, en alguna medida, los definen y limitan. Esta *perspectiva física* del mundo digital o *giro hardware* es defendido por algunos autores, como Luciano Floridi, para dar entrada en el ámbito del ciberespacio a cuestiones como la gobernanza, la soberanía y otras cuestiones éticas, legales y sociales que habían quedado eclipsadas por la propia dinámica de la transformación digital y que ahora, cuando el poder político se ha dado cuenta de la necesidad de controlar lo que ocurre en ese quinto dominio, toman carta de naturaleza por su sustancial relevancia:

> "The material infrastructure (to use an all-encompassing expression) is the *substratum* necessary for any digital connectivity and interaction, so its study is as old as the digital revolution itself. But today, the digital discourse finally focuses on the material aspects of its nature, scope, and development because of the need for countries and other organisations to own and control it (e.g. in terms of data flows and information usage), safeguarding against undue influence or manipulation by other actors, protecting their rights to self-determination and to govern their own infosphere, and gaining influence about the economic and financial aspects (including taxation) of digital markets […]. Although the hardware turn is a consequence of the emergence of digital sovereignty's need to own, control, regulate and patrol the infosphere, this does not mean that the immaterial perception of the digital revolution is mistaken" (FLORIDI, 2024, págs. 5-6) [11].

[11] "La infraestructura material (para usar una expresión que lo abarca todo) es el sustrato necesario para cualquier conectividad e interacción digital, por lo que su estudio es tan antiguo como la propia revolución digital. Pero hoy, el discurso digital finalmente se centra en los aspectos materiales de su naturaleza, alcance y desarrollo debido a la necesidad de los países y otras organizaciones para poseerlo y controlarlo (por ejemplo, en términos de flujos de datos y uso de la información), como salvaguarda contra la influencia o manipulación indebida por parte de otros actores, protegiendo sus derechos a la autodeterminación y a gobernar su propia infosfera y ganando influencia sobre los aspectos económicos y financieros (incluyendo la fiscalidad) de los mercados digitales… Aunque el giro del hardware es consecuencia de la irrupción de la necesidad de la soberanía digital de poseer, controlar, regular y patrullar la infosfera, esto no significa que la percepción inmaterial de la revolución digital sea errónea" (Traducción propia).
Sobre el término *infosfera*, éste hace referencia al entorno digital como espacio común en el que Internet con su información, la propia sociedad y la cultura evolucionan y se desarrollan de manera conjunta.
Disponible en: https://infosfera.com.ar/la_infosfera.asp
https://www.bbc.com/mundo/noticias/2014/11/141128_infosfera_filosofia_tecnologia_finde_dv
(22/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

A partir de esta premisa podemos ya referirnos a la *soberanía digital* como la capacidad de un Estado para ejercer el control sobre su propio espacio digital, lo cual supone una multiplicidad de aspectos políticos y sociales, entre otros, que se interconectan a través de un orden de relaciones sustentadas por dos de los principales atributos de la soberanía:

1. El reconocimiento de la autoridad –local, estatal, supranacional, internacional-.
2. Y el funcionamiento de mecanismos de control –normativa, políticas públicas, sistema regulado de sanciones- (ÁLVAREZ ROBLES, 2024).

En este sentido, conforme a lo defendido por el Grupo de Expertos de Tallinn, el principio de soberanía interior de los Estados aplica en el ciberespacio, de manera que estos despliegan su plena autoridad sobre las infraestructuras de soporte localizadas en su territorio, así como sobre las personas y las actividades a ellas asociadas (SCHMITT, 2017, pp. 13-16).

De esta manera, la suprema autoridad de cada Estado en su territorio incluye las capas física, lógica y social del ciberespacio[12], por lo cual el *quinto dominio* queda englobado en el principio de soberanía, tanto en su dimensión interna como externa, e igualmente sujeto al Derecho Internacional respecto a las violaciones de dicha soberanía por parte de acciones ofensivas como las ciberoperaciones, la práctica de acciones de ciberespionaje o las operaciones de influencia a través de la difusión de propaganda, entre otras.

Diferente cuestión es la distinta *opinio iuris* que los Estados democráticos y los autocráticos defienden sobre cómo aplicar el Derecho Internacional en el ciberespacio, condicionados por su propia forma de entender este espacio común global y su integración con la sociedad. Así, mientras que para los primeros las normas existentes son suficientes para resolver los nuevos retos y conflictos en el *quinto dominio*, para los segundos la ambigüedad del entorno les lleva a pedir tratados y acuerdos específicos para rellenar las *lagunas legales* que consideran que existen (B.M.J. PIJPERS, 2024, pág. 14). Actualmente la que predomina es la perspectiva democrática del ciberespacio pero, en todo caso:

> "The legal differences between authoritarian and Western states on the application of international law to cyberspace should not be exaggerated […]. Both authoritarian and Western states leverage international law to legitimise their perspectives on cyberspace. The call for or warning against new international conventions on cyberspace serve as a strategic instrument in this regard" (B.M.J. PIJPERS, 2024, pág. 18) [13].

[12] Según el *Manual Tallinn 2.0*, la capa física la componen el hardware, la infraestructura de red, los servidores y resto de elementos de soporte material para las comunicaciones en la red. La capa lógica hace referencia a la conexión entre los dispositivos, las aplicaciones y los protocolos de intercambio de datos. Finalmente, la capa social la componen los grupos de personas e individuos que operan y se relacionan en el ciberespacio.

[13] "No hay que exagerar las diferencias jurídicas entre los Estados autoritarios y los Occidentales sobre la aplicación del Derecho Internacional al ciberespacio […]. Tanto los Estados autoritarios como los Occidentales aprovechan el Derecho Internacional para legitimar sus perspectivas sobre el ciberespacio.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Desde una posición geoestratégica opuesta a la occidental y con una visión propia de la soberanía digital, Rusia parece estar dando pasos hacia la consolidación de un *segmento nacional de Internet* autónomo[14], con el objetivo de garantizarse la protección contra posibles amenazas provenientes del ciberespacio. Acorde con este planteamiento:

> "Digital sovereignty (*tsifrovoi suverenitet*) is in this context used primarily as a political term, and can be understood as the right and capability of a government to determine its fate within its own information space. Russian information technology expert, Igor Ashmanov, divides digital sovereignty in two: electronic sovereignty, which encompasses robust Internet infrastructure protected from malware and malicious cyber actors; and information sovereignty, the self-sufficient control of information and resistance to information attacks. Thus, the ideal state of affairs would consist of autonomous hard- and software, Internet infrastructure, subordinated mass media, a unifying ideology, and a strong legal system"[15].

Pero también ha ayudado a considerar la necesidad de impulsar la soberanía digital como elemento integrador de la Red, el poder que han acumulado algunos de los *stakeholders* que operan en ella, principalmente referidos a empresas propietarias de tecnologías innovadoras y modelos de negocio exitosos, los cuales ofrecen sus servicios en Internet bajo el paradigma de la personalización *ad hoc* conforme a las necesidades del cliente a cambio de sus datos. Y aquí radica la clave: al igual que la sociedad industrial se construyó en torno a la *producción* -dónde están y a quién pertenecen las fábricas- la sociedad del ciberespacio se está construyendo en torno al *dato* -dónde están y a quién pertenecen los datos-.

La pugna por el control de los datos ha sido un elemento esencial para la reivindicación en Europa de la soberanía digital y, a la vez, la llamada de atención sobre dos de sus principales atributos: la *autonomía tecnológica* y la *autonomía estratégica*. Es a partir de las declaraciones que realiza Edward Snowden en 2013, sobre el alcance del sistema de vigilancia masiva que la Agencia Nacional de Seguridad (NSA) estadounidense llevó a cabo durante años sobre los datos privados de millones de personas provenientes de

---

El llamamiento o la advertencia contra la creación de nuevos acuerdos internacionales sobre el ciberespacio constituyen un instrumento estratégico a este respecto" (Traducción propia).

[14] En octubre de 2019, entró en vigor la ley *Internet soberana de Rusia*, que permite al gobierno desconectarse de la Internet global a su discreción. Con este fin, el Kremlin pretende que para el 2024 sólo el 10% del tráfico de Internet ruso se enrute a través de servidores extranjeros.

Russia´s Strategy in Cyberspace. NATO Strategic Communications Centre of Excellence & NATO Cooperative Cyber Defence Centre of Excellence. June 2021. Página 12. Disponible en: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf (05/03/2024).

[15] IBIDEM, página 12.

"La soberanía digital (*tsifrovoi suverenitet*) se utiliza en este contexto principalmente como un término político y puede entenderse como el derecho y la capacidad de un gobierno de determinar su destino dentro de su propio espacio de información. El experto ruso en tecnologías de la información, Igor Ashmanov, divide la soberanía digital en dos: soberanía electrónica, que abarca una infraestructura robusta de Internet, protegida contra malware y ciberataques maliciosos; y la soberanía de la información, como el control autosuficiente de la información y la resistencia a los ataques de información. Por lo tanto, la situación ideal consistiría en hardware y software autónomos, infraestructura de Internet, medios de comunicación subordinados, una ideología unificadora y un sistema legal fuerte" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

distintas plataformas de Internet y compañías de telecomunicaciones[16], cuando la Unión Europea se comienza a preocupar por el abuso de posición dominante de EE.UU. a través de sus grandes empresas tecnológicas y, al mismo tiempo, toma conciencia de su alto nivel de dependencia digital y de que tiene que recuperar el control de sus datos si quiere alcanzar el lugar que pretende en el escenario internacional como espacio soberano y proveedor de seguridad.

En este contexto de pérdida de confianza desde la costa oriental del Atlántico, el Parlamento Europeo pivota entre, por un lado, mantener la necesaria cooperación con EE.UU. en la lucha contraterrorista[17] y, por otro, su preocupación por el espionaje a gran escala de la NSA[18], que supuso a todas vistas una grave violación de la privacidad y la protección de datos personales de los europeos, llegando así a requerir explícitamente a EE.UU.:

> "[…] que revisen sin demora su legislación para adecuarla al Derecho Internacional, reconozcan el derecho a la intimidad y otros derechos de los ciudadanos de la UE, proporcionen vías de recurso jurisdiccional para los ciudadanos de la UE, pongan los derechos de los ciudadanos de la UE en el mismo plano que los derechos de los ciudadanos de los EE.UU. y suscriban el Protocolo Opcional que permite las denuncias individuales en virtud del PIDCP"[19].

En línea con lo anterior, el Parlamento Europeo suspende el *Acuerdo SWIFT* relativo al intercambio de datos entre la UE y los EE.UU. en la lucha contra la financiación del

[16] En junio de 2013 Edward Snowden, que trabajó para la NSA, desvela que el Gobierno de EE.UU. autorizó un programa de espionaje masivo sobre las comunicaciones de millones de personas de todo el mundo bajo el pretexto de combatir al terrorismo internacional, a través del acceso de la NSA y otras agencias estadounidenses a los servidores de compañías como Microsoft, Google o Yahoo, entre otras. A partir de ese momento el cifrado de las comunicaciones se convirtió en un mínimo imprescindible para operar con garantías de privacidad en la Red. Disponible en: https://cnnespanol.cnn.com/2013/06/10/quien-es-edward-snowden-el-hombre-que-filtro-datos-secretos-de-la-nsa/ https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/ https://www.washingtonpost.com/magazine/2020/05/11/2013-edward-snowden-leaked-top-secret-national-security-agency-documents-showing-how-us-was-spying-its-citizens-heres-what-happened-next/ (07/02/2024).

[17] Como por ejemplo el *Programa de Seguimiento de la Financiación del Terrorismo*, conforme al Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo**.** 22010A0727(01). Diario Oficial n° L 195 de 27/07/2010 p. 5 – 14. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A22010A0727%2801%29 (28/02/2024):

[18] Esta inquietud determinó que el Parlamento Europeo impulsara una Resolución para investigar los hechos y sacar conclusiones con las que tomar medidas, titulada Programa de vigilancia de la ANS de los EE.UU., servicios de inteligencia en varios Estados miembros e impacto en la privacidad de los ciudadanos de la UE. Resolución del Parlamento Europeo, de 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE (2013/2682(RSP)) (2016/C 075/14). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013IP0322&from=MT (28/02/2024).

[19] Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior. 2013/2188(INI). Recomendación 31. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52014IP0230 (28/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

terrorismo y solicita la investigación técnica de los hechos denunciados, estimando que las medidas de seguridad aplicables a cualquier tipo de amenaza deben implementarse en el marco de los valores fundamentales de la UE, delimitado por el respeto del Estado de Derecho y la garantía de los derechos fundamentales, incluidos los relativos a la privacidad y la protección de datos de sus ciudadanos[20].

De esta manera se forjan los cimientos de la Estrategia de Ciberseguridad de la Unión, superando la hasta entonces constreñida perspectiva nacional en pro de un enfoque europeo amplio y conjunto, participativo y centrado en la seguridad humana, con especial atención a la injerencia extranjera. Al mismo tiempo, se llevaron a cabo acciones para recuperar el control de las infraestructuras físicas críticas y de soporte de los datos de la UE:

> "[…] a nivel tecnológico y económico, se evidenció una nueva producción de redes informáticas vinculadas a los servicios de comercio y de almacenamiento de información reservados para la zona europea. Esta iniciativa de respuesta se produjo también a través de la creación e implementación de aplicaciones y sistemas informáticos alternos, así como con la relocalización de servidores digitales destinados a servicios de comercio e infraestructuras críticas" (CRESPO-PAZMIÑO, 2020, págs. 91-92).

Posteriormente, este compromiso con la idea de crear una Europa apta para la Era Digital se recoge por la Comisión Europea, entre otros, en su documento *Configurar el futuro digital de Europa*, donde expresamente manifiesta que:

> "Para el desarrollo de muchos productos y servicios, es necesario que los datos estén ampliamente disponibles y sean de fácil acceso, utilización y tratamiento. Los datos se han convertido en un factor clave de la producción, y el valor que crean tiene que ser compartido con toda la sociedad que contribuye a facilitarlos. Esta es la razón por la que necesitamos construir un verdadero mercado único europeo de datos: un espacio europeo de datos basado en normas y valores europeos"[21].

Es así que la *autonomía tecnológica* y la *autonomía estratégica* se convierten en prioridades para la Unión con el objetivo de alcanzar un control exclusivo sobre las comunicaciones y los datos de sus ciudadanos, a través de un conjunto normativo propio que regule, entre otras cuestiones, el ciberespacio y las relaciones de alto contenido transnacional que en él se desenvuelven. Vemos con ello como se aúnan las dos consideraciones de soberanía de los siglos XX y XXI, relacionadas con la

[20] Suspensión del acuerdo SWIFT como resultado de la vigilancia de la Agencia Nacional de Seguridad de los EE.UU. P7_TA(2013)0449. Resolución del Parlamento Europeo, de 23 de octubre de 2013, sobre la suspensión del Acuerdo TFTP a raíz de la vigilancia de la NSA (2013/2831(RSP)). (2016/C 208/14). Considerando 1, página 156. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52013IP0449 (28/02/2024).

[21] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Configurar el futuro digital de Europa*. Página 7. Bruselas, 19.2.2020. COM (2020) 67 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0067 (28/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

supranacionalidad -cesión de soberanía e integración en la UE- y la virtualización de las relaciones -soberanía digital-.

Este ejercicio *de facto* de la soberanía digital no hace sino dar forma a la gobernanza en Internet para tratar de equilibrar los intereses de los tres principales grupos de actores que comparten la esfera digital: los *Estados* que defienden su soberanía en ese nuevo dominio, las *grandes empresas y compañías* que reclaman sus beneficios económicos en una red abierta y de libre competencia, y los *ciudadanos* que requieren la protección de sus derechos de privacidad y libertad de expresión en un ciberespacio que les ofrezca confiabilidad y seguridad (GUEHAM, 2017, págs. 4-9).

La acción de conjugar estos intereses hace que el propio concepto de *soberanía digital* se adapte a la realidad de una sociedad hiperconectada y altamente dependiente de la tecnología que, en el ejercicio de sus valores liberales y democráticos, le pide al Estado no solo la protección de sus derechos y el control regulador de las grandes empresas en la red sino, también, que le haga partícipe de su autoridad en el ciberespacio, puesto que:

> "[…] la soberanía digital no es un fin en sí mismo. Por el contrario, para lograr una verdadera democratización de la soberanía digital, debemos reflexionar aún más sobre el marco procedimental que permite que el poder soberano rinda cuentas y se abra a la reflexión y el control públicos" (POHLE & THIEL, 2020, pág. 18).

De esta forma podemos concluir que, pese a las innovadoras y cambiantes formas de las oportunidades y amenazas asociadas al ciberespacio como lugar virtual global, común, abierto y descentralizado que exige una superación de la clásica concepción westfaliana de la soberanía del Estado, en su nueva faceta digital ésta sigue representando un principio fundamental del Derecho Internacional con plena vigencia para alcanzar dos objetivos:

1. Por un lado, articular exitosamente el modelo de gobernanza que permita el equilibrio de intereses legítimos de los principales actores involucrados, pero con la lógica prevalencia del bien público sobre cualquier otro de carácter particular, y también del interés general para defender los derechos humanos y libertades fundamentales.
2. Y por otro, redefinir las alianzas en el escenario geopolítico mundial para gestionar de manera compartida y segura los datos en un ciberespacio confiable que, a su manera, no deja de tener un componente físico o material.

1.2. La organización de la seguridad como faceta de la soberanía

El Estado agrario de estructura feudal era débil de cara al exterior e inestable internamente frente a nobles y facciones, que en un momento determinado podían unirse con el enemigo para alcanzar mayores cotas de poder propio. Las guerras contra otros Estados servían así para distraer la ambición de los nobles que, con exiguos ejércitos mercenarios reclutados para la contienda, se batían en condiciones muy igualadas que, raramente, conseguían triunfos rápidos y decisivos que aclarasen el contexto político, por lo que el conflicto se enquistaba haciendo muy complicado

Ediciones Universidad de Salamanca | CC BY-NC-ND

diferenciar estrictamente entre la guerra y la paz, que se fundían íntimamente en una línea temporal continua convirtiendo en precaria la seguridad media de la población. En este sentido, Meinecke señala que:

> "El confuso entrecruzamiento de guerra y paz, consecuencia de los escasos medios de poder por parte de los Estados, explica la escasa validez que se atribuía a las obligaciones internacionales" (MEINECKE, 2014, págs. 423-425).

La madurez del Estado absoluto trae consigo la desaparición de los enfrentamientos feudales con el rey, el asentamiento de la economía mercantilista y la recaudación de impuestos que va a permitir el fortalecimiento de las estructuras de poder con la fundación de ejércitos profesionales y permanentes. A partir de este momento los habitantes de un territorio distinguen claramente las situaciones de paz y de guerra, que dejan de ser una situación combinada o mixta. Al mismo tiempo, aumentan las medidas de policía en el ámbito de la soberanía estatal y, como consecuencia, aumenta la seguridad de la población (MEINECKE, 2014, págs. 423-425). En el ámbito de las relaciones entre Estados, el nuevo contexto hace que estos se reconozcan como iguales y que se respeten en la paz, aunque la guerra es considerada instrumento que acompaña a la política para la resolución de conflictos.

Depurar conceptos tan utilizados a lo largo de la historia y transversales al desarrollo de las relaciones humanas no es tarea fácil, por lo que el estudioso de la materia puede encontrar tantas definiciones de *seguridad* como visiones aplicadas al caso concreto y al marco temporal que le corresponda. No sólo es la dificultad de acordar un concepto ajustado y certero que describa lo que para una sociedad y sus ciudadanos representa la seguridad, sino que, además, "el concepto de seguridad es complejo, difuso y con muchas vertientes" (ANGUITA OSUNA, 2021, pág. 17).

La Real Academia Española define *seguro* como lo que está libre de peligro o riesgo, y *seguridad* como la sensación de total confianza que se tiene en algo o alguien. Tal definición muestra que la seguridad tiene un componente objetivo, respecto a la amenaza, y otro subjetivo, referido a la percepción personal de la posibilidad de materializarse la misma. De esta manera, tanto el crimen como la consiguiente sensación de miedo, son factores que conforman la realidad social en cuanto que generan cambios conductuales en los individuos, cambios que indefectiblemente tienen un reflejo en lo que se percibe y se entiende como seguridad. Consecuentemente, cabe entender la seguridad no tanto como la ausencia de delitos sino como la ausencia del riesgo de sufrirlos (RAMÍREZ, 2005, pág. 28).

Respecto a la *Seguridad Nacional*, tradicionalmente se ha entendido a través del paradigma realista para el que la política mundial es una permanente lucha por el poder entre naciones en la defensa de sus intereses, donde el Estado constituye el núcleo referente de la seguridad asumiendo la responsabilidad de proteger a sus ciudadanos a cambio de su lealtad, de manera que la seguridad de éstos queda garantizada a través de la propia seguridad de aquel (LABORIE IGLESIAS M. , 2011, pág. 1). Con la evolución de los tiempos este concepto se va ampliando para afrontar un abanico mayor de riesgos y amenazas, de forma que la última Estrategia española publicada en el año 2021, presenta una *visión integral* de la Seguridad Nacional entendida como "la acción del

Ediciones Universidad de Salamanca | CC BY-NC-ND

Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos"[22].

Como señalábamos, la doctrina no es pacífica a la hora de acotar este concepto que, por su naturaleza, adquiere una dimensión cambiante en atención a las variables multidimensionales que le afectan y que, desde comienzos del siglo XXI, no han hecho sino evolucionar dentro de un escenario global, altamente tecnificado y profundamente condicionado por los intereses económico-industriales que contribuyen a aumentar aún más si cabe la demanda de seguridad.

Es así como se ha ido dando cuerpo a conceptos como el de *seguridad humana*, que pone el acento en el desarrollo sostenible a través de su vinculación con el respeto a los derechos humanos y libertades fundamentales de la persona (MARTÍNEZ QUINTEIRO, 2018, págs. 35-70), el de *seguridad integral*, que implica una visión amplia de la seguridad a través del equilibrio entre sus dimensiones políticas, económicas, socioculturales y medioambientales (BALLESTEROS MARTÍN M. A., 2016, pág. 106), el de *seguridad cooperativa*, que defiende la construcción de relaciones internacionales basadas en la confianza y la inclusión, junto a los Estados, de actores no estatales y organizaciones internacionales en el grupo decisor de cualquier negociación que pretenda una solución estable en el tablero de juego internacional, o el de *seguridad sostenible*, que propone un enfoque aglutinador de las perspectivas nacional, humana y colectiva de la seguridad, coordinando de esta forma las tres líneas de acción exterior: la defensa, la diplomacia y el desarrollo (LABORIE IGLESIAS M. , 2011, págs. 1-9), cuestión que denota la conexión de la seguridad -en cualquiera de sus formas- con la soberanía por cuanto ambos conceptos se adjetivan en función del bien jurídico a proteger.

1.2.1. La seguridad como principio básico de la vida social organizada

El desarrollo conceptual de la seguridad evoluciona históricamente a la par que el de soberanía, como hermanos que crecen parejos y se necesitan el uno al otro para justificarse frente a la comunidad. Inicialmente la seguridad se identifica con la paz social dentro de las fronteras, cuestión que ya estipula la curia regia de León en 1188 en sus *Decreta*, donde don Alfonso IX, rey de León y de Galicia, establece y confirma "bajo juramento que a todos los de mi reino, tanto clérigos como laicos, les respetaría las buenas costumbres que tienen establecidas por mis antecesores"[23], y que habrán también de solicitar las Cortes de Valladolid de 1440 al rey Juan II "recordándole que su

[22] *Estrategia de Seguridad Nacional 2021: Un proyecto compartido*. Disponible en: https://www.dsn.gob.es/index.php/es/es/actualidad/sala-prensa/estrategia-seguridad-nacional-2021 (14/05/2023).

[23] Versión de José M.ª FERNÁNDEZ CATÓN: *La curia regia de León de 1188 y sus "Decreta" y constitución*. León: Centro de Estudios e Investigación "San Isidoro" – Archivo Histórico Diocesano, 1993; pp. 93-117. Realizada a partir del texto latino fijado del contraste de las versiones contenidas en las copias del siglo XVI de los códices de la Biblioteca Nacional de España, Mss. 12909, fols. 307v-310v; Mss. 772, fols. 305r-308r; y Biblioteca capitular de Sevilla, Sign. 56-2-20, fols. 189v-192r. Disponible en: https://www.cultura.gob.es/dam/jcr:5e01f9da-8205-47ee-8053-2c3a68e198ef/decreta-leon-version-espanola.pdf (14/05/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

primer deber es acallar las disensiones interiores" (MARAVALL CASESNOVES, 1986, pág. 216) ante la situación de inestabilidad que vive la Corona de Castilla, donde los tumultos y los enfrentamientos intestinos son la principal amenaza a la tranquilidad de los súbditos y, además, lastran el comercio entre las ciudades. Es así como la paz en el interior del territorio, que se traduce en seguridad y se vincula con la propiedad, se convierte en el primer y más obligado fin de todo buen príncipe, lo que llevará a "que sea en España donde se inicie en gran parte el régimen de Estado moderno, en cuanto organización garantizadora de la paz social interna" (MARAVALL CASESNOVES, 1986, pág. 216), tan necesaria para la apetencia burguesa de seguridad que le permita el comercio, el cultivo de los campos y, en definitiva, la tranquilidad de su vida cotidiana.

Posteriormente, será el desarrollo de la economía y el modo de vida de la burguesía los aspectos sociales que apuntalarán, aún más, la dedicación del poder soberano y sus estructuras a garantizar la protección humana ante los peligros provenientes tanto de los hombres como de la propia Naturaleza –seguridad física–, así como de la propiedad y beneficios derivados de su comercio –seguridad material-, aún a costa de la renuncia voluntaria a los derechos naturales que todo hombre posee según la teoría política hobbesiana. Es la manera en que el Estado absolutista legitima su poder frente al ciudadano, que necesita la garantía de una situación de paz y estabilidad para su desarrollo, siendo cierto que en la guerra:

> "[…] no existe oportunidad para la industria, ya que su fruto es incierto; por consiguiente no hay cultivo de la tierra, ni navegación, ni uso de los artículos que pueden ser importados por mar, ni construcciones confortables, ni instrumentos para mover y remover las cosas que requieren mucha fuerza, ni conocimiento de la faz de la tierra, ni cómputo del tempo, ni arte, ni letras, ni sociedad; y, lo que es peor de todo, existe continuo temor y peligro de muerte violenta; y la vida del hombre es solitaria, pobre, tosca, embrutecida y breve" (HOBBES, 2013, págs. 167-168).

De esta manera, son las propias dinámicas sociales las que llevan a las monarquías absolutas europeas del siglo XVIII a adaptarse a las nuevas demandas que se plantean y, con ello, a:

> "[…] tomar decisiones encaminadas, primero, a la articulación de una herramienta de control del orden público y, en segundo lugar, encaminadas al proceso de institucionalización de la policía como organización del Estado. Sin duda, la necesidad de un cuerpo policial emerge de la propia sociedad, y será la sociedad quien -históricamente hablando- determine y pergeñe la función policial, a demanda, pues la evolución de la vida en el mundo urbano fue determinando las competencias que se asignaban a la policía, ampliando la envergadura de su orgánica progresivamente" (HERRERO FERNÁNDEZ-QUESADA & TURRADO VIDAL, 2023, págs. 15-16).

Es en este momento histórico, en el tránsito del siglo XVII al XIX, cuando el equilibrio entre la libertad individual y la seguridad ya se comienza a apreciar en documentos como la *Declaración de Derechos de Virginia* de junio de 1776, donde los representantes del pueblo establecen como norma la igualdad natural de todos los hombres y el derecho irrenunciable a la vida, a la libertad, a la propiedad y a la búsqueda de la

Ediciones Universidad de Salamanca | CC BY-NC-ND

"felicidad y la seguridad"[24], para continuar fijando que "el gobierno es instituido, o debería serlo, para el común provecho, protección y seguridad del pueblo, nación o comunidad", siendo la mejor forma de gobierno aquella que produzca el más alto grado de felicidad y seguridad, de forma que cuando un gobierno resulte inadecuado o contrario a estos principios tenga la comunidad el "derecho indiscutible, inalienable e irrevocable" de cambiarlo conforme a lo que se estime conveniente para el bien público[25]. Resulta interesante el hecho de que se refieran los ilustrados constituyentes americanos a la *felicidad individual de los ciudadanos* cuando este término, como señalan algunos autores como Maravall Casesnoves, deriva de la escolástica renacentista que entiende la felicidad como el *bonum commune*, que encadena los bienes del alma, del cuerpo y los de la fortuna que la nación comparte con cada uno de sus habitantes, a la vez que proclaman el derecho a la seguridad del pueblo como colectivo, anticipando lo que hoy definimos como seguridad nacional (MARAVALL CASESNOVES, 1986, pág. 212).

Avanzando en el tiempo e inspirada en la anterior, la Asamblea Nacional francesa aprueba el 26 de agosto de 1789 la *Declaración de los derechos del hombre y del ciudadano*, que vuelve a referirse en su preámbulo a la *felicidad de todos* como objetivo de la acción del gobierno, a la vez que declara como finalidad última de toda forma de sociedad la protección de los "derechos naturales e imprescriptibles del hombre", cuales son la libertad, la propiedad, la seguridad y la resistencia a la opresión[26].

Por lo tanto, la felicidad es la esencia de la convivencia en paz y comprende la seguridad de las personas y los bienes, como reflejan los textos constitucionales de la época que consagran la protección de los derechos humanos. De esta forma, en la segunda mitad del siglo XVIII se va configurando la seguridad como derecho de los ciudadanos en cuanto personas libres e iguales y, en paralelo, la responsabilidad de preservarla por parte del Estado como entidad única, soberana e independiente.

Conforme a lo anterior, podemos decir que la seguridad tiene tres componentes que la definen. En primer lugar, es un bien público, en cuanto beneficio colectivo "íntimamente ligado a la calidad de vida y al nivel de bienestar económico, político y social de una comunidad" (MOLOEZNIK GRUER, 2019, pág. 149). En segundo lugar, por lo que representa de beneficio individual, la seguridad es un derecho básico "del que todos los habitantes deben gozar por el solo hecho de ser persona humana, a partir de definir como seguro a lo que esté libre y exento de todo peligro, daño o riesgo" (MOLOEZNIK

[24] El artículo I de la *Declaración de Derechos de Virginia* del 12 de junio de 1776 establece "Que todos los hombres son por naturaleza igualmente libres e independientes y tienen ciertos derechos innatos, de los que, cuando entran en estado de sociedad, no pueden privar o desposeer a su posteridad por ningún pacto, a saber: el goce de la vida y de la libertad, con los medios de adquirir y poseer la propiedad y de buscar y obtener la felicidad y la seguridad". Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2698/21.pdf (16/05/2023).

[25] IBIDEM, artículo III.

[26] El artículo 2 de la *Declaración de los Derechos del Hombre y del Ciudadano* establece que "La finalidad de cualquier asociación política es la protección de los derechos naturales e imprescriptibles del Hombre. Tales derechos son la libertad, la propiedad, la seguridad y la resistencia a la opresión". Disponible en: https://www.conseil-constitutionnel.fr/sites/default/files/2019-02/20190225_derechosdelhombre_1789_0.pdf (16/05/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

GRUER, 2019, pág. 149). Y, en tercer lugar, la seguridad se convierte en una responsabilidad del Estado, por el componente de reto que supone para el gobierno dar respuesta a los cada vez mayores requerimientos de protección de los ciudadanos (ESTRADA RODRÍGUEZ, 2013, pág. 368).

Y es aquí, en este contexto en el que el Estado se constituye garante de la paz social y, como tal, está legitimado para controlar el orden público, donde la seguridad se vincula con la *policía*, que en su origen griego *politeia* ya se refería al buen gobierno de la *polis*, la ciudad, así como a la urbanidad, el aseo y la limpieza de la misma. En este sentido, Ramón Lázaro de Dou y Bassols, reformador catalán moderado que fue elegido primer presidente de las Cortes de Cádiz en 1810, apunta a una doble distinción del referido término en el Capítulo XIII de sus *Instituciones de Derecho Público General de España con noticia del Particular de Cataluña*, *y de las principales reglas de gobierno en cualquier Estado* (1800), dedicando su Sección I a la función propiamente material de la policía, de seguridad pública, haciendo especial hincapié en la labor preventiva que evite el delito así como su necesaria adaptación a las particulares circunstancias del entorno en que se desarrolle, y recogiendo en la Sección II lo concerniente a la salud y vida de los ciudadanos[27]. Son estas dos cuestiones adelantadas a su tiempo, por cuanto el autor se refiere a dos términos esenciales en la función policial moderna: la gestión anticipativa y la adaptación a la realidad de la amenaza que debe afrontar.

De esta forma, la actividad administrativa y los fines para los que se desempeña se van asimilando a los propios del Estado para atender las necesidades públicas, consideradas como "todo deseo o interés de un extenso grupo social que es imprescindible satisfacer" (JORDANA DE POZAS, 1951, pág. 15), y que se articulan a través de tres tipos de acciones: las de *policía*, las de *fomento* y las de *servicio público*. En este contexto temporal de mediados del pasado siglo, la actividad de *policía* como modo directo de garantizar el orden público se liga a la prevención y, llegado el caso, a la represión para restituir mediante la fuerza legítima la seguridad subvertida. Al contrario, la acción de *fomento* abriga y promueve el logro de la utilidad general de manera indirecta, a través del estímulo de los particulares que, por sus propios medios y conforme al más puro talante liberal, habrán de actuar por propio convencimiento. Finalmente, el *servicio público* queda como el paradigma del modo de acción directo para lograr las finalidades propias del Estado, que en conjunto definen los niveles mínimos de bienestar establecidos por ley y tutelados por la administración (JORDANA DE POZAS, 1949, págs. 41-54).

[27] El autor, en el Capítulo XIII titulado De la policía, Sección I De las cosas generalmente útiles ó necesarias para la policía, punto 8 De las cosas pertenecientes á policía en general, literalmente señala: "Entro ya á hablar de la seguridad pública para proteger y defender en quanto se pueda con medios preventivos el sosiego, la vida, la salud, los bienes, y la comodidad de los particulares, ya sea dentro ya fuera de las poblaciones, empezando por las últimas.[…] No tanto entiendo, quando se trata de policía, la indicada seguridad como las medidas que la facilitan. El castigar á un ladron y obligarle á restituir lo que ha hurtado es propio de la justicia: el precaver que no se hurte con el alumbrado, rondas y otras providencias lo es de la policía".
Posteriormente, en el punto 18 *Medios para impedir y contener los tumultos* establece que "En todos tiempos y especialmente en los de disensiones y alborotos es menester suma vigilancia y solicitud, usándose de todos los medios, que dicte la prudencia, acomodados á las circunstancias del tiempo, lugar y personas, para impedir, que nazca la sedición, ó para contenerla después de empezada". Disponible en: https://bvpb.mcu.es/es/consulta/registro.cmd?id=403995 (18/05/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Será por ello que el liberalismo contemporáneo asuma la extrapolación de la seguridad al ámbito territorial del Estado, hasta entonces constreñida por el Antiguo Régimen a los límites de la ciudad, y con ello identifique a la policía, institución administrativa, con la *defensa del orden público* propio de un poder político democrático organizado en torno a la defensa de los derechos humanos y las libertades políticas, sociales y económicas que lo sustentan, donde la seguridad ocupa un lugar destacado como principio estructurador de la vida moderna.

1.2.2. La seguridad como monopolio incontestable del Estado

Ya en la antigüedad, pensadores de la talla de Platón y Cicerón debatieron sobre el aspecto diferenciador de la comunidad política de gobierno, considerando que este elemento no podía ser otro que la *justicia* por cuanto hacia coincidir la comunidad de intereses con la ley. Posteriormente otros, como Agustín (años 354-430), rechazan este planteamiento basándose en que la organización de la sociedad humana no puede ser absolutamente justa, pues dicha cualidad únicamente se consiente en el marco teológico (KLEY, 2010, pág. 223).

Con la caída el imperio romano y el advenimiento de la época feudal se fragmenta el poder político en toda Europa sobre la base del control de la tierra y la población que la ocupa. La Edad Media es particularmente violenta y solo los señores feudales, en el marco de su dominio y de la relación de vasallaje, pueden garantizar una frágil seguridad a los que trabajan sus tierras a cambio de algunos tributos, obediencia y lealtad. En esta sociedad medieval prácticamente no existe estructura institucional por lo que la distinción entre lo público y lo privado es prácticamente inexistente. Habrá que esperar a la consolidación del comercio y su intrincada estructura de relaciones económicas para que, al albor de la nueva clase social burguesa, vayan estableciéndose las bases de una nueva forma de organización política que Maquiavelo, a comienzos del siglo XVI, ya denomina Estado y para el que:

> "[…] un príncipe no debe tener otro objetivo ni otra preocupación, ni debe considerar como suya otra misión que la de la guerra, su organización y su disciplina. Porque esa es la única misión que compete a quien gobierna, y su importancia es tal que no sólo mantiene en el poder a los que han nacido príncipes, sino que muchas veces hace que alcancen ese grado hombres de privada condición; también se observa, por el contrario, que los príncipes que se han preocupado más de las comodidades que de las armas han perdido su estado" (MAQUIAVELO, 1994, pág. 105).

La seguridad, por ahora, tiene un enfoque exclusivo hacia la defensa del territorio y la unidad frente a las amenazas exteriores, para lo cual se confía en el ejército, sea "propio o mercenario, auxiliar o mixto" (MAQUIAVELO, 1994, pág. 91)

Más de un siglo después, en el *Leviathan*, Hobbes presenta su teoría del Estado como estructura pactada de poder dirigida a proteger y defender al ciudadano, con base en el contrato social y la imposición de la obediencia a las leyes para, así, mantener a los hombres en una situación de paz y justicia que evite su tendencia natural a la violencia.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Solo en este contexto puede prosperar la expectativa del disfrute de la libertad y la propiedad, bienes supremos que el régimen absolutista de la época se encarga de vincular al soberano y su estructura de gobierno que, a cambio de la legitimidad de su poder, deben garantizarlos para librar al hombre del continuo riesgo de muerte violenta, consagración explícita del monopolio soberano del uso de la violencia y, consecuentemente, de la prohibición a los súbditos del uso privado de la misma. De esta forma:

> "[…] en virtud de esta autoridad que se confiere por cada hombre particular el Estado posee y utiliza tanto poder y fortaleza que por el terror que inspira es capaz de conformar las voluntades de todos ellos para la paz en su propio país, y para la mutua ayuda contra sus enemigos, en el extranjero. Y en ello consiste la esencia del Estado, que podemos definir así: una persona de cuyos actos una gran multitud, por pactos mutuos realizados entre sí, ha sido instituida por cada uno como autor, al objeto de que pueda utilizar la fortaleza y medios de todos como lo juzgue oportuno para asegurar la paz y defensa común. El titular de esta persona se denomina soberano, y se dice que tiene poder soberano; cada uno de los que lo rodean es súbdito suyo" (HOBBES, 2013, pág. 193).

Continuando con el desarrollo de esta premisa, la firma de la Paz de Westfalia en 1648, referente de la conceptualización del Estado moderno, institucionaliza el monopolio estatal de la fuerza y el legítimo recurso a la guerra como forma de solución de conflictos entre Estados, marcando la línea de pensamiento que, a partir de entonces y desde una perspectiva instrumental, entiende la seguridad como respuesta coercitiva y exclusiva del Estado ante cualquier amenaza en el ámbito exterior y, por extensión, también para la preservación del orden interior, que proscribe el ejercicio privado de la violencia por los ciudadanos.

Es así que, por ejemplo, la Asamblea nacional francesa deja claro, en el articulado de su Declaración de Derechos de 1789, que la manera de garantizarlos es a través de una fuerza pública integrada en el aparato administrativo del Estado, para cuyo mantenimiento deben contribuir equitativamente todos los ciudadanos, pues todos se benefician de su labor[28]. La consagración de esta panoplia de derechos subjetivos ciudadanos determina, por un lado, que la legítima acción punitiva dentro del territorio sea patente única del órgano de gobierno que, a través de la policía, gestiona el orden público y consolida la garantía de los derechos y, por otro, que será deber de todos los ciudadanos sufragar ese servicio que les presta, a cada uno de ellos, la seguridad básica para desarrollarse en su esfera privada cotidiana. Y lo mismo se aplica a la soberanía exterior y la defensa de las fronteras, cuya seguridad se encomienda a un ejército profesional y sufragado desde el Estado.

[28] La *Declaración de los Derechos del Hombre y del Ciudadano* recoge en su artículo 12 que "La garantía de los derechos del hombre y del ciudadano necesita de una fuerza pública; por lo tanto, esta fuerza ha sido instituida en beneficio de todos, y no para el provecho particular de aquellos a quienes ha sido encomendada". Por su parte, el artículo 13 señala que "Para el mantenimiento de la fuerza pública y para los gastos de administración, resulta indispensable una contribución común; ésta debe repartirse equitativamente entre los ciudadanos, proporcionalmente a su capacidad".

Ediciones Universidad de Salamanca | CC BY-NC-ND

De esta forma, se mantienen en delicado equilibrio dos dinámicas distintas pero complementarias: la del hombre, emotiva, que reivindica su libertad y sus derechos, y la del Estado, institucional, fruto del acuerdo que garantiza la vida en sociedad y cuya consecución justifica el monopolio de la violencia (MONGARDINI, 2007, pág. 61).

Cobra así sentido la teoría kantiana que considera la seguridad como competencia del Estado, garante de los derechos inalienables de sus ciudadanos frente a las amenazas idiosincráticas del estado de derecho natural, que requiere para su perfección la creación de un ordenamiento jurídico internacional similar al existente en el interior de los Estados, que coarte el recurso a la violencia por parte de éstos y regule su actuación con imperativos morales en las relaciones internacionales (ANGUITA OSUNA, 2021, págs. 24-25).

En 1919 Max Weber, en el ciclo de conferencias donde expone *La Política como profesión*, define al Estado moderno como *la única fuente del derecho a la violencia física*, la cual ejerce como medio específico y de manera legítima dentro de su territorio cuando así lo necesite para garantizar la seguridad de los miembros de la comunidad que lo justifica y mantiene (WEBER, 2007, págs. 56-57). Tres aspectos determinan esta interpretación occidental de la seguridad como monopolio incontestable del Estado: quién está autorizado a utilizar la fuerza; qué se considera uso legítimo de la violencia; y bajo qué circunstancias y con qué propósitos puede el Estado usarla. Respecto a la primera y segunda de las cuestiones, queda claro desde la perspectiva analizada que lo específico del Estado se identifica con la prohibición a los ciudadanos del uso privado de la fuerza, y la garantía de su cumplimiento a través de la reserva que para sí hace del empleo físico de la violencia aunque, evidentemente, ésta siempre represente la *última ratio* y la excepción. En cuanto al tercer considerando, la legitimidad del uso de la fuerza se soporta en el proceso democrático de toma de decisiones, que lo garantizan y que obligan al Estado a rendir cuentas ante el órgano de representación establecido (KRAHMANN, 2009).

La consolidación durante los pasados tres siglos del *Estado nación* como forma de articular las democracias modernas y las prácticas internacionales de ello derivadas, sirve de base para la legitimación del uso de la violencia centralizada en instituciones como las fuerzas armadas y los cuerpos policiales (KRAHMANN, 2009), enraizando la canalización exclusiva de las demandas sociales de seguridad hacia el Estado, fuente de autoridad política y único actor de la escena que garantiza un entorno de convivencia pacífica en el que poder realizar los derechos y libertades humanas, que constitucionalmente refrenda el sistema democrático. Por extensión, los actos de violencia privada son sancionados por el derecho penal y, consecuentemente, desaprobados por el Estado.

Pero como el Derecho y las instituciones evolucionan con el momento histórico y la realidad humana a la que sirven, el papel del Estado debe igualmente evolucionar para atender las demandas ciudadanas en un momento de cambio de paradigma en las relaciones internacionales, fruto del contexto geopolítico surgido a raíz del final de la Guerra Fría.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Efectivamente, la reunificación de Alemania con la caída del Muro de Berlín en 1989 y la posterior disolución del Pacto de Varsovia y de la URSS entre 1990 y 1991, supone el final del bipolarismo y la confrontación ideológica que sostuvo los cuarenta y cinco años de Guerra Fría dejando a EE.UU., momentáneamente, como única gran potencia a la que se le presenta la doble oportunidad de, por un lado, expandir su modelo basado en la democracia y el capitalismo y, por otro, de actuar como director del teatro mundial.

La eclosión de Internet y las nuevas tecnologías al albor del nuevo siglo impulsan definitivamente el fenómeno de la globalización, que se caracteriza por una integración como nunca antes a lo largo de la historia de los ámbitos productivo, económico, político, militar, social y cultural, todos ellos al mismo tiempo y en cualquier parte del mundo, con consecuencias que trascienden las clásicas fronteras del Estado, ensalzan los derechos individuales y fomentan maneras de pensar más homogéneas, vigorizando la interconexión entre comunidades, pueblos y naciones.

Esta interdependencia del mundo actual ofrece evidentes oportunidades, como el desarrollo del estado de bienestar o el enriquecedor intercambio cultural, pero, a su vez, conlleva nuevos riesgos como los flujos migratorios, las consolidación del poder de las estructuras de crimen organizado, la expansión del terrorismo internacional, la aparición de los ciberataques, la dependencia tecnológica, el cambio climático o las crisis económicas que generan graves vulnerabilidades que erosionan los pilares del Estado y pueden desencadenar crisis interconectadas con efectos en cascada. Todo ello actúa como factor estresor de los tradicionales instrumentos de respuesta del Estado y, en relación con el tema que nos ocupa, ha dado entrada a novedosas y extensivas interpretaciones del concepto de seguridad, así como al empleo privado de la fuerza.

Una de las primeras consecuencias es que deja de tener sentido la distinción entre *seguridad interior* y *seguridad exterior* puesto que, fruto de la hiperconectividad y de la transmisión de información en tiempo real, lo que ocurre allende nuestras fronteras ahora tiene un efecto directo en nuestro entorno próximo. Por otro lado, los Estados deben aprender a gestionar la gobernabilidad dando cabida a distintos actores con intereses multisectoriales, entre los que destacan las empresas privadas y las organizaciones no gubernamentales. En este entorno de decisión poliédrico, en el que intervienen una amplia gama de partes privadas interesadas, el Estado pierde el monopolio de poder y tiene que ejercer, desde un puesto lógicamente preponderante y privilegiado, como coordinador de actores. La acción de gobernar es ahora un fenómeno cada vez más híbrido, multidimensional y plural, donde al sector público se le exige que contribuya a la competitividad de su entorno, y que mantenga la responsabilidad en la organización eficaz de los mercados y la defensa de los intereses de los ciudadanos (ZIMMERMANN, 2007, pág. 189).

Esta *red de actores* y la presión social en la conducción de los asuntos que les afectan es la que obliga al Estado a abrirse a nuevas formas de actuación donde se difumina la distinción entre lo público y lo privado (PETERS & PIERRE, 2005, págs. 40-41). Es así como, desde finales del siglo pasado, se comienza a gestar un clima global de intensa y creciente actividad económica, de eficacia y eficiencia que obliga al adelgazamiento de las administraciones, de digitalización y de evolución tecnológica vinculada al progreso

Ediciones Universidad de Salamanca | CC BY-NC-ND

y la prosperidad que promueven una fuerte demanda de seguridad que el Estado no llega a cubrir y que, por tanto, es satisfecha por el mercado libre como si de un sector económico más se tratase, de forma que los servicios proporcionados por las empresas militares y de seguridad privada se integran en los procedimientos operativos y estrategias de seguridad de gobiernos, organizaciones internacionales, organizaciones no gubernamentales (ONG) y empresas multinacionales que precisen sus servicios (LABORIE IGLESIAS M. , 2013, pág. 14).

La consecuencia inmediata de esta situación *de facto* es la crisis de la fórmula clásica referida al monopolio del ejercicio legítimo de la violencia por parte del Estado, que afecta a los fundamentos normativos y a la prestación de la seguridad ciudadana, y que exige una reconsideración de las leyes nacionales e internacionales, planteadas desde la perspectiva del Estado nación y la prohibición de la fuerza privada (KRAHMANN, 2009).

A todo ello viene a sumarse la necesidad de arbitrar una esfera de seguridad en el ámbito del ciberespacio que permita un uso fiable de ese nuevo marco de relaciones humanas, caracterizado por "la ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan" y que "definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad"[29].

1.3. De la garantía de seguridad a la seguridad como garantía: la seguridad humana

De acuerdo a lo expuesto hasta ahora la seguridad, desde los orígenes de la vida en sociedad, se ha sentido como una necesidad vital del ser humano que ha tenido su correspondiente desarrollo conforme a la evolución del sistema político y social de los sucesivos periodos históricos, con reflejo, a su vez, en los cuerpos normativos coetáneos para tratar de vincular, poco a poco, la interpretación de la seguridad a la garantía de los derechos ciudadanos, y de legitimarla a través de la atribución al Estado del monopolio legal de la fuerza como máximo exponente de protección.

En este sentido de vinculación entre seguridad y derechos, aun cuando no hablamos de valores sociales o éticos que varían en las dimensiones de espacio y tiempo, es adecuado considerar que los conceptos -ideas que conforman el entendimiento-, por cuanto precisan de la dimensión comunicativa del lenguaje, evolucionan para adaptarse a la realidad del momento y del entorno en que deben ser aplicados. Por ello, y porque la Constitución es *norma normarum,* norma para la creación de normas, fuente de las fuentes del derecho que funda todo el ordenamiento jurídico (MARAÑÓN GÓMEZ & ARÉVALO GUTIÉRREZ, 2019, pág. 10), puede convenirse que la Constitución "es sólo cognoscible y comprensible, si se la pone en relación con el resto del ordenamiento" (LÓPEZ GUERRA, 1983, pág. 9), en cuanto sistema completo de normas en el que también se señala los órganos de poder con capacidad normativa y los tipos de normas que de ellos pueden derivarse. Avanzando en esta idea, el constitucionalismo del siglo

[29] Estrategia Nacional de Ciberseguridad 2019. Op. Cit., Cap.1, pág. 43440.

Ediciones Universidad de Salamanca | CC BY-NC-ND

XX se construye en torno a la consideración de los derechos fundamentales desde una doble vertiente, como derechos subjetivos ciudadanos exigibles frente al Estado y, también, como elementos sistémicos de su propia estructura política que obligan a los poderes públicos en su actuación como garantes de aquellos (RIDAURA MARTÍNEZ, 2014, pág. 324).

Paradójicamente, con el inicio del nuevo siglo la sociedad occidental alcanza las mayores cotas de seguridad de su historia, con elevados niveles de riqueza económica y multitud de servicios de carácter público a disposición de los ciudadanos con los que, en teoría, cubrir una satisfactoria sensación de seguridad y bienestar. Sin embargo, algunos autores llaman la atención sobre la percepción subjetiva de inseguridad de esta sociedad que, objetivamente, no parece estar bajo amenazas más graves que en cualquier otro tiempo pretérito (RAMÍREZ, 2005, pág. 16) pero que percibe el mundo como un lugar inseguro y desigual que alimenta crisis consecutivas, interconectadas y multidimensionales.

El ser humano, individualmente considerado, ya no se siente seguro bajo el anquilosado andamiaje del *Estado nación*, soberano detentador del monopolio de la fuerza más preocupado por proteger su territorio de la amenaza externa que de procurar el bienestar de aquellos a los que, según la teoría política, representa. La garantía de la seguridad tal como se entendía hasta los años noventa del siglo XX ya no es suficiente. Las nuevas amenazas emergentes y los desafíos vinculados a la expansión del horizonte de libertades, posibilidades de desarrollo y fundadas pretensiones de vida digna en igualdad de condiciones, propias del nuevo siglo, exigen un concepto de seguridad igualmente amplio, que no acabe en la mera protección frente a la violencia física entre las personas, sino que afronte esta dimensión multidimensional que aglutina todos los derechos humanos. Desde ahora la seguridad, necesariamente, debe estar vinculada al bienestar del ser humano, y ser entendida y preservada como *medio* para alcanzar una vida sin miedo, sin pobreza y con dignidad. Es la seguridad como garantía colectiva para todos los seres humanos. Se trata de hacer realidad lo que parece imposible.

Todo ello conduce a lo que la doctrina señala como *la expansión del concepto de seguridad* en una doble vertiente:

1. Expansión vertical, en cuanto que ya no es el Estado sino el ciudadano el foco de atención de la seguridad que, además, se ve afectada por nuevos actores de carácter no estatal.
2. Expansión horizontal, en referencia a aquellas amenazas tradicionalmente consideradas de carácter internacional que ahora pasan a tener una dimensión nacional o regional, al mismo tiempo que desafíos hasta ahora de naturaleza estatal comienzan a adquirir dimensión global (ABAD QUINTANA & PRIEGO MORENO, 2003, pág. 54).

1.3.1. El concepto de *seguridad humana*

Para encarar el estudio de esta cuestión hay que comenzar recordando que el final de la Guerra Fría supone un elemento disruptivo generador de profundos cambios en el orden internacional, al perder las referencias ideológicas y de bipolarización heredadas de la

Ediciones Universidad de Salamanca | CC BY-NC-ND

Segunda Gran Guerra, lo cual afecta no solo a la esfera geopolítica, a sus actores y al modelo de relaciones internacionales, sino también a la forma en que se comienza a ver la propia configuración del Estado westfaliano y, por ende, de conceptos clave como la seguridad y el conjunto de amenazas y riesgos que pueden poner en peligro este orden tradicional.

Como hemos apuntado anteriormente, ya no se comparte ese enfoque menguado y clásico que, desde la consideración de la soberanía como único valor supremo a defender frente a la amenaza exterior, ampara una visión estatocéntrica, castrense y territorial de la seguridad que legitima la acción interventora del Estado. Enfrentándolo, irrumpe un pensamiento crítico liderado en gran medida por actores supranacionales que pivota sobre dos ejes: la globalización como paradigma de las nuevas interacciones, y el desarrollo como pieza clave del bienestar social y de la seguridad.

De acuerdo al primero de ellos, el *Estado nación* ya no es el único actor legitimado en la arena internacional y su forma de entender la seguridad deja de lado a los ciudadanos, al no poder garantizarles la paz social y despreciar cualquier otra amenaza que no sea la militar. La aparición en escena de nuevos *actores no estatales* con diferentes intereses sociales, culturales, políticos, religiosos o económicos, entre otros, abre la puerta de entrada a inéditos focos de atención que se cuelan en las agendas de política de seguridad del mundo desarrollado y que miran hacia el ser humano y su relación con el entorno para conseguir una vida estable y pacífica (ZAVALETA HERNÁNDEZ, 2015, págs. 65-87). El Estado ya no puede afrontar en solitario estas nuevas demandas derivadas de la visión humana de la seguridad y que superan el tradicional marco de la violencia física. Necesita para ello de la participación del sector privado y del compromiso de la sociedad civil que, bajo las consignas de la *nueva gestión pública* y de la *gobernanza*, van ocupando espacios antes reservados para aquel en exclusiva.

El segundo de los ejes críticos gira en torno a la vinculación de la seguridad con el derecho al desarrollo de las sociedades, para hacer frente a amenazas emergentes como las migraciones, la pobreza, las pandemias, las crisis económicas y financieras repentinas, la escasez de recursos, las cuestiones de género o el cambio climático, que trata de romper con la idea de que la seguridad de las personas se consuma en la dimensión clásica que la equipara con la del Estado (FONT & ORTEGA, 2012, págs. 161-172). La seguridad, el desarrollo y los derechos humanos forman a partir de este momento un triunvirato que gobierna las agendas de los Estados soberanos, que no puede, ni debe, ser destronado.

Comienza así a interpretarse la *seguridad como factor de desarrollo* indivisible e íntimamente vinculado con la democracia y los derechos humanos, tal y como se concluye en la Reunión de Moscú de la Conferencia sobre la Seguridad y la Cooperación en Europa (CSCE)[30], de octubre de 1991, donde los Estados participantes se declaran:

[30] La *Conferencia sobre la Seguridad y la Cooperación en Europa* (CSCE) celebró en París una primera reunión del 30 de mayo al 23 de junio de 1989, fruto de la cual surgió la *Carta de París para la Nueva Europa* donde, en un marco multilateral y alineado con la premisa de la consideración de la democracia como único sistema de gobierno adecuado para la consecución de sus objetivos, se analizaban los desafíos en materia de seguridad que surgían en el nuevo escenario mundial que dejaba la finalización de la Guerra

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] decididos a lograr aún mayores progresos en la aplicación de esas disposiciones dado que el pleno respeto de los derechos humanos y las libertades fundamentales y el desarrollo de sociedades basadas en una democracia pluralista y en el estado de derecho son requisitos previos para un orden duradero de paz, seguridad, justicia y cooperación en Europa"[31].

Apenas tres años después, en el marco del Programa de las Naciones Unidas para el Desarrollo (PNUD), el *Informe sobre Desarrollo Humano 1994* explora "las nuevas fronteras de la seguridad humana en las vidas cotidianas de las personas; se trata de descubrir señales de alerta temprana que puedan desencadenar acciones de diplomacia preventiva a fin de que una sociedad no llegue a un punto de crisis"[32], proponiendo un fortalecimiento sustancial del papel de las Naciones Unidas (NNUU) para poder dar satisfacción a las necesidades de la humanidad no solo en materia de paz sino, también, de desarrollo. En este sentido, el informe es innovador al declarar que:

> "[…] el concepto de seguridad se ha interpretado en forma estrecha durante demasiado tiempo: en cuanto seguridad del territorio contra la agresión externa, o como protección de los intereses nacionales en la política exterior o como seguridad mundial frente a la amenaza de un holocausto nuclear. La seguridad se ha relacionado más con el Estado nación que con la gente"[33].

A partir de este novedoso planteamiento, el Informe del PNUD delimita las cuatro características básicas de la *seguridad humana* -centrada en las personas, universalidad, interdependencia y gestión preventiva- y los siete ámbitos que la conforman -seguridad económica, alimentaria, sanitaria, ambiental, personal, comunitaria y política-.

Esta visión de NNUU que define el concepto integrador de *seguridad humana* es un elemento trascendental para la evolución normativa en la materia a nivel mundial, por cuanto redimensiona y contextualiza la seguridad en relación con la *percepción de inseguridad* de la mayoría de la población que:

> "[…] se debe más a las preocupaciones acerca de la vida cotidiana que al temor de un cataclismo en el mundo. La seguridad en el empleo, la seguridad del ingreso, la seguridad en la salud, la seguridad del medio ambiente, la seguridad respecto del delito: son éstas las preocupaciones que están surgiendo en todo el mundo acerca de la seguridad humana"[34].

Fría. La segunda de estas reuniones se celebró en Copenhague del 5 al 29 de junio de 1990 y la tercera tuvo lugar en Moscú del 10 de septiembre al 4 de octubre de 1991, bajo el lema de Conferencia sobre la Dimensión Humana. A partir de 1994 se transformó en la Organización de Seguridad y Cooperación en Europa (OSCE).

[31] Documento de la Reunión de Moscú de la Conferencia sobre la dimensión humana de la OSCE, de octubre de 1991. Página 1. Disponible en: https://www.osce.org/files/f/documents/1/a/14315.pdf (02/02/2024).

[32] Página III del Prefacio del Informe sobre Desarrollo Humano 1994, Programa de las Naciones Unidas para el Desarrollo, publicado por el Fondo de Cultura Económica y disponible en: https://hdr.undp.org/system/files/documents/hdr1994escompletonostats.pdf (02/02/2024).

[33] IBIDEM, página 25.

[34] IBIDEM, página 3.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Y para abordar este reto es preciso enfocar el *desarrollo* como un proceso de extensión de las capacidades y libertades de las personas (FONT & ORTEGA, 2012, pág. 170).

En el año 2005 la Asamblea General NNUU va más allá presentando una interpretación aún más amplia de la libertad que abarca el desarrollo, la seguridad y los derechos humanos, concluyendo que "no tendremos desarrollo sin seguridad, no tendremos seguridad sin desarrollo y no tendremos ni seguridad ni desarrollo si no se respetan los derechos humanos"[35]. Además, incorpora un tercer elemento en la búsqueda de la paz como base de la seguridad humana, añadiendo a los dos ya definidos por el Informe de 1994 del PNUD -libertad para vivir sin miseria y libertad para vivir sin temor-, el de la libertad para vivir con dignidad, por cuanto "en un mundo cada vez más interdependiente, los avances en el ámbito del desarrollo, la seguridad y los derechos humanos han de correr parejos" [36].

Ese mismo año, en el Documento Final de la Cumbre Mundial 2005 de la Asamblea General NNUU, se hace una referencia expresa a la *seguridad humana* en el párrafo 143 como derecho a vivir sin temor y en igualdad de oportunidades para desarrollar todo el potencial individual de las personas, que deviene en pieza clave para, a partir de ahí, promover la aceptación y la comprensión de este concepto en el seno de la comunidad internacional, comprometiéndose para ello a "examinar y definir el concepto de *seguridad humana* en la Asamblea General" [37].

El 10 de septiembre de 2012 marca un hito por cuanto la Asamblea General de NNUU aprueba la Resolución 66/290 de Seguimiento del párrafo 143, relativo a la seguridad humana, del Documento Final de la Cumbre Mundial 2005[38], en la que los Estados miembros convienen un entendimiento común de la seguridad humana que, a partir de entonces, engloba siete aspectos decisivos:

1. Las tres dimensiones de la libertad de toda persona para desarrollar su potencial: *vivir en libertad y con dignidad, libres de la pobreza y la desesperación*.
2. La exigencia de respuestas orientadas para y por las personas, respuestas exhaustivas y adaptadas a cada contexto.

---

[35] Asamblea General de las Naciones Unidas, A/59/2005/add.1, de 23 de mayo de 2005. Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos. Informe del Secretario General. Párrafo 17, página 6. Disponible en: https://www2.ohchr.org/spanish/bodies/hrcouncil/docs/gaA.59.2005.Add.1_Sp.pdf (02/02/2024).

[36] IBIDEM, página 61.

[37] Asamblea General de las Naciones Unidas, A/RES/60/01, de 24 de octubre de 2005, Documento Final de la Cumbre Mundial 2005, párrafo 143: "Subrayamos el derecho de las personas a vivir en libertad y con dignidad, libres de la pobreza y la desesperación. Reconocemos que todas las personas, en particular las que son vulnerables, tienen derecho a vivir libres del temor y la miseria, a disponer de iguales oportunidades para disfrutar de todos sus derechos y a desarrollar plenamente su potencial humano. Con este fin, nos comprometemos a examinar y definir el concepto de seguridad humana en la Asamblea General". Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/487/63/PDF/N0548763.pdf?OpenElement (02/02/2024).

[38] Resolución aprobada por la Asamblea General el 10 de septiembre de 2012, A/RES/66/290, de 25 de octubre de 2012, sobre el *Seguimiento del párrafo 143, relativo a la seguridad humana, del Documento Final de la Cumbre Mundial de 2005*. Disponible en: https://www.un.org/es/ga/66/resolutions.shtml https://www.refworld.org/es/ref/themreport/unga/2013/es/34012 (02/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

3. La gestión anticipativa como base de la protección, puesto que se trata de evitar el riesgo, no esperar a tener que solucionar los efectos de su causación.
4. La necesaria implicación de los Estados para velar por su aplicación y reforzar las soluciones de carácter local, puesto que sin el compromiso del nivel político es inviable la adopción de las medidas necesarias.
5. La complementariedad de la seguridad nacional como elemento indispensable para la paz y la estabilidad, avanzando la idea de que la seguridad nacional se vertebra no solo en torno al Estado sino, también, sobre los derechos de los ciudadanos.
6. El reconocimiento de la profunda interrelación entre la paz, el desarrollo y los derechos humanos.
7. Y, finalmente, el respeto del orden internacional prestablecido sobre la base de la soberanía de los Estados, la integridad territorial y la no injerencia en sus asuntos internos. Es decir, la plena vigencia del Derecho Internacional.

Una vez consensuado el concepto, en enero de 2016, el Fondo Fiduciario de las NNUU para la seguridad humana publica un manual en el que ofrece un enfoque integrado del mismo con el objetivo de crear un marco que genere sinergias para la consecución de la *Agenda 2030* y los *Objetivos de Desarrollo Sostenible* (ODS). Se pretende así poner en valor este enfoque de la seguridad humana como "forma novedosa de pensar acerca del abanico de desafíos que enfrenta el mundo en el siglo XXI y la respuesta de la comunidad internacional"[39], marco multidimensional e interrelacionado imprescindible para alcanzar el desarrollo sostenible. De esta forma, el concepto de seguridad humana se integra por el conjunto de derechos de las personas y las comunidades, por un enfoque operativo que considera el amplio espectro de riesgos y amenazas, por la coherencia derivada de la interrelación entre las políticas afectadas, por la contextualización de estas conforme al país y la comunidad implicada, por la formación de sinergias entre los distintos actores implicados, por su enfoque eminentemente preventivo y, finalmente, por el fomento de la resiliencia[40] de las personas para actuar por sí mismas en su propio beneficio[41].

No obstante, esta interpretación de la *seguridad humana* presenta objeciones para alguno de los expertos dedicados al estudio de la materia, como Martínez Quinteiro. La primera es la que se refiere a que esta visión de la seguridad tiene su origen en la Carta de las Naciones Unidas de 1945, en cuyo artículo 55 ya se estipula que las condiciones de estabilidad y bienestar necesarias para la paz requieren el compromiso de sus miembros con el respeto a los derechos humanos, la solución de los problemas internacionales que subyacen a la pobreza y la desigualdad, y la consecución de mejores

[39] *Manual de Seguridad Humana*. Un enfoque integrado para la consecución de los Objetivos de Desarrollo Sostenible y los ámbitos de acción prioritarios de la comunidad internacional y el sistema de las Naciones Unidas. Apartado 1. El enfoque de la seguridad humana y su valor agregado. Fondo Fiduciario de las NNUU para la Seguridad Humana, enero 2016. Página 6. Disponible en: https://www.un.org/humansecurity/wp-content/uploads/2023/02/HS-handbook-Spanish.pdf (02/02/2024).

[40] La resiliencia se entiende como la capacidad de ser flexible para aguantar y recuperarse, conforme al documento *La resiliencia en el marco de la seguridad nacional*. Presidencia del Gobierno, marzo 2024. NIPO 143-24-031-8. Página 9. Disponible en: https://www.dsn.gob.es/index.php/node/23443 (11/01/2025).

[41] *Manual de Seguridad Humana*, Op. Cit., páginas 9-11.

Ediciones Universidad de Salamanca | CC BY-NC-ND

niveles de vida, trabajo, desarrollo y progreso económico y social para todos[42], por lo que considera que el derecho a la seguridad humana no es un derecho realmente nuevo sino una "re-denominación afortunada de otro preexistente, o una síntesis de las varias dimensiones ya reconocidas del *Derecho Humano a la Seguridad*" que ya consagraba la Constitución Francesa de 1793 al definirla "como el derecho de toda persona a ver garantizados todos los derechos" (MARTÍNEZ QUINTEIRO, 2018).

Otra parte de la doctrina, como Font y Ortega, advierte sobre los riesgos derivados de relacionar los problemas del desarrollo con la seguridad, por cuanto puede conllevar que la cooperación y la acción solidaria de los países más desarrollados hacia otros menos favorecidos quede subyugada a intereses estratégicos o, directamente, sirva de camuflaje para campañas militares interesadas (FONT & ORTEGA, 2012, págs. 161-172). De hecho, podemos convenir que es a través de este enfoque como la seguridad trasciende el clásico esquema que distingue entre *interior* y *exterior* para alcanzar una perspectiva multidimensional, que engloba intervenciones de distinto carácter, fuera del propio territorio, para prevenir amenazas transfronterizas y globales. El uso de medidas militares, diplomáticas, civiles, policiales y de cooperación se convierten en importantes componentes de la estrategia de seguridad de los Estados occidentales, que buscan de esta manera crear un cinturón de estabilidad en los países de su entorno más o menos próximo, con distinto alcance y repercusión en algunos de los más desfavorecidos que han sido objeto de ellas[43].

Finalmente, hay autores como Mejía Molina, que entienden que el debate sobre la articulación de la seguridad internacional no está cerrado, ni previsiblemente lo esté nunca, por la propia evolución de la realidad a la que atañe. En este sentido, coligen que no existe un acuerdo que permita interpretar que la *seguridad humana*, causalmente multidimensional y objetivamente individual, prevalezca como modelo frente a la *seguridad clásica*, orientada a la defensa del Estado y sus tres pilares -soberanía, territorio y población-, concluyendo que las dos concepciones de seguridad "siguen vigentes y deberían reforzarse mutuamente. Si la seguridad del Estado mejora también la seguridad humana se verá fortalecida" (MEJÍA MOLINA, 2009).

A nuestro juicio, estas discrepancias doctrinales enriquecen el debate aportando una nueva perspectiva de la *seguridad integral* que, a la vista del desarrollo normativo actual, consideramos más adecuada a la realidad internacional que, en todo caso, es

[42] Artículo 55 de la *Carta de las Naciones Unidas*: "Con el propósito de crear las condiciones de estabilidad y bienestar necesarias para las relaciones pacíficas y amistosas entre las naciones, basadas en el respeto al principio de la igualdad de derechos y al de la libre determinación de los pueblos, la Organización promoverá:

a. niveles de vida más elevados, trabajo permanente para todos, y condiciones de progreso y desarrollo económico y social;
b. la solución de problemas internacionales de carácter económico, social y sanitario, y de otros problemas conexos; y la cooperación internacional en el orden cultural y educativo; y
c. el respeto universal a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión, y la efectividad de tales derechos y libertades".

[43] Sirvan como ejemplo las intervenciones estadounidenses y europeas en Irak, Afganistán, Pakistán, Yemen, Somalia, Mali y Oriente Próximo, entre otros.

Ediciones Universidad de Salamanca | CC BY-NC-ND

compleja y exige respuestas pactadas y multidimensionales para satisfacer los ODS, con diferentes niveles de responsabilidad que se imbrican en el marco de las alianzas en las que, por un lado, los Estados nacionales siguen asumiendo una función primordial de protección de sus ciudadanos propia de la soberanía que detentan y, por otro, la comunidad internacional, con las entidades no gubernamentales y otros actores regionales y locales liderados por las NNUU, los complementa y refuerza para garantizar el pleno respeto de los derechos humanos y, a la vez, de la soberanía, la integridad territorial y autonomía de gobierno de esos mismos Estados.

1.3.2. El valor agregado de la seguridad humana

Dejando para un capítulo posterior el análisis de las opiniones que consideran que la estructura de las NNUU se ha mostrado poco efectiva a lo largo de sus casi ochenta años de existencia, evidenciando problemas de paralización por el discutido y anacrónico *derecho a veto* de sus miembros permanentes del Consejo de Seguridad, la falta de capacidad para lograr consensos entre miembros cada vez más polarizados y de cuya aportación económica depende su continuidad, la quiebra permanente del respeto a los derechos humanos por la falta de compromiso de Estados que no creen en ellos y su, en definitiva, inoperancia para enfrentar los cambios de profundo calado que se necesitan para devolverle la legitimidad y eficacia pretendida en la Carta de San Francisco (MARTÍNEZ QUINTEIRO, 2018), hay que reconocer que a la sombra del discurso no vinculante de las NNUU han ido creciendo compromisos internacionales que han permitido configurar derechos como, por ejemplo, el de la seguridad humana, que actualiza y trae a la nueva era digital, global, cambiante y tecnificada viejos ideales de paz, igualdad y desarrollo que, de otra forma, probablemente hubiesen quedado mermados, si no olvidados.

Con ello pretendemos poner en valor el enfoque de la seguridad humana como incentivo y guía a los Estados para establecer estrategias que permitan afrontar los problemas consustanciales a promover el marco político, económico, social y cultural necesarios para garantizar la paz, el desarrollo y los derechos humanos de sus ciudadanos. Estos desafíos que debe afrontar la comunidad internacional en su conjunto son complejos y están interconectados, por lo que exigen una respuesta anticipativa, proactiva, contextualizada y coherente que aporte soluciones integrales y adaptadas.

La aplicación del enfoque de la seguridad humana a la realidad específica de cada Estado se concreta a través de programas y planes nacionales, que el Manual de 2016 del Fondo Fiduciario de las NNUU para la Seguridad Humana[44] operativiza en tres fases: una primera de análisis, identificación y planificación del despliegue de medidas; la segunda de aplicación al entorno concreto de la comunidad afectada; y la tercera de evaluación del rendimiento y rango de objetivos alcanzados.

En relación a la UE, su Estrategia Global para la Política Exterior y de Seguridad de 2016 incluye específicamente como objetivo, en el marco de la aproximación integral a los conflictos y crisis en nuestro entorno de influencia, esta visión de la seguridad humana:

[44] *Manual de Seguridad Humana*. Op. Cit., páginas 9-11.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "The EU will engage in a practical and principled way in peacebuilding, concentrating our efforts in surrounding regions to the east and south, while considering engagement further afield on a case by case basis. The EU will foster human security through an integrated approach"[45].

En España, esta formulación de la seguridad humana tiene cabida, como se analizará en el Capítulo 4, en el Modelo de Seguridad 2030 del Ministerio del Interior, donde ocupa una situación preferente respecto a la misión policial, junto a la defensa de la libertad.

Continuando con el análisis de los componentes de la seguridad humana sobre los que se estima el posible impacto de las amenazas, estos se agrupan en siete aspectos relacionados con los diferentes planos económico, alimentario, sanitario, ambiental, personal, comunitario y político que analizamos a continuación.

1) Seguridad económica

El dominio económico de la seguridad atiende principalmente a la necesidad de hacer frente al aumento de la pobreza y la desigualdad, a prevenir las crisis financieras y económicas y, a través de esto, resolver los flujos migratorios tanto a nivel interno -del ámbito rural al urbano- como extrafronterizo -desde el sur pobre hacia el norte rico-.

Para ello es necesario implementar políticas económicas dinámicas y de crecimiento, que se apoyen no solo en la inversión pública sino, también, en el sector privado, para ser capaces de generar empleo de calidad y adecuados niveles de renta a medio y largo plazo. En este sentido, es necesario que los Estados abran el acceso a la financiación y que se apueste por inversiones en capital humano y en infraestructuras orientadas al desarrollo, básicamente en los sectores de la energía, el transporte y las comunicaciones. En este mismo sentido, el empoderamiento de la mujer ha demostrado ser uno de los motores más eficaces del desarrollo.

Las causas de la inseguridad económica son, entre otras, el desempleo, la falta de oportunidades de desarrollo en origen, la escasa inversión pública y la disminución de la productividad agregada de la economía de los países más desfavorecidos.

2) Seguridad alimentaria

Este componente de la seguridad humana se fija en la inflación y su incidencia en el incremento del gasto de los hogares en alimentos básicos, así como su interrelación con

[45] "Observamos cada vez más que Estados frágiles se desmoronan en conflictos violentos. Estas crisis, y la violencia y el sufrimiento humano indescriptibles que dan origen, amenazan nuestros intereses vitales compartidos. La UE participará de manera práctica y basada en principios en la consolidación de la paz, concentrando nuestros esfuerzos en las regiones circundantes al este y al sur, considerando al mismo tiempo un compromiso más lejano caso por caso. La UE fomentará la seguridad humana mediante un enfoque integrado" (Traducción propia).
Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union´s Foreign And Security Policy. June 2016. Página 28. Disponible en: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (15/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la explotación agrícola y ganadera del entorno, cuyo nivel de producción se encuentra muy vinculado a los factores ambientales y climáticos. Los habitantes de las zonas rurales empobrecidas necesitan alicientes económicos, capacitación técnica, recursos materiales y fácil acceso a medios de transporte, agua y energía que les permitan rentabilizar su esfuerzo e inversiones, para asegurar la producción de alimentos y su reparto a través de las cadenas de distribución.

Los factores determinantes de la inseguridad alimentaria son el precio de los alimentos, la gestión del reparto y la falta de prácticas agrícolas sostenibles, junto con otras causas de carácter transversal como, por ejemplo, las crisis económicas que tienen consecuencias devastadoras en los países más pobres.

3) Seguridad sanitaria

Los indicadores de salud de la población son otro de los componentes de la seguridad humana que se gestiona a través del acceso universal y libre a la asistencia sanitaria, y el adecuado dimensionamiento de la infraestructura de atención primaria para dar cobertura a todos los ciudadanos.

Las causas de la inseguridad sanitaria se relacionan con el aumento de dolencias y la propagación de enfermedades infecciosas, el azote de pandemias y la falta de medios y recursos para dar la debida cobertura médica a la población. Para neutralizarlas son necesarias medidas de mejora de los sistemas de atención sanitaria y la educación preventiva de la población.

4) Seguridad ambiental

Garantizar la sostenibilidad del medio ambiente es crucial para evitar la pérdida de recursos naturales y poder garantizar el acceso de la población a la tierra, al agua potable y a los servicios de saneamiento básicos, así como a la calidad del aire que se respira, principalmente en zonas urbanas superpobladas.

Los cambios climáticos son una causa de riesgo transversal que exigen fijar prioridades como la repoblación forestal para luchar contra la desertización, la ordenación de los recursos hídricos para asegurar el acceso al agua, la preservación de especies y ecosistemas que garanticen la biodiversidad y la reducción de la contaminación que mejore la esperanza de vida, todo ello en un marco legal adecuado y consecuente con estos objetivos.

5) Seguridad personal

El terrorismo transnacional y la delincuencia organizada son amenazas globales que exigen una respuesta coordinada y única para defender los valores democráticos y el respeto de los derechos humanos. Para ello se precisa un esfuerzo de delimitación conceptual de estos fenómenos delincuenciales, junto con el acercamiento de las legislaciones nacionales para poder adoptar las medidas necesarias y castigarlos con sanciones penales efectivas, proporcionadas y disuasorias.

Ediciones Universidad de Salamanca | CC BY-NC-ND

También resulta estratégica la prevención de los conflictos armados, tanto internos como externos, que afectan cada vez a mayor número de población civil y que, por sus devastadoras consecuencias, minan la confianza de estos en las instituciones. Para lograr esta prevención, se consideran esenciales los planes nacionales de desarrollo y reducción de la pobreza a través de alianzas con actores locales y nacionales que promuevan la generación de tejido social estable y con proyectos de futuro.

Finalmente, la violencia derivada de la delincuencia común, la violencia sobre personas vulnerables, la violencia doméstica y de género, entre otras, también son indicadores a tener en cuenta en el conjunto global de la seguridad humana.

6) Seguridad comunitaria

La pertenencia a un grupo racial o étnico, a una familia o determinada comunidad confiere al ser humano una identidad cultural con cuyos valores y tradiciones se siente vinculado. Partiendo de esto, hay que señalar que la exclusión social y la marginación son realidades muy asentadas en la mayoría de las comunidades humanas, que tienen un origen diverso y relacionado con otros muchos factores.

Por ello, todos los actores sociales involucrados en su prevención deben estar particularmente atentos a los factores de radicalización y polarización que alimentan el odio entre los distintos grupos de población por cuestiones étnicas o ideológicas, y donde el fenómeno de las migraciones y los colectivos de refugiados puede actuar como precursor de tensiones y conflictos sociales. No es esta cuestión baladí ni, tampoco, exclusiva de países más o menos pobres, con más o menos recursos. Los extremismos son hoy cuestión de alcance global, que alcanzan incluso a países líderes como EE.UU., baluarte de la libertad y la democracia, tal y como señala Roger Senserrich:

> "El fenómeno de las dos Américas, las enormes diferencias políticas y sociales entre norte y sur, campo y ciudad, regiones ricas y regiones pobres no es nuevo. Lo que sí lo es, y que parece haberse acelerado en tiempos recientes, es cómo una de ellas ha decidido darle la espalda a cualquier atisbo de progreso, se opone políticamente a cualquier medida que pueda ayudarla e insiste sin cesar en que la verdadera esencia del país, lo que deseaban los padres fundadores, es ella" (SENSERRICH SOGUES, 2024, pág. 261).

En este sentido, el compromiso de los Estados con el fomento de la educación, el acceso a una vivienda digna y a los servicios básicos, son elementos cruciales para ofrecer opciones de desarrollo igualitarias que sirvan para garantizar unos medios de vida dignos y suficientes para todos.

7) Seguridad política

Uno de los aspectos más relevantes de la seguridad humana es poder vivir en una sociedad respetuosa con los derechos fundamentales. Por ello, los actos de represión, persecución, extorsión, censura o tortura contra la población, así como la violación de

Ediciones Universidad de Salamanca | CC BY-NC-ND

los derechos humanos en cualquiera de sus formas, son indicadores de máxima relevancia a los que atender para evaluar la seguridad política en un Estado.

Para prevenirlos es esencial la gestión política desde el respeto a la democracia y sus procesos, con criterios de buena gobernanza que den entrada a los diferentes actores interesados en la acción de gobierno, con una firme apuesta por conseguir instituciones responsables que luchen de manera decidida contra la corrupción a través de una administración profesional y con sentido de servicio público.

Una vez analizados los siete componentes de la seguridad humana, debemos referirnos a continuación a la Agenda 2030 y los ODS para poder presentar la arquitectura de seguridad en este primer cuarto de siglo XXI.

1.3.3. La visión integral de la seguridad a través de la Agenda 2030 y los ODS

Sobre los rescoldos del evidente fracaso de la comunidad internacional para erradicar la pobreza extrema a través de los Objetivos de Desarrollo del Milenio (ODM), acordados en el año 2000 en la *Cumbre del Milenio* de Nueva York[46], quince años después, el 25 de septiembre de 2015, la Asamblea General NNUU aprueba la Resolución titulada *Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible*[47] tras un elaborado proceso de más de dos años de consultas y debates entre instituciones oficiales y representantes de la sociedad civil, y la presenta como "un plan de acción en favor de las personas, el planeta y la prosperidad" que también busca "fortalecer la paz universal dentro de un concepto más amplio de la libertad"[48].

En la idea de que "la gestión de la globalización necesita ser reconducida de forma que, incluyendo valores, evolucione hacia una globalización sostenible e inclusiva, que permita y mejore las condiciones de vida en todo el planeta y que no deje a nadie descolgado" (GARCÍA SÁNCHEZ, 2019), la Agenda 2030 se gesta como avanzada frente a los retos que presenta la realidad actual marcada, por un lado, por las grandes diferencias de oportunidades, el desequilibrio de los grupos de poder, la desigual distribución de la riqueza y la brecha digital en los países más desfavorecidos pero que, por otro, ofrece una faceta de oportunidades de mejora y progreso gracias a los avances de la medicina, la mejora de la educación, la innovación científica, la expansión de las

[46] La *Cumbre del Milenio* se celebró entre el 6 y el 8 de septiembre de 2000 en Nueva York, y concluyó con la adopción de la Declaración del Milenio por los 189 Estados participantes, en la que se establecen ocho Objetivos de Desarrollo del Milenio: erradicar la pobreza extrema y el hambre, lograr la enseñanza primaria universal, promover la igualdad de género y el empoderamiento de la mujer, reducir la mortalidad infantil, mejorar la salud materna, combatir enfermedades y virus como el VIH/SIDA y el paludismo, garantizar la sostenibilidad del medio ambiente y fomentar una asociación mundial para el desarrollo. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/559/51/PDF/N0055951.pdf?OpenElement (02/02/2024).

[47] Resolución aprobada por la Asamblea General el 25 de septiembre de 2015, A/RES/70/01, de 21 de octubre de 2015. *Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible*. Disponible en: https://unctad.org/system/files/official-document/ares70d1_es.pdf (02/02/2024).

[48] IBIDEM, página 1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

tecnologías de la información y las comunicaciones (TIC) y la interconexión digital a nivel mundial[49].

Partiendo de la necesidad de lograr una alianza colaborativa global y multidimensional como base ideal para su implementación, lección aprendida del fiasco de los ODM, que "hicieron evidente la necesidad de involucrar no sólo a los organismos gubernamentales en la consecución de las metas marcadas, sino a todos los actores que conformaban la sociedad" (GARRO, 2019), la Agenda 2030 incluye como novedad el ODS 16, que representa uno de sus objetivos más ambiciosos destinado a "promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas"[50].

Antes de proseguir con su análisis debe significarse que todos los ODS, como metas globales, son "normas multilaterales no vinculantes, dentro del ámbito del *soft law*, que tratan de conciliar las necesidades de coordinación y acción colectiva con el principio de soberanía nacional" (SANAHUJA, 2019), y esta es precisamente una de sus fortalezas por cuanto permite que los Estados, celosos defensores del orden westfaliano, puedan comprometerse con objetivos enmarcados en el ámbito del *deber ser* delegando su ejecución a actores de distinta naturaleza liderados por NNUU, que legitima de esta manera su actuación multilateral y su narrativa global.

El escenario de la seguridad cuenta ahora con un número mayor de actores, que interpretan papeles novedosos con un enfoque social y sostenible, cuya actuación da sentido a una trama que busca resolver problemas de carácter global, multidimensional y transnacional, donde los ODS que vinculan el desarrollo, el respeto a los derechos humanos y la paz son aceptados por todos como referencia y pilares de la estructura que soporta dicho escenario de seguridad. Todos ellos están interrelacionados y no pueden conseguirse sino de manera conjunta. Por eso la relevancia del ODS 16, que "comporta una aproximación a la seguridad integral y holística, de carácter societal", orientada a la persona como parte de un grupo humano que quiere vivir en paz y desarrollarse en un entorno de respeto, inclusivo y próspero, en comunión con la naturaleza y donde las instituciones de gobierno ya no son el fin sino el medio para conseguirlo (SANAHUJA, 2019).

Esa visión 360º del ODS16 pivota sobre tres grupos temáticos diferentes:

1. La *paz* como base del desarrollo, entendida no ya como *ausencia de guerra* sino en un sentido amplio, vinculado a sociedades inclusivas y sostenibles que buscan su desarrollo en plenitud.
2. La *justicia* referida al amparo judicial universal, para todos, vinculado a un sistema judicial que garantice la efectividad del mismo.
3. Las *instituciones sólidas* como base de estabilidad y buen gobierno, referido a la estabilidad del sistema y la efectividad de la acción de gobierno.

[49] IBIDEM, página 6.
[50] IBIDEM, página 29.

Ediciones Universidad de Salamanca | CC BY-NC-ND

A su vez, esta línea argumental converge con las *tres dimensiones de la libertad* que el Documento Final de la Cumbre Mundial 2005 de la Asamblea General de NNUU presenta en su párrafo 143 como base de la seguridad humana, de acuerdo al siguiente esquema de relaciones:

1) *Libertad para vivir sin miedo*, dimensión de la seguridad que se incardina en las siguientes metas del ODS16:
   - 16.1 Reducir significativamente todas las formas de violencia y las correspondientes tasas de mortalidad en todo el mundo.
   - 16.2 Poner fin al maltrato, la explotación, la trata y todas las formas de violencia y tortura contra los niños.
   - 16.4 De aquí a 2030, reducir significativamente las corrientes financieras y de armas ilícitas, fortalecer la recuperación y devolución de los activos robados y luchar contra todas las formas de delincuencia organizada.
   - 16.a Fortalecer las instituciones nacionales pertinentes, incluso mediante la cooperación internacional, para crear a todos los niveles, particularmente en los países en desarrollo, la capacidad de prevenir la violencia y combatir el terrorismo y la delincuencia.

2) Libertad respecto de la miseria, perspectiva de la seguridad humana que se vincula con las siguientes metas del ODS16:
   - 16.6 Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas.
   - 16.8 Ampliar y fortalecer la participación de los países en desarrollo en las instituciones de gobernanza mundial

3) *Libertad para vivir con dignidad,* elemento íntimamente relacionado con el respeto de los derechos humanos y que, de manera innegociable, conforma la visión amplia de la seguridad humana que se relaciona con las siguientes metas del ODS16:
   - 16.3 Promover el estado de derecho en los planos nacional e internacional y garantizar la igualdad de acceso a la justicia para todos.
   - 16.5 Reducir considerablemente la corrupción y el soborno en todas sus formas.
   - 16.7 Garantizar la adopción en todos los niveles de decisiones inclusivas, participativas y representativas que respondan a las necesidades.
   - 16.9 De aquí a 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos.
   - 16.10 Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales.
   - 16.b Promover y aplicar leyes y políticas no discriminatorias en favor del desarrollo sostenible.

En conjunto, los diecisiete ODS y las ciento sesenta y nueve metas de carácter integrado e indivisible que, desde el principio de responsabilidades comunes pero diferenciadas, presenta la Resolución de la Asamblea General de NNUU de 2015, aplican a todos los

Ediciones Universidad de Salamanca | CC BY-NC-ND

países independientemente de su nivel de desarrollo y a las partes interesadas mediante una alianza de colaboración. Al mismo tiempo, conforman el horizonte de la seguridad que no solo engloba las tres dimensiones de la libertad humana -violencia, pobreza, dignidad- sino que también conjuga las otras tres del desarrollo sostenible -económica, social y ambiental- como única forma de dar respuesta coherente a los retos actuales, interrelacionados y globales, a todos los niveles.

Esta *visión integral de la seguridad* será la que inspire en España, entre otras, la Ley de Seguridad Nacional de 2015 y su aplicación a través, primeramente, de la Estrategia de Seguridad Nacional de 2017 y, a posteriori, de la de 2021, así como sus desarrollos de segundo nivel que dan sustento, por ejemplo, a la creación de la Oficina Nacional de Garantía de los Derechos Humanos[51], a la definición de los Planes Estratégicos de las Fuerzas y Cuerpos de Seguridad del Estado y otros específicos como el Plan de Responsabilidad Social Corporativa de la Policía Nacional[52], que permiten una verdadera multiplicación de las dimensiones vinculadas a la seguridad.

No obstante, algunos autores como el profesor Sansó-Rubert, se muestran cautos ante el verdadero alcance de los ODS ante la posibilidad de que:

> "[…] pasen a engrosar el cúmulo de textos bienintencionados destinados a permanecer inactuados por la omisión de la voluntad política. Resulta crucial abogar por su efectiva materialización, si de verdad se pretende que ejerzan su poder como escudo constitucional frente al lawfare y la manipulación informativa. Ahora es el tiempo de los hechos, no de las palabras. *Facta non verba*." (SANSÓ-RUBERT PASCUAL, 2024, pág. 133).

1.4. Conclusiones: el estado de salud de los conceptos de soberanía y seguridad en la Era Digital

Debemos comenzar esta reflexión señalando que la visión de la *seguridad humana* que lidera NNUU desde el año 1994 y que, por su propia concepción, afecta a la dimensión estatocéntrica de la seguridad westfaliana, lejos de suponer una amenaza a la soberanía del Estado lo que consigue es, precisamente, complementarla para que se adapte a la lógica evolución de los tiempos. En este sentido, la Asamblea General de NNUU señala en su Resolución 66/290 de 2012 que la seguridad humana "se basa en la implicación nacional" y que "no sustituye a la seguridad del Estado"[53], reconociendo al mismo tiempo "el pleno respeto a la soberanía de los Estados, la integridad territorial y la no

[51] Instrucción 1/2022, de 10 de febrero, de la Secretaría de Estado de Seguridad, por la que se crea la *Oficina Nacional de Garantía de los Derechos Humanos*.

[52] Resolución de 18 de septiembre de 2023 de la Dirección General de la Policía por la que se aprueba el *Plan de Responsabilidad Social Corporativa de la Policía Nacional*. Publicada en la Orden General de la Dirección General de la Policía número 2674, de fecha 18 de septiembre de 2023.

[53] Resolución aprobada por la Asamblea General el 10 de septiembre de 2012, A/RES/66/290, de 25 de octubre de 2012, sobre el *Seguimiento del párrafo 143, relativo a la seguridad humana, del Documento Final de la Cumbre Mundial de 2005*, página 2, considerando 3, epígrafes E y F. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/476/25/PDF/N1147625.pdf?OpenElement (02/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

injerencia en asuntos que son esencialmente de la jurisdicción interna de los Estados"[54], principios que son replicados exactamente en el Manual de Seguridad Humana de NNUU de enero de 2016[55].

No obstante, como hemos señalado anteriormente, a la sombra de fenómenos propios del siglo XXI como la globalización o la entrada en los ámbitos de influencia internacionales de poderes privados que restan atribuciones al Estado, el concepto de soberanía adquiere una naturaleza polifacética que abarca realidades diversas como la economía, la política, la tecnología o los derechos humanos, interconectadas a través de la relación entre poderes de distinto nivel, públicos y privados, que como fuerzas contrapuestas se equilibran. Como señala la profesora Álvarez Robles:

> "[…] esta tensión, que merma la eficacia estatal, lleva a contemplar lo supranacional como una respuesta viable. Los Estados, de manera individual, carecen de la capacidad necesaria para abordar y controlar los desafíos planteados por la globalización y la digitalización, optando por ceder parte de su soberanía a instituciones como la Unión Europea" (ÁLVAREZ ROBLES, 2024)

A ello hay que sumar el factor diferencial propio del siglo XXI, representado por la transformación digital de la sociedad, la evolución tecnológica y la particular infraestructura abierta y descentralizada de Internet que hace de los datos uno de los principales activos estratégicos mundiales, y que en conjunto conforman un entorno cibernético que desafía al concepto tradicional de soberanía poniendo en entredicho la vinculación entre el ciberespacio y la autoridad del Estado referida al territorio y a la población que lo ocupa.

Por esta razón, desarbolar estas teorías y reivindicar la aplicación de los conceptos de soberanía y seguridad no solo en el ámbito físico sino, también, en el digital, es la base de la actual política de seguridad europea que busca ser más fuerte y competente a través de su Política Común de Seguridad y Defensa, donde ocupa un lugar preferente el dominio y control de sus datos, siendo que "para los responsables políticos europeos, la idea de la soberanía digital forma parte de una lucha más amplia, a la que se enfrentan para mantener su capacidad de actuar y proteger a sus conciudadanos en un mundo de creciente competencia geopolítica"[56]. En línea con este planteamiento estratégico, los Estados miembros deben avanzar, a partir del ejercicio de la soberanía digital, en el gobierno de su propia esfera digital como garantía de salvaguarda de sus intereses y los de sus ciudadanos.

Para ello, la Unión necesita alcanzar la autonomía tecnológica y estratégica que le permita ejercer el liderazgo que pretende representar en la escena internacional, sincronizando al mismo tiempo la aplicación de sus valores democráticos, de cooperación multilateral y de respeto al Derecho Internacional que le confirmen como un proveedor de seguridad fiable y creíble para sus aliados y, lógicamente, a tener en

[54] IBIDEM, página 2 (epígrafe H).
[55] Manual de Seguridad Humana. Op. Cit.
[56] *La soberanía digital de Europa: de regulador a superpotencia en la era de la rivalidad entre EE.UU. y China*. Telefónica Digital Policy Lab. Página 7. Disponible en: https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/06/COLECCION-DE-ENSAYOS-FINAL.pdf (03/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

cuenta por sus competidores estratégicos. En ese sentido, el documento de la Comisión Europea titulado *Configurar el futuro digital de Europa* identifica como estratégicas las tecnologías referidas a la inteligencia artificial (IA), la Internet de las cosas (IoT), la tecnología cuántica, la ciberseguridad y las redes de comunicación 5G, entre otras, señalando que:

> "La soberanía tecnológica europea empieza por garantizar la integridad y la resiliencia de nuestra infraestructura de datos, redes y comunicaciones. Exige crear las condiciones adecuadas para que Europa se desarrolle y despliegue sus propias capacidades fundamentales, reduciendo así nuestra dependencia respecto de otras partes del mundo para las tecnologías más cruciales. Estas capacidades reforzarán la competencia europea para definir sus propias normas y valores en la era digital. La soberanía tecnológica europea no se define contra nadie, se centra en las necesidades de los europeos y del modelo social europeo. La UE permanecerá abierta a quien esté dispuesto a respetar las normas y a cumplir los estándares europeos, independientemente de su lugar de establecimiento"[57].

Pero no se pueden lanzar las campanas al vuelo porque queda mucho camino por recorrer, ya que en 2020 Europa aún "depende de empresas extranjeras para la mayor parte de su vida digital. La identidad digital de muchos ciudadanos europeos depende de direcciones de correo electrónico extranjeras; el 92 por ciento de los datos del mundo occidental se almacenan en EE.UU." (AMIOT, PALENCIA, BAENA, & DE POMMEROL, 2020). Las cifras indican que el esfuerzo a realizar para doblegarlas será intenso en dedicación y compromiso político, de amplio espectro en cuanto a la profundidad de los ámbitos afectados y de largo recorrido por su mantenimiento en el tiempo. Las políticas europeas de imponer un impuesto digital o multar a las grandes empresas tecnológicas estadounidenses por prácticas anticompetitivas reflejan la "creciente sensación de dependencia *neocolonial* de las compañías de Internet de EE.UU."[58].

Este empeño es el que justifica el esfuerzo coral de la Unión para avanzar a nivel mundial en la gobernanza de Internet, nuevo ámbito de carácter estratégico para el desarrollo de las sociedades democráticas que requiere de la soberanía digital como factor de seguridad y respeto a los derechos fundamentales de las personas, que se tratan de proteger mediante la coherencia normativa. En este mismo sentido se manifiesta el Presidente francés, Emmanuel Macron, en su discurso en La Sorbona el 25 de abril de 2024[59], señalando que Europa se ha percatado de que es en el ciberespacio donde se está librando una *batalla cultural y civilizatoria*, donde se juegan los valores y principios que sustentan nuestra democracia liberal en cuya defensa debemos comprometernos

[57] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Configurar el futuro digital de Europa*. Página 2. Bruselas, 19.2.2020. COM (2020) 67 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0067&from=en (05/02/2024).

[58] La soberanía digital de Europa: de regulador a superpotencia en la era de la rivalidad entre EE.UU. y China. Op. Cit., página 9.

[59] Discurso del Presidente de la República Francesa, en La Sorbona, el 25 de abril de 2024, titulado *Construir un nuevo paradigma europeo*. Disponible en: https://legrandcontinent.eu/es/2024/04/25/construir-un-nuevo-paradigma-el-discurso-completo-de-emmanuel-macron-en-la-sorbona/ (26/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

todos los europeos, día a día, puesto que la libertad y el Estado de derecho son conquistas que nunca debemos entender como hechos consumados.

En consonancia con este objetivo, el marco regulatorio digital europeo es avanzado e innovador a la vez que prolijo, y atiende a los diferentes planos que presenta esta realidad poliédrica que suponen las relaciones humanas a través de Internet, como por ejemplo:

1. La regulación y persecución de delitos en la Red conforme al Convenio de Budapest sobre la ciberdelincuencia de 2001 y sus posteriores Protocolos adicionales[60], o la propuesta en la que trabaja el Consejo UE para el mejor acceso a las pruebas electrónicas para combatir la ciberdelincuencia a través de un Reglamento sobre las órdenes europeas de entrega y conservación de este tipo de pruebas en los procesos penales[61].
2. La protección de datos personales de los ciudadanos a través del Reglamento General de Protección de Datos (RGPD)[62].
3. La gobernanza de datos no personales conforme a los valores y principios de la UE mediante la Ley Europea de Gobernanza de Datos (Data Governance Act)[63], o la regulación sobre quién puede utilizar y acceder a según qué tipo de datos y con qué fines, conforme a la Ley Europea de Datos (Data Act)[64].
4. El mercado único digital para eliminar barreras nacionales a las transacciones en línea y conseguir un espacio digital más seguro, innovador y equitativo a través

[60] El *Convenio de Budapest sobre la Ciberdelincuencia*, de 23 de noviembre de 2001, tiene por objeto la lucha contra los delitos cometidos mediante la utilización de tecnologías, tanto como objetivo del delito como herramienta para la comisión del mismo, o donde la tecnología sea el instrumento para mejorar la acción de otro, proporcionando orientaciones a los países firmantes para desarrollar su legislación penal sobre ciberdelincuencia y fomentar la cooperación internacional. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/convention-on-cybercrime.html (14/03/2024).

[61] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - Analysis of the final compromise text. Brussels, 20 January 2023. 5448/23. Disponible en: https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf (16/03/2024).

[62] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679 (14/03/2024).

[63] Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Ley de Gobernanza de Datos). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868 (14/03/2024).

[64] Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas sobre el acceso equitativo y el uso de datos y por el que se modifica el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Ley de Datos). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1704709568425 (14/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de la Ley de Servicios Digitales (DSA)[65] y la Ley del Mercado Digital (DMA)[66], o el Reglamento P2B[67] que promueve la equidad y la transparencia en la relación entre proveedores de servicios de intermediación en línea y las empresas que comercializan sus productos en Europa a través esas plataformas.

5. La identidad digital europea para conseguir un marco legal adecuado a las nuevas necesidades de empresas y ciudadanos en el marco de las transacciones en la Red con el Reglamento eIDAS2[68].
6. La seguridad de las redes y sistemas ante el riesgo cada vez mayor de ciberataques, mediante la Directiva NIS2[69] y la Ley de Resiliencia Operativa Digital (DORA)[70], que entra en vigor en 2025.
7. O la innovadora propuesta de Ley de Inteligencia Artificial (AI Act)[71], para la que el Consejo y el Parlamento Europeo alcanzan un acuerdo provisional en enero de 2024, con el objetivo de garantizar que los sistemas de IA que operen en la UE sean seguros y respeten los derechos de los ciudadanos, al tiempo que se estimula la inversión y la innovación en el mercado europeo.

Esta regulación digital que, a nivel mundial, lidera la UE es necesaria para avanzar en la autonomía tecnológica "si espera salvaguardar verdaderamente sus valores e intereses en el espacio digital, cosechar los beneficios económicos de las tecnologías digitales emergentes y mantener a los europeos a salvo de la desinformación y los ataques

---

[65] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). DOUE L 277/1, de 27 de octubre de 2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065 (14/03/2024).

[66] Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados competitivos y justos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Ley de Mercados Digitales). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A265%3ATOC&uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG (16/03/2024).

[67] Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Diario Oficial de la Unión Europea, 11.07.2019, L 186/57. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R1150 (08/02/2024).

[68] Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea. Bruselas, 3.6.2021. COM(2021) 281 final. 2021/0136(COD). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0281 (16/03/2024).

[69] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963 (16/03/2024).

[70] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962 (16/03/2024).

[71] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement. Brussels, 26 January 2024. 5662/24. Disponible en: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf (16/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

cibernéticos”[72]. Para conseguirlo hay que adaptar las herramientas disponibles de forma que este cuerpo normativo de la Unión sea capaz de conjugar la protección de los derechos de los consumidores y usuarios, sus derechos fundamentales y las libertades públicas con la seguridad nacional de los Estados miembros y la seguridad jurídica que necesitan para operar las empresas. Al mismo tiempo, este cuerpo normativo debe mantener vigente el derecho de competencia en el mercado y ofrecer mecanismos de gestión eficaz del ejercicio de las potestades públicas en el marco de gobernanza propio del ciberespacio. Y, además, todo ello debe lograrse sin caer en la trampa de la sobrerregulación, cuyo impacto podría afectar negativamente a la rentabilidad de las empresas y a su capacidad competitiva e innovadora, con efectos indeseados a su vez sobre el mercado y el papel de la Unión como actor protagonista en el actual contexto geopolítico internacional.

A partir de estas consideraciones, podemos concluir que es la necesidad de seguridad de las personas en todas las esferas de su vida la que, a lo largo de los tiempos y, principalmente, en el marco de las democracias actuales, permanece como una de las principales claves de legitimación de la soberanía del Estado, responsable de dar respuesta adaptada a la naturaleza cambiante de los desafíos y de proteger los derechos y libertades de los ciudadanos en cualquier ámbito de su realidad, tanto física como digital. Por ello, tanto la soberanía como la seguridad, obligadas por el nuevo entorno global y tecnológico que determina la evolución de los riesgos y amenazas, deben flexibilizarse para mantenerse activas como garantes del bienestar ciudadano, de su protección y de sus garantías de desarrollo, procurando vigencia al viejo aforismo latino *salus populi suprema lex.*

[72] La soberanía digital de Europa: de regulador a superpotencia en la era de la rivalidad entre EE.UU. y China. Op. Cit., página 62.

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 2. LA CONSTRUCCIÓN DEL CONCEPTO DE SEGURIDAD MULTIDIMENSIONAL: NACIONES UNIDAS Y LA ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE

Tras la catástrofe humanitaria que supuso la Primera Guerra Mundial los países occidentales, liderados por Estados Unidos, ven la necesidad de seguir avanzando en la fórmula para solucionar pacíficamente los conflictos y reducir el impacto de la guerra. Este modelo conciliador comenzó a elaborarse en las Conferencias de La Haya de 1899 y 1907 con la propuesta de métodos basados en la figura de la Corte Permanente de Arbitraje, los buenos oficios y la mediación. Consecuencia de esos diálogos, en junio de 1919 se firma el Tratado de Versalles, considerado como "un documento sobre un nuevo orden establecido en el mundo, mucho más que de un Tratado de paz" (DE AREILZA Y MARTÍNEZ DE RODAS, 1992, pág. 9).

Es relevante considerar que, en el Tratado de Versalles, se integra el Pacto de la Sociedad de las Naciones[73] como una organización internacional con la finalidad de "promover la cooperación internacional y lograr la paz y la seguridad internacionales por la aceptación de obligaciones de no recurrir a la guerra"[74]. Debemos señalar que la Sociedad de las Naciones (SDN) surge en un contexto viciado de origen por cuanto, en el marco del propio Tratado de Versalles, declara a Alemania causante de la contienda y le obliga al pago de más de ciento treinta mil millones de marcos de la época en concepto de reparaciones de guerra, al tiempo que establece una reducción de sus tropas y la confiscación de sus armas y buques, se apropia de sus colonias y, para mayor humillación, el acuerdo se firma en la Galería de los Espejos del Palacio de Versalles, lugar de proclamación del II Imperio Alemán.

Todo ello conduce al sentimiento generalizado de deshonra, a la insatisfacción y al dolor de herida mal cerrada con que el pueblo alemán interpreta Versalles, generando el caldo de cultivo en el que brota el nazismo y la consigna de revancha totalitaria que deviene en un nuevo conflicto de carácter global apenas unos años más tarde, la Segunda Guerra Mundial. Tras seis años de enfrentamiento, la contienda se vuelve a decantar en contra

[73] Los fundadores de la Sociedad de las Naciones son los 32 países firmantes del Tratado de Versalles, como beligerantes durante la Primera Guerra Mundial, y 13 países neutrales recogidos en el Anexo I del Tratado, entre los que se encuentra España. Posteriormente y hasta 1937, firmaron otros 21. A partir de 1946 la Sociedad de las Naciones deja de existir, entregando todos sus activos a las Naciones Unidas. Disponible en: https://www.un.org/es/about-us/history-of-the-un/predecessor (25/03/2024).

[74] El preámbulo del Pacto de la Liga de las Naciones comienza señalando que "las altas partes contratantes, con el fin de promover la cooperación internacional y lograr la paz y la seguridad internacionales, por la aceptación de obligaciones de no recurrir a la guerra, por la prescripción de relaciones abiertas, justas y honorables entre las naciones, por el establecimiento firme de los entendimientos del Derecho Internacional como la regla real de conducta entre los gobiernos, y por el mantenimiento de la justicia y el respeto escrupuloso de todas las obligaciones de los tratados en las relaciones de los pueblos organizados entre sí, aceptar este Pacto de la Sociedad de Naciones". Disponible en: https://www.iri.edu.ar/publicaciones_iri/manual/Doc.Naciones%20Unidas/Pacto%20de%20la%20Sociedad%20de%20las%20Naciones.pdf (25/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de los intereses de Alemania, que nuevamente se presenta como la gran derrotada frente a la Europa aliada, los EE.UU. y la URSS.

El cierre de la Segunda Guerra Mundial deja en evidencia dos claras situaciones de debilidad: por un lado, la europea, como resultado de la destrucción que conlleva el conflicto y, por otro, la del Derecho Internacional, fruto del fracaso del propio Tratado de Versalles. Consecuentemente, este escenario se traduce en el fin del protagonismo y el dominio ejercido hasta entonces por la vieja Europa, y en un nuevo reparto de la hegemonía y el poder entre las dos potencias ganadoras que ahora toman el relevo, basado en el delicado contrapeso de la amenaza nuclear.

Así, en los acuerdos de la Conferencia de Yalta celebrada en febrero de 1945, los EE.UU. y la URSS, con sus radicalmente opuestas concepciones ideológicas, se reparten su espacio de influencia tras la contienda. Stalin, aunque parte con un país muy debilitado por la guerra, goza de la legitimidad del vencedor que le sirve para, instrumentalizando la ideología comunista, extender su dominio político en los países de Europa del Este y la zona oriental de Alemania. Por su parte EE.UU., con una economía robustecida, ostenta el título de primera potencia mundial que ejerce con gusto el rol de árbitro sobre el terreno de juego.

Tratando de alejar la sombra del comunismo y de contrarrestar la política expansiva de la URSS a través de sus Estados satélites, la administración Truman despliega en 1947 el *Plan Marshall* para ayudar a levantarse a la Europa en ruinas que ha quedado y fortalecer aún más si cabe los lazos derivados del conflicto, contexto en el que se funda la Organización del Tratado del Atlántico Norte (OTAN). Como respuesta, el bloque del Este firma el Pacto de Varsovia en 1955, alzándose sobre el continente el Telón de Acero y dando comienzo la Guerra Fría.

Este orden internacional bipolar, de democracias ricas y de comunismo proletario, dota de sentido a ambas interpretaciones del mundo, otorga significado y contexto ideológico a disputas que verdaderamente nacen de otras causas que quedan maquilladas y ocultas, estratifica y ubica a todos los actores en escena para que sepan exactamente cuál es su papel dentro del guion y, en consecuencia, determina sus formas de dirigirse tanto interna como externamente. No hay espacio para otras interpretaciones fuera de esta trama férreamente dirigida por EE.UU. y la URSS. Claro ejemplo de ello es el corto recorrido que tiene la Comunidad Europea de Defensa (CED)[75], la cual:

> "In 1952, the EDC Treaty was adopted and then nothing. The end of the Korean War and the death of Stalin created a momentary thaw in the Cold War that removed the urgency in moving forward with the plan. In 1954, the EDC ended

[75] El Tratado constitutivo de la Comunidad Europea de Defensa se firmó en mayo de 1952 por los representantes de Francia, Bélgica, Países Bajos, Luxemburgo, Italia y Alemania (Occidental) pero no llegó siquiera a entrar en vigor porque la Asamblea Nacional francesa, en agosto de 1954, denegó su aprobación definitiva. Como consecuencia, y en la tranquilidad de la cobertura de la OTAN, la idea de la defensa autónoma europea va sufriendo diversos fracasos hasta el Consejo Europeo de Helsinki, celebrado en diciembre de 1999, donde se comienza a fraguar la Política Europea Común de Seguridad y Defensa.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> where it began when France, sharply divided over the idea of European defense, failed to ratify the Treaty" (PALACIO, 2020, pág. 9)[76].

Es este un orden sólido y absoluto que aprovechan tanto los EE.UU. como la URSS para consolidarse como auténticos imperios, en cuyo contexto tienen lugar acontecimientos de máxima relevancia histórica como la creación de las Naciones Unidas (NNUU) y la aprobación de la Carta de los Derechos Humanos, "que planteaba exigencias nunca antes acordadas internacionalmente para la convivencia humana" (OTTONE, 2017, pág. 35).

Tras este periodo de más de cuarenta años, el equilibrio del terror nuclear implosiona con la caída del Muro de Berlín y el desmoronamiento de la URSS, dando paso a un nuevo escenario unipolar que algunos altos dirigentes internacionales quisieron entender como un *nuevo orden mundial* que sería liderado por las NNUU con el apoyo de sus principales socios, y en especial por los EE.UU. mediante su abrumadora superioridad militar. En este sentido, el presidente George H. W. Bush a lo largo del año 1991:

> "[…] confirmó, en actos públicos, que existía, a su parecer, «un Nuevo Orden Mundial» y que la tarea histórica de los Estados Unidos era la de utilizar su considerable poderío castrense para defender ese orden «como un gendarme universal»" (DE AREILZA Y MARTÍNEZ DE RODAS, 1992, pág. 13).

No obstante, esta teoría pronto se reveló utópica ante la tozuda realidad de violencia que, en esos años, se materializó en las guerras del Golfo, de Croacia, de Bosnia o Chechenia, entre otras, y que llevaron a parte de la doctrina a considerar que el "nuevo orden mundial, se parece demasiado al viejo, aunque con un nuevo disfraz" (CHOMSKY, 1994, pág. 344).

Posteriormente, con el comienzo del nuevo siglo, se abre un complejo horizonte de competidores sistémicos que, superando la tradicional visión occidentalista, construyen sus argumentos de poder mirando hacia o desde la región Asia-Pacífico, reinterpretando el antiguo guion de la Guerra Fría por el que la seguridad exige un absoluto control universal, operado a través de las zonas de influencia que generan y el ejercicio de la disuasión desde la tecnología y la supremacía militar.

En el actual contexto internacional, agotado el modelo estatocéntrico que vincula la seguridad con la soberanía como valor supremo a defender frente a la amenaza exterior, la relación entre *seguridad* y *desarrollo* se constituye como principal eje vertebrador de las políticas de los Estados y, necesariamente, de las relaciones entre ellos. Estas, además, se enriquecen y complican al mismo tiempo como consecuencia de la legitimación de nuevos *actores no estatales* que defienden distintos intereses que obligan a abrir el foco de atención hacia riesgos y amenazas emergentes que, por su

[76] "En 1952, el Tratado CED fue adoptado y nada más. El fin de la Guerra de Corea y la muerte de Stalin propiciaron un deshielo momentáneo en la Guerra Fría que acabó con la urgencia de seguir adelante con el plan. En 1954, la CED terminó donde empezó cuando Francia, muy dividida sobre la idea de una defensa europea, no ratificó el Tratado" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

complejidad y conexión, superan la capacidad de respuesta individual de los propios Estados. Se generan nuevos espacios de relación en los que, de manera simultánea, operan con diferentes objetivos y voluntades instituciones privadas y públicas, de nivel local, nacional o supranacional. El Estado pasa a ser un actor más, aunque cualificado, de entre todos los *stakeholders* que confluyen en este nuevo escenario de gobernanza multinivel.

De esta manera, la comunidad internacional se desenvuelve en un intrincado y complejo sistema de relaciones que exige un enfoque mucho más amplio y colaborativo de las políticas de Estado en sus distintos planos. La seguridad ya no se entiende aislada, adquiriendo a partir de ahora una *vertiente multinivel* -por cuanto los conflictos no se supeditan al ámbito interestatal, sino también al intra y supraestatal- y *multidimensional* -desde la defensa de los derechos y libertades de los ciudadanos a su protección frente a las catástrofes naturales, pasando por la respuesta ante las variadas tipologías delictivas o la garantía de las condiciones de desarrollo humano- que exige respuestas coordinadas, cooperativas y contextualizadas para aportar soluciones holísticas a los nuevos desafíos que debe atender (VARGAS VILLAMIZAR, 2022, págs. 111-114).

Todo ello no hace sino confirmar la necesidad de apostar por el Derecho Internacional como clave de entendimiento y, a la larga, de subsistencia en una cada vez más subvertida escena mundial, donde estructuras como NNUU o la OTAN están obligadas a constituir opciones reales de acercamiento entre los opuestos.

2.1. La Organización de las Naciones Unidas

2.1.1. El periodo fundacional y la Guerra Fría (1945-1989)

"Nosotros los pueblos" es la frase que abre la Carta de las Naciones Unidas, firmada en San Francisco (EE.UU.) el 26 de junio de 1945 por cincuenta países y que, en sí misma, representa la exposición de motivos de este tratado internacional concebido como un foro de debate para promover la paz y la cooperación internacional a través de acuerdos multilaterales.

Partiendo del innegable legado de la SDN, algunos autores como Malone y Day, subrayan que:

> "[…] el diseño de las Naciones Unidas obedeció a la determinación de Franklin D. Roosevelt y Winston Churchill de impedir que se repitieran los errores del Tratado de Versalles de 1919, que había sido excesivamente punitivo con las potencias derrotadas en la Primera Guerra Mundial" (MALONE & DAY, 2021, pág. 590).

Nosotros nos inclinamos a pensar que, aun siendo ese un argumento de peso, el proyecto fue más bien la consecuencia de un serio intento por parte de EE.UU., como potencia líder del momento, y de Europa, como víctima desconcertada por su propia devastación, para tratar de construir un marco de actuación que permitiese consolidar la paz y la seguridad internacionales como instrumento para evitar que se pudiera reproducir otra conflagración como las acaecidas en la primera mitad del siglo XX.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Nos lleva a pensar así el Preámbulo de la Carta de San Francisco que, con redacción firme, muestra la resolución por preservar a las generaciones futuras de la guerra que por dos veces *ha infligido a la Humanidad sufrimientos indecibles*, institucionalizando la protección de todos sus miembros como iguales en su Asamblea General y la construcción de consensos como núcleo de las relaciones entre Estados. Esta cuestión se muestra principal y, de hecho, se mantiene como propósito en el ideario de sus miembros con el paso de los años, siendo así que:

> "In the world summit´s final declaration in 2005, all member states acknowledged their collective obligation to prevent or stop wide-spread human suffering where a state does not live up to its responsibility to protect its population" (MAYER & WEINLICH, 2007, pág. 46)[77].

Guiadas por esta noble aspiración y en el contexto de Guerra Fría soportada en el equilibrio de poderes bilateral del momento, las NNUU se marcan como propósitos el mantenimiento de la paz y la seguridad internacionales, el fomento de las relaciones de amistad desde la igualdad de derechos y la libre determinación de los pueblos, la cooperación internacional y el respeto a los derechos humanos y libertades fundamentales sin discriminación de ningún tipo, y la voluntad de armonizar los esfuerzos de todas las naciones para la consecución de tales objetivos conjuntos[78].

A continuación, en su vocación de piedra angular del Derecho Internacional, la Carta fija sus principios básicos[79] en torno a la igualdad soberana de todos sus miembros, la buena

[77] "En la declaración final de la Cumbre Mundial de 2005, todos los Estados miembros reconocieron su obligación colectiva de prevenir o detener el sufrimiento humano generalizado cuando un Estado no cumple con su responsabilidad de proteger a su población" (Traducción propia).

[78] Artículo 1 de la Carta de NNUU: "Los propósitos de las Naciones Unidas son: 1) Mantener la paz y la seguridad internacionales, y con tal fin: tomar medidas colectivas eficaces para prevenir y eliminar amenazas a la paz, y para suprimir actos de agresión u otros quebrantamientos de la paz; y lograr por medios pacíficos, y de conformidad con los principios de la justicia y del Derecho Internacional, el ajuste o arreglo de controversias o situaciones internacionales susceptibles de conducir a quebrantamientos de la paz; 2) Fomentar entre las naciones relaciones de amistad basadas en el respeto al principio de la igualdad de derechos y al de la libre determinación de los pueblos, y tomar otros medidas adecuadas para fortalecer la paz universal; 3) Realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión; y 4) Servir de centro que armonice los esfuerzos de las naciones por alcanzar estos propósitos comunes". Disponible en: https://www.un.org/es/about-us/un-charter (25/03/2024).

[79] Artículo 2 de la Carta de NNUU: "Para la realización de los Propósitos consignados en el Artículo 1, la Organización y sus Miembros procederán de acuerdo con los siguientes Principios: 1) La Organización está basada en el principio de la igualdad soberana de todos sus Miembros. 2) Los Miembros de la Organización, a fin de asegurarse los derechos y beneficios inherentes a su condición de tales, cumplirán de buena fe las obligaciones contraídas por ellos de conformidad con esta Carta. 3) Los Miembros de la Organización arreglarán sus controversias internacionales por medios pacíficos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia. 4) Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas. 5) Los Miembros de la Organización prestarán a ésta toda clase de ayuda en cualquier acción que ejerza de conformidad con esta Carta, y se abstendrán

Ediciones Universidad de Salamanca | CC BY-NC-ND

fe vinculada al *pacta sunt servanda*[80] consecuente con la adhesión a la misma[81], la recomendación a los Estados de resolver las controversias por medios pacíficos y la libre elección de estos medios basados en la confianza mutua[82], la proscripción de la amenaza o el uso de la fuerza contra otro Estado como hecho diferencial respecto a los Estados no firmantes, el compromiso de apoyo a la Organización como reflejo de los valores de la comunidad normativa y de seguridad que representa, la intención de universalidad de estos principios y el respecto a la jurisdicción interna de los Estados.

Algunos autores advierten que el "nuevo organismo internacional fue creado utilizando como base la coexistencia de dos principios políticos contrapuestos: uno denominado principio de *equilibrio*, y el otro, el principio de *supraordenación*" (ARGÉS, 2021, pág. 254). El primero enlaza con la existencia de los cinco miembros permanentes con *derecho a veto* en el Consejo de Seguridad[83] que, introducido por Stalin para no tener restricciones a su libertad de acción, no encuentra oposición en británicos y estadounidenses sino que, todo lo contrario, lo consideran la fórmula perfecta para mantener el consenso necesario en este *nuevo orden mundial* y que, sin embargo, se mantiene hoy día como una reminiscencia de aquel pretendido equilibrio entre las cinco grandes potencias del momento (ECHEVERRÍA JESÚS, 2019, pág. 65). El segundo de los principios, el de *supraordenación*, se vincula con la naturaleza representativa e

---

de dar ayuda a Estado alguno contra el cual la Organización estuviere ejerciendo acción preventiva o coercitiva. 6) La Organización hará que los Estados que no son Miembros de las Naciones Unidas se conduzcan de acuerdo con estos Principios en la medida que sea necesaria para mantener la paz y la seguridad internacionales. 7) Ninguna disposición de esta Carta autorizará a las Naciones Unidas a intervenir en los asuntos que son esencialmente de la jurisdicción interna de los Estados, ni obligará; a los Miembros a someter dichos asuntos a procedimientos de arreglo conforme a la presente Carta; pero este principio no se opone a la aplicación de las medidas coercitivas prescritas en el Capítulo VII".

[80] Pilar jurídico clave en el ámbito contractual por el que las partes se obligan a cumplir de buena fe con las condiciones y términos acordados entre ellos. Este principio del Derecho Civil tiene su transferencia al Derecho Internacional, en cuanto que los países firmantes de un Tratado o Convenio se obligan al cumplimiento de lo estipulado en ellos.

[81] Conforme al artículo 2.2, los Estados miembros están obligados a cumplir de buena fe las obligaciones que, en base a la firma de la Carta, asumen como forma de guiar sus relaciones internacionales. Al fin y al cabo, los pactos se firman para ser cumplidos y son ley entre las partes.

[82] El artículo 33.1 de la Carta de NNUU, relativo al arreglo pacífico de las controversias entre Estados, complementa al artículo 2.3 al establecer que "las partes en una controversia cuya continuación sea susceptible de poner en peligro el mantenimiento de la paz y la seguridad internacionales tratarán de buscarle solución, ante todo, mediante la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección".

[83] El artículo 24 de la Carta de NNUU establece que el Consejo de Seguridad es el responsable de mantener la paz y la seguridad internacionales, a cuyo fin se orientan sus resoluciones, de carácter vinculante para los estados firmantes, por lo que en caso de incumplimiento podrá aplicar medidas coercitivas como sanciones económicas, embargo de armas o acciones militares colectivas, entre otras.

Por su parte, el artículo 27.3 de la Carta de NNUU instaura el conocido como *derecho de veto* de los cinco Miembros Permanentes -EE.UU., Rusia, China, Francia y Reino Unido- al fijar las bases de votación en el Consejo de Seguridad: "1) Cada miembro del Consejo de Seguridad tendrá un voto. 2) Las decisiones del Consejo de Seguridad sobre cuestiones de procedimiento serán tomadas por el voto afirmativo de nueve miembros. 3) Las decisiones del Consejo de Seguridad sobre todas las demás cuestiones serán tomadas por el voto afirmativo de nueve miembros, incluso los votos afirmativos de todos los miembros permanentes; pero en las decisiones tomadas en virtud del Capítulo VI y del párrafo 3 del Artículo 52, la parte en una controversia se abstendrá de votar.

Ediciones Universidad de Salamanca | CC BY-NC-ND

igualitaria de la Asamblea General[84], donde cada Estado miembro tiene un voto. Nótese que nos estamos refiriendo a dos órganos distintos que funcionan de manera diferente: el restringido y cualificado Consejo de Seguridad en el primero de los supuestos, y la abierta e igualitaria Asamblea General en el segundo de los casos.

Una vez más se repite la historia y, como ocurre en Versalles, es evidente el sesgo occidental que imprimen los vencedores de la guerra trazando las líneas interpretativas de las relaciones entre sus miembros y, con ello, provocando efectos no deseados como, por ejemplo, la tan criticada inacción del Consejo de Seguridad derivada del ejercicio del derecho de veto que, aplicado por primera vez el 23 de febrero de 1946 por la URSS[85], se arrastra hasta hoy día (TORRES CAZORLA, 2008, pág. 67).

Aunque las NNUU comparten este rasgo de origen con su antecesora, la Sociedad de las Naciones, por cuanto son los vencedores los que definen el marco de las relaciones internacionales y ambas pretenden la cooperación internacional y la aceptación del no recurso a la guerra como forma de alcanzar la paz y la seguridad internacionales, debemos referirnos al principal hecho diferencial entre ellas, referido a que mientras que los artículos 12, 13 y 14 del Pacto de la Liga de las Naciones se refieren al compromiso de los Estados miembros de someterse a los mecanismos de arreglo pacífico de sus disputas pero consideran lícito el recurso a la guerra una vez intentado aquel[86], por el contrario, el artículo 2.4 de la Carta de San Francisco sí prohíbe tajantemente el recurso a la guerra (ECHEVERRÍA JESÚS, 2019, págs. 62-63).

Durante la Guerra Fría la interpretación de este compromiso de NNUU se centra en una visión clásica de la guerra con el objetivo final de impedir el choque violento entre Estados, para lo cual las misiones de paz despliegan fuerzas militares de reducidas dimensiones con el único propósito de patrullar y supervisar el cese del fuego, como forma de ayudar a los combatientes a resolver por ellos mismos el conflicto (BLANCO, 2014, pág. 268). Esta *definición negativa de la paz*, en cuanto no existencia de conflicto entre los dos bloques, configura el modelo de seguridad de las NNUU durante sus primeros años, y es consecuencia lógica de diversos factores como el principio de no intervención que consagra el artículo 2.7 de su Carta, la vigencia del concepto de

[84] El artículo 9.1 de la Carta de NNUU señala que "la Asamblea General estará integrada por todos los Miembros de las Naciones Unidas" y, en este sentido, el artículo 18.1 consagra que "cada Miembro de la Asamblea General tendrá un voto". La Asamblea General, conforme al artículo 10, se ocupa de todos los asuntos excepto de los relacionados con la paz y la seguridad -que son competencia del Consejo de Seguridad-, para lo cual emite resoluciones y declaraciones, ninguna de las cuáles son de obligado cumplimiento.

[85] El primer ejercicio del *derecho de veto* se llevó a efecto por la URSS en la 23ª reunión del Consejo de Seguridad, celebrada en Church House el sábado 16 de febrero de 1946, en el asunto referente a la retirada de tropas de Siria y Líbano. Puede consultarse el acta de dicha sesión en S/PV.23, disponible en: https://research.un.org/es/docs/sc/quick/meetings/1946 (26/03/2024).

[86] El artículo 12 del Pacto de la Liga de las Naciones establece que "los Miembros de la Liga acuerdan que, si surgiera entre ellos alguna disputa que pudiera conducir a una ruptura, someterán el asunto a arbitraje o arreglo judicial o a investigación del Consejo, y acuerdan en ningún caso recurrir a la guerra hasta tres meses después del laudo de los árbitros o de la decisión judicial, o del informe del Consejo. En cualquier caso, en virtud de este artículo, el laudo de los árbitros o la decisión judicial se hará dentro de un plazo razonable, y el informe del Consejo se hará dentro de los seis meses siguientes a la presentación de la controversia".

Ediciones Universidad de Salamanca | CC BY-NC-ND

soberanía asociada al Estado, la ausencia de regulación expresa de las operaciones de paz y, finalmente, el bipolarismo sustentado en la *doctrina de la destrucción mutua asegurada* (MAD)[87] de John von Neumann (MONTOYA BARREIROS, 2023).

Con estas reglas de juego y en un mundo dividido en dos bloques antagónicos que se contrarrestan mutuamente buscando el equilibrio de su poder, las NNUU se ven obligadas a adaptarse para tratar de ser eficaces en la consecución de su principal objetivo de garantizar la paz, así como superar los obstáculos que provocan cuestiones como el veto en el Consejo de Seguridad o los intereses soberanos como principal *leitmotiv* de los Estados nación. Todo ello obliga, por un lado, a que la Asamblea General desarrolle una participación más activa en el mantenimiento de la seguridad internacional y, por otro, a que el Secretario General asuma nuevas funciones deduciendo poderes implícitos de la Carta de San Francisco, permitiendo así enviar "contingentes de Naciones Unidas para vigilar el cese del fuego, treguas y separación de tropas" (MÉNDEZ CHANG, 2017, pág. 178).

2.1.2. El final de la Guerra Fría y la reordenación de los actores internacionales

Pero el cambio es factor permanente de evolución y, por lo tanto, de la Historia entendida como la "transformación direccional y coherente de las sociedades humanas que afecta a toda, o a casi toda, la humanidad" (FUKUYAMA, 2015, pág. 113), lo que nos da pie para afirmar que el año 1989 representa un auténtico hito en la historia que, incluso, tiene un carácter dual por cuanto, para unos, supone el prematuro final del siglo XX y, para otros, anuncia los primeros síntomas del nacimiento del siglo XXI. En cualquier caso, de entre las interpretaciones que se han hecho del fin de la Guerra Fría deben destacarse dos de ellas por su notoriedad e influencia, "una quizás atolondradamente optimista y otra excesivamente pesimista y alarmante" (OTTONE, 2017, pág. 46).

La primera de ellas corresponde a Francis Fukuyama que, en su artículo *¿El fin de la Historia?* publicado en 1989, meses antes de la caída del Muro de Berlín, advierte que:

> "Lo que podríamos estar presenciando no es simplemente el fin de la Guerra Fría o la desaparición de un determinado período de la historia de la postguerra, sino el fin de la historia como tal: esto es, el punto final de la evolución ideológica de la humanidad y la universalización de la democracia liberal occidental como la forma final de gobierno humano" (FUKUYAMA, 2015, pág. 57).

No significa esto que las guerras y los conflictos hayan desaparecido del horizonte para siempre sino que, conforme a la realidad de los hechos, con la derrota del fascismo en la Segunda Guerra Mundial y la caída del comunismo con la desaparición de la URSS en los años noventa, el sistema democrático liberal y capitalista se muestra como la mejor

[87] También conocida por sus siglas en inglés MAD -Mutually Assured Destruction-, que explica el equilibrio entre las dos potencias sistémicas de la Guerra Fría, EE.UU. y URSS, en base a la consideración de que ninguna de ellas se atrevería a lanzar un ataque nuclear porque tendría una respuesta igual o superior por parte de su antagónica, lo cual supondría la indudable destrucción de ambas, asumiendo dos presupuestos sobre el modo de actuar del adversario: que se regiría en sus decisiones por el modelo racional, y su deseo de supervivencia a la respuesta elegida.

Ediciones Universidad de Salamanca | CC BY-NC-ND

opción para organizar las sociedades. Por ello, se plantea como razonable la extensión de este patrón de gobierno ideológicamente atractivo y legítimo a todo el mundo. Ello es así porque:

> "[…] «al final de la historia no es necesario que todos los países se conviertan en sociedades liberales exitosas, basta simplemente con que pongan punto final a sus pretensiones ideológicas de representar formas diferentes y más elevadas de sociedad humana.» O dicho con otras palabras: «el fin de la Historia» no equivale a haber alcanzado un sistema perfecto, sino a la eliminación de alternativas mejores" (FUKUYAMA, 2015, págs. 29-30).

Y este modelo occidental es precisamente el que NNUU exporta en sus operaciones de paz que, en este nuevo contexto, adquieren protagonismo debido al sustancial incremento de las guerras civiles alimentadas por la retirada de las dos superpotencias rivales que, ahora, optan por reducir el gasto militar en zonas que pierden relevancia estratégica y cuyo vacío hace aflorar problemas larvados durante la anterior etapa (BLANCO, 2014, págs. 271-273), junto con el hecho de una mayor disposición y capacidad operativa de la Organización facilitadas por el consenso en el Consejo de Seguridad. Ejemplo de lo antedicho es que:

> "[…] the "demand" for new multilateral peace operations swelled at the end of the Cold War. Simultaneously, the United Nations and other international organizations were more willing and able to "supply" these new missions, and a new collegiality in the UN Security Council raised the possibility of reaching consensus (or at least avoiding vetoes) on proposals to deploy new operations to countries that were experiencing, or just recovering from, civil conflicts. The result of this combined growth in demand and supply was a sharp rise in the number of multilateral missions launched in the years immediately following the Cold War. In the decade from 1989 to 1999, the United Nations deployed thirty-three peace operations, more than double the fifteen missions that the organization conducted in the four preceding decades"[88] (PARIS, 2004, pág. 17).

La segunda de las interpretaciones más relevantes que se han hecho del fin de la Guerra Fría, menos optimista que la de Fukuyama, es la que en 1996 enuncia Samuel P. Huntington en su obra *El choque de las civilizaciones y la reconfiguración del orden mundial* en la que, partiendo de la consideración de los valores culturales y sus instituciones como elemento esencial de las sociedades humanas y de ineluctable referencia para comprender su evolución y desarrollo político, económico y social, juzga evidente que "la política global se está reconfigurando de acuerdo con criterios

[88] "La "demanda" de nuevas operaciones multilaterales de paz aumentó al final de la Guerra Fría. Al mismo tiempo, las Naciones Unidas y otras organizaciones internacionales estaban más dispuestas y capacitadas para "suministrar" estas nuevas misiones, y una nueva colegialidad en el Consejo de Seguridad de Naciones Unidas planteó la posibilidad de llegar a un consenso (o al menos evitar los vetos) sobre las propuestas para desplegar nuevas operaciones en países que estaban sufriendo, o simplemente se estaban recuperando, de conflictos civiles internos. El resultado de este crecimiento combinado de la demanda y la oferta fue un fuerte aumento en el número de misiones multilaterales lanzadas en los años inmediatamente posteriores a la Guerra Fría. En la década de 1989 a 1999, las NNUU desplegaron treinta y tres operaciones de paz, más del doble de las quince misiones que la organización llevó a cabo en las cuatro décadas anteriores" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

culturales. Los pueblos y los países con culturas semejantes se están uniendo. Los pueblos y países con culturas diferentes se están separando" (HUNTINGTON, 1997, pág. 147). Para Huntington, la civilización se entiende como una entidad cultural, la más amplia, con compromiso de permanencia y, al mismo tiempo, de evolución. En este sentido, sus principales exponentes son las civilizaciones china, la japonesa, la hindú, la islámica, la ortodoxa, la occidental, la latinoamericana y, posiblemente, la africana.

De ahí que los conflictos antes definidos por la confrontación ideológica entre superpotencias, ahora adquieran un *carácter intercivilizatorio* en base a las diferencias de civilización, distinguiendo entre conflictos *de línea de fractura*[89] y conflictos *de Estados Centrales*[90]. A partir de esta explicación, Huntington concluye que la existencia de conflictos en la historia humana, lejos de acabar, continuará con guerras que obedecerán al enfrentamiento entre culturas, siendo "probable que en el futuro los choques más peligrosos surjan de la interacción de la arrogancia occidental, la intolerancia islámica y la autoafirmación sínica" (HUNTINGTON, 1997, pág. 217).

En nuestra opinión, ni la visión extremadamente optimista de Fukuyama, que anima a concluir que:

> "[…] la democracia liberal y los mercados libres constituyen el mejor régimen o, más concretamente, la mejor alternativa de las disponibles para organizar las sociedades humanas" (FUKUYAMA, 2015, pág. 107).

ni tampoco la visión harto pesimista de Huntington, que le lleva incluso a suponer que:

> "[…] la intervención occidental en asuntos de otras civilizaciones es probablemente la fuente más peligrosa de inestabilidad y de conflicto potencial a escala planetaria en un mundo multicivilizatorio" (HUNTINGTON, 1997, pág. 374).

ofrecen una aproximación abierta y, mucho menos, flexible que permita entender el rol desempeñado por las NNUU a partir de los años noventa del pasado siglo. Entendemos que ninguna de las dos posturas responde al espíritu que anima a NNUU que, en comunión con la búsqueda kantiana de la paz perpetua como deber y "esperanza bien fundada mientras se le considere un ideal proyectado por la propia razón y al cual nos podemos acercar poco a poco, pero de manera constante" (SANTIAGO OROPEZA, 2004, pág. 10) trata, ahora sí, de construir una paz positiva a través de la consolidación de sociedades seguras y estructuras de gobierno responsables y comprometidas con los derechos humanos, la libertad y la dignidad de sus ciudadanos, abriendo así una nueva línea estratégica de acción que, progresivamente, sustituye el eje Oriente-Occidente por el eje Norte-Sur.

[89] Huntington entiende en su obra que los *conflictos de línea de fractura* son aquellos que, a pequeña escala, se producen entre Estados vecinos pertenecientes a civilizaciones diferentes; entre grupos de diferentes civilizaciones dentro de un mismo Estado; o entre grupos que están tratando de crear nuevos Estados a partir de otros anteriores.

[90] En cuanto a los *conflictos de Estados Centrales*, se producen entre Estados de diferentes civilizaciones por cuestiones de territorio, obtención de influencia, poder militar o económico, la movilización para la protección de compatriotas o la defensa de valores identitarios propios que, a modo de modernas cruzadas, legitiman la posesión de la verdad y la lucha por ella.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Para defender nuestra posición nos remitimos al informe *Un programa de paz. Diplomacia preventiva, establecimiento de la paz y mantenimiento de la paz*[91] que, en junio de 1992, presenta el Secretario General Boutros-Ghali. La relevancia de este informe se debe a que, en el mismo, finalizada la Guerra Fría, se vislumbra una nueva oportunidad para alcanzar los objetivos de las NNUU relativos no sólo a la paz y a la seguridad sino, también, de respeto a los derechos humanos, de progreso social y de nuevas dimensiones de libertad. Cierto es que, para su consecución, se requiere del impulso y compromiso de todos los Estados miembros, incluidos los de reciente incorporación. En el documento ya se habla de "una era de transición caracterizada por tendencias singularmente contradictorias", en la que aparecen asociaciones regionales como nuevas formas de cooperación y avanzan las comunicaciones y el comercio mundial trascendiendo las fronteras nacionales, mientras que los Estados se ven amenazados por luchas étnicas, religiosas, sociales, culturales o lingüísticas.

En este contexto, la Organización presenta cinco procedimientos para procurar la paz: 1) la prevención de los conflictos; 2) el establecimiento de medidas para resolver los problemas que ocasionan el conflicto; 3) la aplicación de actividades de mantenimiento de paz; 4) la consolidación de la paz a través de las instituciones e infraestructuras una vez acabado el conflicto; 5) y el ataque a las causas profundas de los conflictos en el plano económico, social y político.

Este nuevo *enfoque multidimensional* entiende que la *fragilidad de los Estados*, equivalente a instituciones y sistemas de gobernanza débiles, es un obstáculo para la consolidación de la paz, el desarrollo y la seguridad mundial. "Esta preocupación internacional respecto a la fragilidad del Estado se vuelve operativa por medio de la conceptualización de *Estados fallidos*" (BLANCO, 2014, pág. 293), definición que se relaciona directamente con la inestabilidad del Estado y la incapacidad para mantener y ejercer el monopolio del uso legítimo de la fuerza (ALONSO BERRIO, 2003, pág. 199), todo ello vinculado con los principales focos de inseguridad internacional, esto es, el terrorismo, el crimen organizado, el tráfico de armas, los movimientos insurgentes, la pobreza y el subdesarrollo.

Dichos *Estados fallidos,* y las situaciones de ellos derivadas, dan lugar a intervenciones internacionales -mayormente de carácter Occidental- ligadas a la pretendida construcción de estructuras de gobierno sustentadas en el dominio del territorio, la protección de su población y la exclusividad del uso de la fuerza que, con el tiempo, sean capaces de ejercer liderazgos responsables y legitimados socialmente para corregir así desigualdades, impulsar la justicia y recuperar el desarrollo. Todo lo cual, partiendo de que no es empresa fácil, saca a colación de nuevo la contrargumentación ética y política basada en que la traslación de modelos, sin atender a la identidad cultural -idioma, historia, religión, valores, memoria, etc.-, puede incluso agravar el problema que se trata

[91] Un programa de paz. Diplomacia preventiva, establecimiento de la paz y mantenimiento de la paz. A/47/277 de 17 de junio de 1992, del cuadragésimo séptimo período de sesiones de la Asamblea general. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N92/259/64/PDF/N9225964.pdf?OpenElement (26/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de solucionar, siendo que "lo que para Occidente es universalismo, para el resto del mundo es imperialismo" (HUNTINGTON, 1997, pág. 218).

Simultáneamente, se va poniendo de relieve que en esta empresa pacificadora las NNUU se van encontrando de frente con las prioridades internas de las principales potencias –EE.UU., Rusia y la emergente China-, las cuales se desmarcan de las resoluciones de la Asamblea General siempre que les suponga alterar su *statu quo* en el marco de las relaciones políticas, económicas o estratégicas que tengan en su línea de acción. De esta manera, a la falta de carácter jurídico vinculante de las resoluciones de la Asamblea General, se une también el colapso del Consejo de Seguridad y su evidente inacción por el bloqueo al que contribuye el *derecho de veto*.

Esta situación acaba generando una crisis de legitimidad (MALONE & DAY, 2021, págs. 585-587) auspiciada por las continuas guerras, que dejan en evidencia la irrelevancia de NNUU, y episodios como el ataque de EE.UU. a Irak en marzo de 2003 en contra del veto del Consejo, bajo "la consigna de una *guerra preventiva* en razón de la *inminente* amenaza que suponía la posesión de armas de destrucción masiva por parte del gobierno de Saddam Hussein" (MIRALLES CASTELLANOS, 2003, pág. 201). Esta agresión estadounidense se justificó forzando la interpretación del *derecho de legítima defensa* que consagra el artículo 51 de la Carta de NNUU[92] en caso de ataque armado a un Estado miembro, y dejó patente la falta de poder ejecutivo sobre el terreno de la Organización para preservar la paz y seguridad internacionales.

No obstante, mientras el pilar de paz y seguridad sufre esos reveses, la acción para el desarrollo económico y social es administrado, entre otras, a través de agencias son sólida reputación como el *Fondo de las Naciones Unidas para la Infancia* (UNICEF)[93] o la *Organización Mundial para la Salud* (OMS)[94]. Este frente toma impulso en el año 1999 con el *Pacto Global de NNUU*, que supone un llamamiento a la responsabilidad social de las empresas para incorporar los principios universales relacionados con los derechos humanos, las relaciones laborales, el medio ambiente y la lucha contra la corrupción en sus estrategias y procedimientos corporativos, alineándose con los objetivos de NNUU para generar un impacto global en el mercado que vincule el desarrollo de las empresas con el de las sociedades y, a través de ello, logre una adecuada redistribución de la riqueza (GÓMEZ PATIÑO, 2011, págs. 227-228).

[92] El artículo 51 de la Carta de NNUU acuerda que "ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales".

[93] Fondo de las Naciones Unidas para la Infancia (UNICEF). Disponible en: https://www.unicef.org/es (02/11/2023).

[94] Organización Mundial para la Salud (OMS). Disponible en: https://www.who.int/es/ (02/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Posteriormente, en el año 2000, NNUU presenta los *Objetivos de Desarrollo del Milenio*[95], con un enfoque novedoso frente al cambio climático y la degradación medioambiental, que son extendidos en el 2015 por la *Agenda 2030 para el Desarrollo Sostenible*[96]. No obstante, también en este frente ha habido contratiempos, como la retirada del gobierno estadounidense durante el mandato del presidente Trump del *Tratado de París* de diciembre de 2015[97], con lógica afectación a la necesaria solidaridad internacional para financiar el programa que trata de limitar el calentamiento mundial por debajo de 2 grados centígrados en el siglo XXI. No obstante, cabe concluir que en esta etapa se refuerza el segundo pilar sobre el que se sustenta la Organización, esto es, el compromiso con los derechos humanos desde una perspectiva social, prestacional y asistencial.

2.1.3. Balance y situación actual tras 75 años de Naciones Unidas: ¿realidad o ficción de su rol como árbitro de la seguridad internacional?

En el año 2020, paradójicamente cuando la pandemia del COVID-19 desafía al mundo con un brote de enfermedad y muerte que, además, conlleva una recesión económica generalizada y un replanteamiento del modelo global de distribución y suministro de recursos, se conmemora el 75º aniversario de las Naciones Unidas con una Declaración *ad hoc* de su Asamblea General[98].

La Declaración sobre la conmemoración del 75º aniversario de las Naciones Unidas pone de manifiesto la importancia de la Carta de San Francisco firmada en 1945, por cuanto se trata del:

> "[…] acuerdo internacional más importante del sistema internacional, no solo porque la gran mayoría de los Estados internacionalmente reconocidos lo han ratificado, sino porque articula a la única organización internacional con pretensión de universalidad y con mayor rango de alcance en referencia a los temas frente a los que se manifiesta" (ARRIETA-LÓPEZ, 2022, págs. 525-526).

En esta Declaración, en su primer punto, se pone el acento sobre cuestiones capitales para la Organización, refiriéndose a la legitimidad, el poder de convocatoria, el impacto

---

[95] Puede consultarse la documentación de NNUU, sobre los *Objetivos de Desarrollo del Milenio*. Disponible en: https://research.un.org/es/docs/dev/2000-2015 (02/11/2023).

[96] Puede consultarse en la página web oficial de NNUU. Disponible en: https://www.un.org/sustainabledevelopment/es/2015/09/la-asamblea-general-adopta-la-agenda-2030-para-el-desarrollo-sostenible/ (05/11/2023).

[97] El *Acuerdo de París*, firmado en diciembre de 2015 en la Conferencia de las NNUU sobre el Cambio Climático (COP21), establece objetivos a largo plazo: 1) reducir las emisiones de gases de efecto invernadero para limitar el aumento de la temperatura global en este siglo a 2 grados centígrados; 2) revisar los compromisos de los países cada cinco años; 3) ofrecer financiación a los países en desarrollo para que puedan mitigar el cambio climático, fortalecer la resiliencia y mejorar su capacidad de adaptación a los impactos del cambio climático. Disponible en: https://unfccc.int/sites/default/files/spanish_paris_agreement.pdf (03/11/2023).

[98] Resolución de la Asamblea General de 21 de septiembre de 2020 (A/75/L.1), aprobando la Declaración sobre la conmemoración del 75º aniversario de las Naciones Unidas. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/248/84/PDF/N2024884.pdf?OpenElement (27/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

normativo y la generación de esperanza para alcanzar el futuro de paz, desarrollo y derechos que la humanidad pretende y que las NNUU representan en su esencia.

Desde la consideración del origen de las NNUU y las oportunidades y desafíos con los que ha tenido que contender a lo largo de su historia, se plantea un futuro que pasa por afrontar, ya en el presente, una serie de retos como las ciberamenazas, el terrorismo internacional o el cambio climático. Estos desafíos, llegados de la mano del proceso globalizador e impulsados en ocasiones por el factor tecnológico-digital, exigen un *enfoque de seguridad multinivel y multidimensional* que involucre al amplio catálogo de actores interesados entre los que aparecen, junto a los Estados, las estructuras políticas supranacionales, las organizaciones no gubernamentales, las asociaciones civiles, el sector privado y otros *stakeholders* representativos de los intereses sociales que, en este entorno de gobernanza, a través de sus tramas de poder e influencia, ejercen presión para incluir en las agendas -políticas y normativas, nacionales, inter y supranacionales- temas como los ya mencionados del clima y el medio ambiente, los derechos humanos y la pobreza, la demografía y las migraciones o el impacto de la tecnología y las nuevas amenazas de ella derivadas. Este ecosistema de intereses, no siempre coincidentes, obliga a compensar constantemente el régimen de contrapesos de la política internacional, labor que las NNUU deben liderar en su rol de institución multilateral orientada a la construcción de consensos frente a estos nuevos retos (MIRALLES CASTELLANOS, 2003, pág. 206).

La realidad de la Organización hoy día, tras casi ochenta años de existencia y de tres de guerra en Ucrania por la invasión rusa del 24 de febrero de 2022, junto con otros viejos conflictos como el palestino israelí, donde el tiempo, lejos de actuar como bálsamo, recrudece el enfrentamiento, presenta aristas cortantes que son analizadas por la doctrina. En este sentido, debemos remitirnos por la claridad y acierto de su propuesta al profesor Xavier Pons Rafols quien, con ocasión de la invasión rusa de Ucrania, presenta cinco *certezas sistémicas insostenibles* en un pretendido entorno de relaciones internacionales pacífico y seguro, que es el principal objetivo de las NNUU.

La primera de estas certezas es el limitado compromiso de los Estados con el Derecho Internacional, cuestión que prueban hechos como, por ejemplo, el acto de agresión perpetrado por Rusia contra Ucrania en febrero de 2022, que pone de relieve:

> "[…] las deficiencias del sistema de seguridad colectiva instituido en la Carta de las Naciones Unidas y de la inexistencia de mecanismos eficaces de uso institucionalizado de la coerción en el Derecho Internacional" (PONS RAFOLS, 2022, pág. 8).

Otra prueba palmaria lo representa el conflicto palestino israelí iniciado como consecuencia de los criminales ataques de Hamás a Israel el 7 de octubre de 2023[99], que supone la muerte de miles de civiles y decenas de miles de desplazados sin recursos ni

[99] Puede consultarse la relevancia de este evento en la prensa internacional. Disponible en: https://www.bbc.com/mundo/articles/c25qq42xll8o#:~:text=Todo%20comenz%C3%B3%20el%20pasado%207,secuestrando%20a%20m%C3%A1s%20de%20200 https://elpais.com/internacional/2023-10-24/guerra-entre-israel-y-gaza-en-directo.html (30/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

suministros básicos para sobrevivir en un territorio, el palestino, intensamente bombardeado en sus calles, hospitales e infraestructuras junto con un férreo bloqueo de sus fronteras que impide el acceso de la ayuda humanitaria. Esta situación induce a las NNUU a aprobar una resolución no vinculante[100] pidiendo una tregua en la Franja de Gaza, exigiendo que ambas partes cumplan el Derecho Internacional Humanitario para facilitar el suministro de ayuda y la liberación de los rehenes civiles, lo cual, lejos de suponer un punto de encuentro que facilite la desescalada del conflicto, conlleva una respuesta de rotundo rechazo de Israel, apoyado por EE.UU., y el inicio de la operación militar terrestre en Gaza[101] como expresión de su derecho de autodefensa, al mismo tiempo que su embajador ante NNUU hace declaraciones considerándola una organización "rota y moralmente corrupta"[102].

Dos meses después, ante la evidencia de una crisis humanitaria flagrante, el Secretario General de NNUU, António Guterres, de nuevo apela a la responsabilidad de la comunidad internacional para poner fin a la crisis e invoca el artículo 99 de la Carta mediante un escrito dirigido al Presidente del Consejo de Seguridad[103], en el que reitera su llamamiento para que se declare urgentemente un alto el fuego que permita restablecer los medios de supervivencia y la entrega de asistencia humanitaria. Una vez más la comunidad internacional se autosabotea, de forma que el conflicto se mantiene con igual virulencia y los EE.UU. vuelven a aplicar su *derecho de veto* en el Consejo de Seguridad[104] a dos días de la celebración del 75º aniversario de la Declaración Universal de los Derechos Humanos bajo el lema "dignidad, libertad y justicia para todas las personas"[105]. Habrá que esperar hasta el 25 de marzo de 2024 para que el Consejo de Seguridad de NNUU, tras varios intentos fracasados por el veto de alguno de los países cualificados, consiga aprobar la Resolución 2728 de alto el fuego durante el mes del Ramadán[106]. Posteriormente el conflicto en la Franja de Gaza se reanuda hasta el alto el

[100] El proyecto de Resolución 23-20614 (S) - A/ES-10/L.25, para la protección de los civiles y cumplimiento de las obligaciones jurídicas y humanitarias, por las medidas ilegales israelíes en la Jerusalén Oriental Ocupada y el resto del Territorio Palestino Ocupado, es aprobada el 26 de octubre de 2023 con 120 votos a favor, 14 en contra y 45 abstenciones, evidenciando el enfrentamiento de posturas de los miembros del Consejo de Seguridad y el resto de miembros de la comunidad internacional, entre ellos los propios de la UE que no consiguen mostrar una postura común. Puede consultarse en la página web de NNUU. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/319/23/PDF/N2331923.pdf?OpenElement (30/10/2023).

[101] Disponible en https://www.bbc.com/mundo/articles/cv20yw3427qo https://efe.com/mundo/2023-10-28/la-asamblea-general-de-la-onu-vota-resolucion-arabe-para-frenar-la-guerra-en-gaza/ (30/10/2023).

[102] Disponible en: https://efe.com/mundo/2023-10-26/israel-vuelve-a-atacar-a-la-onu-como-una-organizacion-rota-y-moralmente-corrupta/ https://www.elperiodico.com/es/internacional/20231026/israel-ataca-onu-tacha-rota-93851208 (30/10/2023).

[103] Disponible en: https://unric.org/es/guterres-invoca-el-articulo-99-al-consejo-de-seguridad/ (10/12/2023).

[104] Disponible en: https://news.un.org/es/story/2023/12/1526302 (10/12/2023).

[105] Disponible en: https://www.un.org/es/observances/human-rights-day (10/12/2023).

[106] Resolución 2728 (2024), aprobada por el Consejo de Seguridad en su 9586ª sesión, celebrada el 25 de marzo de 2024. S/RES/2728 (2024). Disponible en: https://www.un.org/securitycouncil/es/content/resoluciones-aprobadas-por-el-consejo-de-seguridad-de-las-naciones-unidas-en-2024 (01/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

fuego acordado por Israel y Hamás el 15 de enero de 2025, a instancia de EE.UU., Qatar y Egipto, que actúan como mediadores[107].

Pero no es sólo el conflicto palestino israelí y la falta de voluntad de las partes por cumplir el Derecho Internacional Humanitario lo que señala la precariedad sistémica del modelo actual de NNUU, sino la propia interpretación jurídica que EE.UU., uno de los países fundadores de la Organización, pretende hacer en este caso de la Resolución 2728, adoptada por ese mismo Consejo de Seguridad del que forma parte de manera permanente como miembro con *derecho de veto*, y en cuya votación se abstiene para no comprometer más de lo necesario su alianza con Israel. Así, EE.UU. considera la resolución *no vinculante*[108], haciendo una interpretación torticera del artículo 25 de la Carta de las Naciones Unidas, que estipula que "los Miembros de las Naciones Unidas convienen en aceptar y cumplir las decisiones del Consejo de Seguridad de acuerdo con esta Carta", razón por la que sus resoluciones son obligatorias para todos los Estados que integran la Organización, dado que competen a la paz y la seguridad internacionales. Tratar de torcer el brazo a las resoluciones de NNUU, ignorando el pilar jurídico que construye el artículo 38 del Estatuto de la Corte Internacional de Justica[109], es una evidencia más del limitado compromiso de los Estados con el Derecho Internacional y, por ende, con las NNUU.

Para concluir este apartado sobre la falta de compromiso de algunos Estados con el Derecho Internacional, referir el varapalo por parte de Mongolia a la Corte Penal Internacional al incumplir sus obligaciones como firmante del Estatuto de Roma haciendo caso omiso, con ocasión de la visita oficial de Vladimir Putin a su territorio el 2 de septiembre de 2024, a la orden de detención internacional que pesa sobre el Presidente ruso desde marzo de 2023[110] dejando así en evidencia, una vez más, la

---

En esta resolución, de carácter vinculante, que se aprueba con 14 votos a favor y la abstención de EEUU, se exige el alto el fuego inmediato durante el mes del Ramadán, la liberación inmediata e incondicional de todos los rehenes, garantizar el acceso de la ayuda humanitaria a la Franja y que las partes se avengan a cumplir con el Derecho Internacional. Puede consultarse la nota de prensa de NNUU en la página web oficial https://news.un.org/es/story/2024/03/1528586 (26/03/2024).

[107] Puede consultarse esta noticia en prensa nacional e internacional. Disponible en: https://www.bbc.com/mundo/articles/c0e4494vjg5o
https://efe.com/mundo/2025-01-19/alto-el-fuego-gaza-israel/
https://elpais.com/internacional/2025-01-19/el-alto-el-fuego-en-gaza-en-directo.html (19/01/2025).

[108] Puede consultarse la polémica de estas declaraciones de la embajadora de EE.UU. ante NNUU, Linda Thomas-Greenfield, sobre la Resolución 2728 de alto el fuego en Gaza, en los medios de prensa. Disponible en: https://elpais.com/internacional/2024-03-29/ee-uu-provoca-una-polemica-en-la-onu-por-considerar-la-resolucion-de-alto-el-fuego-en-gaza-no-vinculante.html (01/04/2024).

[109] Las fuentes del Derecho Internacional que aplica la Corte son: los tratados, la costumbre, los principios generales del derecho, la doctrina, las decisiones judiciales y la equidad. Asimismo, se incorpora a esta pirámide normativa la legislación internacional.

[110] Las órdenes de detención emitidas por la Corte Penal Internacional sobre el presidente Putin, el exministro de Defensa ruso Serguéi Shoigú y el Jefe del Estado Mayor de las Fuerzas Armadas del Kremlin, Valeri Gerasimov, están activas desde marzo de 2023. La referencia en la prensa al incumplimiento por Mongolia de sus obligaciones internacionales tiene amplio recorrido. Disponible en: https://www.rtve.es/noticias/20240902/putin-llega-mongolia-riesgo-detenido-orden-corte-penal-internacional/16234199.shtml
https://www.eldiario.es/internacional/mongolia-recibe-putin-niega-detenerlo-pese-orden-corte-penal-internacional_1_11624716.html

Ediciones Universidad de Salamanca | CC BY-NC-ND

fragilidad del principio de legalidad en las relaciones entre Estados. No se trata solo de la evidente quiebra de ley, sino también del socavo de la autoridad de dicha institución y de sus repercusiones diplomáticas al más alto nivel por cuanto dicha omisión, en el contexto de la guerra de Ucrania, permite al Presidente ruso Vladimir Putin *mostrar músculo* al reunirse sin impedimento alguno con su homólogo mongol, Ukhnaa Khurelsukh, para concluir la firma de acuerdos que fortalecen los lazos económicos bilaterales y las relaciones energéticas trilaterales entre Rusia, Mongolia y China. Esta misma situación se repite con las visitas oficiales a EE.UU. y Hungría del Presidente israelí, Benjamín Netanyahu, con una orden de arresto en vigor emitida en noviembre de 2024 por la Corte Penal Internacional por presuntos crímenes de guerra y de lesa humanidad en la Franja de Gaza. Ni el ejecutivo de Donald Trump en febrero de 2025[111], ni el de Viktor Orbán en abril del mismo año[112], actúan conforme a lo acordado en el Estatuto de Roma, contribuyendo así a debilitar el Derecho Internacional y su visión de una justicia aplicable a todos los actores internacionales.

Agrava la situación, aún más si cabe, el tráfico de llamadas entre Washington y Moscú en marzo de 2025 para gestionar el posible acuerdo de paz para Ucrania[113]. De esta forma, el Presidente estadounidense Donald Trump, al mismo tiempo que excluye del ámbito negociador a Europa, acrecienta la posición de fuerza de Putin ante la sociedad internacional y da sustento al relato ruso justificador de la *operación militar especial* en Ucrania: *desnazificar* el territorio y socavar el apoyo al gobierno de Zelenski para que acepte una salida negociada al conflicto según los términos del Kremlin.

---

https://es.euronews.com/2024/09/02/putin-llega-a-mongolia-estado-miembro-de-la-corte-penal-internacional-sin-ser-detenido
https://www.france24.com/es/asia-pac%C3%ADfico/20240903-putin-es-bienvenido-y-con-honores-en-mongolia-a-pesar-de-la-orden-de-detenci%C3%B3n-de-la-cpi (05/09/2024).

[111] El respaldo internacional que esta visita a Donald Trump supone para el primer ministro israelí y la consecuente desacreditación para la Corte Penal Internacional, queda reflejada en los medios de comunicación de todo el mundo. Puede consultarse en: https://efe.com/mundo/2025-02-04/trump-netanyahu-apoyo-visita-eeuu/
https://www.elmundo.es/internacional/2025/02/06/67a4f8ab21efa01e2d8b4570.html (03/04/2025).

[112] El Gobierno húngaro no solo no hace efectiva la orden de detención internacional en vigor sobre Benjamín Netanyahu sino que, además, aprovecha la visita oficial del mandatario israelí para anunciar su intención de retirarse del Estatuto de Roma. Esta circunstancia tiene amplio seguimiento en la prensa nacional e internacional. Disponible en: https://www.rtve.es/noticias/20250403/hungria-anuncia-se-retira-corte-penal-internacional-tras-llegada-netanyahu/16519251.shtml
https://es.euronews.com/2025/04/03/hungria-abandona-la-corte-penal-internacional-en-un-gesto-de-apoyo-a-netanyahu-y-putin
https://cnnespanol.cnn.com/2025/04/03/mundo/hungria-anuncia-retirada-corte-penal-internacional-trax (03/04/2025).

[113] La llamada telefónica entre los presidentes de EE.UU. y la Federación de Rusia para abordar el futuro de la guerra en Ucrania, interpretada por la administración Trump como "el primer paso para la paz", tiene amplio seguimiento en prensa por sus evidentes implicaciones geoestratégicas en el orden internacional establecido. Puede consultarse en: https://www.france24.com/es/europa/20250319-qu%C3%A9-acordaron-trump-y-putin-en-su-llamada-sobre-el-futuro-de-la-paz-en-ucrania
https://www.bbc.com/mundo/articles/cz9n245x8peo
https://efe.com/mundo/2025-03-18/trump-putin-llamada-acuerdo-alto-el-fuego-ucrania/ (22/03/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

La siguiente certeza es la referida a la íntima relación entre la seguridad internacional, *variable objetiva*[114], y la percepción particular de cada Estado sobre su propia seguridad, *variable subjetiva*[115]. Esta dicotomía en el enfoque es frecuentemente utilizada, por ejemplo, desde Rusia por cuanto se siente excluida por parte de Occidente, temerosa por la expansión de la OTAN y, evidentemente, nostálgica de su pasado como superpotencia, lo que le lleva a la estrategia del *victimismo armado*[116] para utilizar la rusofobia como argumentario que justifica las políticas que está llevando a cabo el Kremlin desde hace más de una década en Europa, de la que la *operación especial* en Ucrania para combatir al centro del nazismo mundial es solo una muestra reciente[117].

Pero también recurren a este enfoque dual otros actores de igual peso en el Consejo de Seguridad de NNUU, como deja patente la reiterada oposición de EE.UU. a las resoluciones aprobadas por amplia mayoría en la Asamblea General solicitándole el fin del bloqueo económico a Cuba, en vigor desde los años sesenta del pasado siglo, y que supone una grave afectación a la libertad de comercio y navegación del país caribeño, con efectos directos en su economía[118]. Es decir, "la seguridad de unos no puede provocar la humillación y la inseguridad de otros, sino que, al contrario, no habrá seguridad para nadie hasta que no haya seguridad para todos" (PONS RAFOLS, 2022, pág. 13). Esta cuestión viene a resaltar el hecho de que el sistema de seguridad colectiva de las NNUU es asimétrico y poco representativo, siendo su Consejo de Seguridad el máximo exponente de esta debilidad.

Las servidumbres estructurales y la naturaleza instrumental de las NNUU conforman la tercera de las certezas insostenibles que apunta el profesor Xavier Pons Rafols, por la falta de ejecutividad de sus órganos y porque la efectividad de la Organización descansa sobre el Consejo de Seguridad, superado por el *derecho de veto* de sus cinco miembros permanentes[119], la falta de representatividad y la crisis de legitimidad que hacen

[114] Esta variable se mide en razón del número de delitos transnacionales y su afectación a la seguridad de los Estados, los conflictos tanto de carácter interno como internacional, las acciones insurgentes, el nivel de cumplimiento de los tratados y otras similares.

[115] La percepción que cada Estado tenga de cómo es su relación con el resto de la comunidad internacional en cuanto al respeto de sus postulados, sus decisiones o la interpretación de su propia acción diplomática configuran la variable subjetiva de la seguridad de un Estado.

[116] En este sentido es interesante el análisis de EUvsDisinfo donde define el victimismo armado como "una sensación de pérdida de poder y estima entre los grupos sociales que enfrentan desafíos a sus posiciones de estatus tradicionalmente privilegiados". Disponible en: https://euvsdisinfo.eu/the-kremlin-weaponising-victimhood/ (17/10/2023).

[117] La propia Embajada de Rusia en España publica el 8 de noviembre de 2023 este mensaje en su perfil de X. Disponible en: https://twitter.com/EmbajadaRusaES/status/1722218306906804393 (12/11/2023).

[118] Resolución A/77/L.5 de la Asamblea General de Naciones Unidas, sobre la necesidad de poner fin al bloqueo económico, comercial y financiero impuesto por los Estados Unidos de América contra Cuba, con 185 votos a favor, dos en contra (EE.UU. e Israel) y dos abstenciones (Ucrania y Brasil). Disponible en: https://news.un.org/es/story/2022/11/1516617 (12/11/2023).

[119] Las consecuencias del veto sobre la capacidad de NNUU para adoptar resoluciones y posicionarse como le corresponde en los conflictos queda una vez más evidenciada el 18 de octubre de 2023, en el marco del conflicto palestino-israelí con el veto de EE.UU. a la resolución que, auspiciada por Brasil, pretende una condena de los ataques de Hamás a Israel y acordar el alto el fuego para permitir la entrada de ayuda humanitaria a la Franja de Gaza. Una vez más la prensa mundial habla de bloqueo e inoperancia del órgano encargado de velar por la paz y la seguridad mundiales por el ejercicio del derecho de veto de alguno de sus cinco miembros permanentes. Disponible en: https://elpais.com/internacional/2023-10-18/el-veto-

Ediciones Universidad de Salamanca | CC BY-NC-ND

necesaria su reforma. Este órgano ejecutivo se configuró a mediados del siglo XX confiando en la hegemonía de los cinco grandes países del momento -EE.UU., China, Rusia, Francia y Reino Unido- que debían garantizar conjuntamente la paz mundial a cambio del *derecho de veto* en las decisiones del Consejo. Ese equilibrio de poder que legó la Segunda Guerra Mundial queda muy lejos del actual escenario internacional, en el que Francia y Reino Unido han perdido su liderazgo histórico, China está centrada en alcanzar la hegemonía económica y tecnológica sin intención alguna de erigirse como mediador de crisis ajenas mientras vigila celosa a Taiwán, Moscú se desgasta en conflictos territoriales con la aspiración de recuperar el pasado esplendoroso de la Gran Rusia y hace cálculos de fuerza frente a Europa, y EE.UU. se retrae en sí misma a la voz de *Make America Great Again*.

En contraposición, el sur global reclama más protagonismo a través de Estados emergentes como Brasil o Sudáfrica, muy activos en el seno de las NNUU como demuestran la tercera vía diplomática para propiciar una solución dialogada a la guerra de Ucrania[120] o la denuncia contra Israel por genocidio en Gaza[121], presentadas por ambos países respectivamente. A ello hay que sumar la cada vez mayor precariedad presupuestaria de la Organización que, no olvidemos, se financia con las cuotas[122] que abonan sus miembros -no siempre[123]-. No obstante, a pesar de todas estas deficiencias,

---

de-ee-uu-frustra-una-resolucion-para-un-alto-el-fuego-humanitario-en-el-consjeo-de-seguridad-de-la-onu.html
https://www.latimes.com/espanol/internacional/articulo/2023-10-18/EE.UU.-veta-resolucion-de-la-onu-que-condena-ataques-de-Hamás-a-israel-y-violencia-contra-civiles (30/10/2023).

[120] Sobre esta propuesta del Presidente Lula da Silva para la guerra de Ucrania puede consultarse la prensa. Disponible en: https://elpais.com/internacional/2023-02-02/brasil-plantea-una-tercera-via-para-propiciar-una-solucion-dialogada-a-la-guerra-de-ucrania.html
https://cnnespanol.cnn.com/2023/04/24/analisis-presidente-brasil-lanza-coalicion-paz-ucrania-camina-delgada-linea-trax/
https://www.swissinfo.ch/spa/economia/ha-llegado-el-momento-de-hablar-de-paz-en-ucrania/48850064 (02/03/2024).

[121] Sobre esta denuncia puede consultarse su tratamiento en NNUU y en prensa. Disponible en: https://unric.org/es/denuncia-sudafricana-contra-israel-por-genocidio-en-gaza/
https://efe.com/mundo/2024-01-11/denuncia-sudafrica-israel-genocidio-corte-internacional-de-justicia/
https://www.bbc.com/mundo/articles/czrl8zv388eo (02/03/2024).

[122] El presupuesto de NNUU, con el que se abordan desde las crisis humanitarias hasta las operaciones de mantenimiento de la paz o los programas de las Agencias como ACNUR o UNICEF, se financia mediante las cuotas de los Estados miembros, con arreglo a la escala de cuotas que determine la Asamblea General para el ejercicio presupuestario, que es de dos años de duración, tal y como se establece en el Artículo III *Cuotas y otros ingresos*, del Reglamento Financiero y Reglamentación Financiera Detallada de las Naciones Unidas, ST/SGB/2013/4, de 1 de julio de 2013. Si un país no paga sus cuotas pierde su voto en la Asamblea General. Disponible en: https://documents.un.org/doc/undoc/gen/n13/408/60/pdf/n1340860.pdf?token=bxdBD7qIsjh7YozNHV&fe=true (26/03/2024).

[123] En 2019, por ejemplo, el presupuesto de NNUU fue de 3.300 millones de euros, y en el último trimestre del año únicamente 129 de los 193 Estados miembros había ingresado su cuota, que depende del poder económico del país. EEUU es el país que más paga, aproximadamente el 22% del total del presupuesto de NNUU, pero debía aproximadamente 380 millones de dólares de presupuestos anteriores y 670 millones de dólares del ejercicio 2019. Otros países como Brasil, Irán, Israel, México, Corea del Sur, Arabia Saudita y Uruguay no habían pagado. Disponible en: https://news.un.org/es/story/2019/10/1463522
https://www.dw.com/es/la-onu-necesita-dinero-por-qu%C3%A9-sus-arcas-est%C3%A1n-vac%C3%ADas/a-50762944 (26/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

es el sistema de NNUU "el que acaba poniendo los recursos humanos, materiales o financieros para asistir a la población civil víctima de los conflictos y que actúa como conciencia crítica constante" (PONS RAFOLS, 2022, pág. 18).

La cuarta certeza insostenible que se deduce de la invasión rusa de Ucrania es la sempiterna y desigual lucha internacional contra el horror y la barbarie, y el "limitado progreso alcanzado en materia de respeto de los derechos humanos y del Derecho Internacional Humanitario en el contexto de un conflicto bélico" (PONS RAFOLS, 2022, pág. 20). El terror es recurrente y vuelve a verse en idéntica configuración unos meses después en el conflicto palestino israelí donde, desde el terreno, la Media Luna Roja, Equipos Médicos de Emergencia de la Organización Mundial de la Salud o Médicos Sin Fronteras llaman al cese de los bombardeos israelíes sobre centros hospitalarios de la Franja, mientras NNUU trata de evacuar a los heridos que necesitan tratamiento urgente y colapsan los escasos recursos disponibles[124]. En este sentido, se presentan informes de organizaciones independientes como *Acción Contra la Violencia Armada*[125] que constatan en el año 2023, con respecto al anterior, un aumento del 122% en las muertes de civiles a nivel global por causa de armas explosivas, cifras difíciles de asimilar que ponen de relieve:

> "[…] a major escalation in the use of explosive weapons globally, particularly in populated areas. The significant increases in both the frequency of these incidents and the resulting civilian casualties highlight a concerning trend in modern warfare. Israel's military operations, alongside ongoing conflicts in Ukraine, Sudan, Myanmar, and Syria, contributed to an unprecedented recent rise in civilian harm"[126].

La última de las certezas insostenibles que señala el profesor Pons Rafols se refiere al temor que produce el desarrollo armamentístico, y el hecho de que la posesión de un arsenal nuclear supone un desequilibrio de sobreprotección de esos Estados "que puede tener más imitadores, y que necesariamente debe mitigarse, reducirse y eliminarse para garantizar así la seguridad internacional" (PONS RAFOLS, 2022, pág. 29). Es evidente que ni el Tratado sobre la No Proliferación de las Armas Nucleares, firmado en 1968, ni el

---

[124] El ejército israelí fija como objetivo a los hospitales palestinos por considerar que son utilizados por Hamás como cobertura de sus instalaciones. Al quedar sin soporte de energía ni de agua los hospitales no pueden operar con normalidad, por lo que la ONU trata de evacuar tres hospitales de la zona norte de Gaza, entre ellos los de Al Shifa, el mayor de la Franja, y el de Al-Aqsa. Disponible en: https://news.un.org/es/story/2023/12/1526707 https://elpais.com/internacional/2023-11-21/la-onu-trata-de-evacuar-tres-hospitales-de-gaza-asediados-y-bombardeados-por-israel.html (25/01/2024).

[125] Acción Contra la Violencia Armada (Action On Armed Violence -AOAV) registra, investiga y difunde pruebas de violencia armada contra civiles en cualquier parte del mundo, con el objetivo de garantizar la protección de sus derechos humanos y tratar de poner fin a la violencia armada contra civiles en los conflictos. Puede consultarse su página web. Disponible en: www.aoav.org.uk (26/03/2024).

[126] Estas cifras "muestran una importante escalada en el uso de armas explosivas a nivel mundial, particularmente en áreas pobladas. Los aumentos significativos tanto en la frecuencia de estos incidentes como en las bajas civiles resultantes ponen de relieve una tendencia preocupante en la guerra moderna. Las operaciones militares de Israel, junto con los conflictos en curso en Ucrania, Sudán, Myanmar y Siria, contribuyeron a un reciente aumento sin precedentes de los daños civiles" (Traducción propia). Disponible en: https://aoav.org.uk/2024/2023-a-year-of-explosive-violence-harm-reviewed/ (03/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Memorándum de Budapest sobre Garantías de Seguridad, de 1994, han resultado efectivos. En febrero de 2023, prácticamente coincidiendo con el primer aniversario del comienzo de la guerra en Ucrania, Moscú anuncia la suspensión del Tratado de Reducción de Armas Estratégicas (START III).

A modo de conclusión respecto a las repercusiones de la guerra de Ucrania sobre la relevancia y el respeto internacional de NNUU, puede decirse que:

> "El problema de la ONU, en la actualidad, es el fantasma de la Sociedad de Naciones: un enfrentamiento con algunas de las grandes potencias no resolvería el problema de la guerra, pero podría poner en riesgo la supervivencia de la organización. Paradojas de las relaciones internacionales" (BAQUÉS QUESADA, 2022, pág. 34).

De manera que el panorama para contestar a la pregunta de si las NNUU actualmente lideran el multilateralismo y el consenso de los Estados en pro de la paz presenta un aspecto un tanto desolador, por no decir yermo. La tozuda realidad revela que el acatamiento y el respeto al Derecho Internacional y a las NNUU como su máxima valedora están claramente en entredicho. Por su parte, la propia Declaración conmemorativa del 75º aniversario reconoce decepciones a causa de las crecientes desigualdades en el mundo, la pobreza, el hambre, los conflictos armados, la inseguridad o el cambio climático, entre otras. También se muestra evidente que la modernización de los tres pilares de su estructura institucional es tarea principal y urgente, sobre todo del Consejo de Seguridad en cuyo interior se agrava la crisis de legitimidad alimentada por el pulso entre EE.UU., Rusia y China. Esta cuestión no escapa a los países miembros, entre los que se encuentra España, que claramente se refiere en su Estrategia de Seguridad Nacional 2021 a su papel de firme defensora del Derecho Internacional aunque "aboga por una revisión del sistema de las Naciones Unidas, eje central de la acción multilateral concertada para la prevención de conflictos, la acción humanitaria y la consecución de la paz, para lograr una organización más ágil y eficaz, adaptada a los desafíos mundiales actuales"[127].

Visto lo anterior, sin embargo, no sería acertado considerar que solo se cuentan momentos de desesperanza en el balance de NNUU, y debe ponerse en valor el impacto sustancial del esfuerzo que ha llevado a cabo la Organización en el ámbito humanitario durante todos estos años, de manera eficaz y al alza, a través de sus agencias de reconocido prestigio como la Organización de las Naciones Unidas para la Alimentación y la Agricultura (FAO), que lidera el esfuerzo internacional para poner fin al hambre tratando de alcanzar la seguridad alimentaria para todos, el Programa Mundial de Alimentos de las Naciones Unidas (WFP), para la asistencia en zonas postconflicto y víctimas de desastres naturales[128], o el Fondo de las Naciones Unidas para la Infancia (UNICEF), para la defensa de los derechos de la infancia y la ayuda a niñas y niños en países en desarrollo.

[127] Estrategia de Seguridad Nacional 2021. Op. Cit. Capítulo 4, página 96.

[128] LA WFP es la organización humanitaria más grande del mundo que salva vidas en emergencias y da asistencia alimentaria para construir un camino hacia la paz, la estabilidad y la prosperidad de poblaciones que se están recuperando de conflictos y desastres y del impacto del cambio climático. Disponible en: www.es.wfp.org/quienes-somos (12/07/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

No en vano, la Organización y su Secretario General Kofi Annan recibieron el Premio Nobel de la Paz en 2001 "por estar a la vanguardia de los esfuerzos por lograr la paz y la seguridad en el mundo y de la movilización internacional encaminada a hacer frente a los desafíos económicos, sociales y ambientales con que se enfrenta el mundo"[129], honor que repitieron por segunda vez en 2020, esta vez a través del *Programa Mundial de Alimentos* que recibió el Premio Nobel de la Paz "por sus esfuerzos para combatir el hambre, por su contribución a mejorar las condiciones de paz en las zonas afectadas por conflictos y por actuar como motor impulsor de los esfuerzos para prevenir el uso del hambre como arma de guerra y conflicto"[130].

En esta misma línea deben interpretarse los avances conseguidos en el compromiso de los Estados miembros con los graves problemas humanitarios que suponen la migración y el estatuto de los refugiados, a través del *Pacto Mundial para la Migración Segura, Ordenada y Regular*, de diciembre de 2018[131], que da forma al acuerdo para mejorar la cooperación sobre la migración internacional, en orden a que los desafíos y oportunidades que conlleva sean un factor de unión para la comunidad de Estados en vez de un motivo de división, y del *Pacto Mundial sobre los Refugiados*, también de diciembre de 2018, que representa la voluntad política basada en el reconocimiento de la necesidad de la cooperación internacional para dotar de un marco de protección y solidaridad a las personas refugiadas, sobre la base del reparto equitativo de cargas y responsabilidades derivadas entre los países de acogida afectados[132].

Semejante tarea ha sido liderada por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH)[133], desde su compromiso con la promoción y protección de los derechos y libertades consagrados en la Declaración Universal de Derechos Humanos y en el conjunto de tratados internacionales, con el objetivo de prestar asistencia técnica a Estados, coordinar programas de NNUU y mejorar la cooperación internacional en la materia, eliminar obstáculos para la realización de estos derechos y evitar la comisión de violaciones de los mismos, entre

[129] Mención del Comité Noruego del Nobel. Disponible en: https://www.un.org./es/about-us/nobel-peace-prize/kofi-annan-2001 (24/07/2023).
[130] Mención del Comité Noruego del Nobel. Disponible en: https://www.un.org/es/about-us/nobel-peace-prize/wfp-2020 (17/07/2023).
[131] Resolución de la Asamblea General de NNUU de 19 de diciembre de 2018 (73/195). Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/452/03/PDF/N1845203.pdf?OpenElement (18/07/2023).
[132] Resolución de la Asamblea General de 17 de diciembre de 2018 (73/151), en la que se establecen 4 objetivos clave: 1) aliviar las presiones sobre los países de acogida; 2) promover la autosuficiencia de los refugiados; 3) ampliar el acceso a las soluciones que impliquen a terceros países y 4) favorecer en los países de origen circunstancias que propicien un retorno en condiciones dignas y seguras. Disponible en: https://www.acnur.org/media/oficina-del-alto-comisionado-de-las-naciones-unidas-resolucion-aprobada-por-la-asamblea (20/07/2023).
[133] El Alto Comisionado para la promoción y la protección de todos los derechos humanos se crea por la Resolución de la Asamblea General 48/141, de 7 de enero de 1994 para desempeñar "su cometido en el marco de la Carta de las Naciones Unidas, la Declaración Universal de Derechos Humanos, otros instrumentos internacionales de derechos humanos y el Derecho Internacional". Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N94/012/59/PDF/N9401259.pdf?OpenElement (25/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

otros, aunque con desigual éxito en sus requerimientos, siendo una buena muestra de ello la reprobación por la ejecución programada para finales de enero de 2024 en el Estado de Alabama (EE.UU.) de un preso condenado a la pena capital, mediante el uso de un gas de nitrógeno que "podría constituir tortura u otro trato o castigo cruel, inhumano o degradante conforme a la normativa internacional de derechos humanos"[134], sentencia que finalmente se consuma el 25 de enero a pesar de las críticas y el rechazo internacional y la propia denuncia del ACNUDH por la crueldad del sistema aplicado[135].

Con todo, esta labor desempeñada por la Organización en sus más de 75 años de historia suma en su haber unos niveles sin precedentes de cooperación internacional en materia social, económica, política y de desarrollo que han desembocado en la toma de conciencia de que "el multilateralismo no es una opción, sino una necesidad en nuestra tarea de reconstruir para mejorar en pro de un mundo más igualitario, más resiliente y más sostenible"[136], desafíos que plantea el siglo XXI frente a los cuales pueden y deben estar las NNUU.

En este mismo sentido, otro de los desafíos que urge a medio y largo plazo es el derivado de un escenario medioambiental marcado por el cambio climático y el agravamiento de los fenómenos asociados que, consecuentemente, tendrán un impacto en la población mundial, con especial incidencia en los países menos desarrollados, generando así una demanda de asistencia humanitaria que contribuirá a tensionar el *statu quo* y el modo de vida actual por el requerimiento de más recursos dedicados, de manera más frecuente y con un soporte presupuestario adecuado para su mantenimiento. Solo una labor de concienciación universal asociada a una estrategia de acción resuelta, conjunta y coordinada por NNUU puede ofrecer garantía de éxito frente a este nuevo reto de la humanidad.

Y ese liderazgo a nivel global solo puede ser ejercido por la Organización porque, pese a todas las dificultades, debilidades, crisis y problemas, mayormente derivados de la actuación de los Estados que en ocasiones tratan de instrumentalizarla para su propio beneficio, sigue siendo un referente único en su especie, sin posible sustituto a fecha de hoy, del que solo cabe concluir que "resulta innegable que a lo largo de estos 75 años el mundo sin las Naciones Unidas habría sido mucho peor" (ANDRÉS SÁENZ DE SANTA MARÍA, 2021).

---

[134] Puede consultarse la nota de prensa de la Portavoz del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Ravina Shamdasani, sobre la ejecución del preso Kenneth Eugene Smith, condenado a muerte por el Estado de Alabama. Disponible en: https://www.ohchr.org/es/press-briefing-notes/2024/01/us-alarm-over-imminent-execution-alabama (25/01/2024).

[135] El Estado de Alabama llevó a cabo la ejecución de Kenneth Eugene Smith el 25 de enero de 2024, mediante el procedimiento de asfixia por nitrógeno, a pesar de la reprobación por parte de la opinión internacional y del ACNUDH. Disponible en: https://www.elmundo.es/internacional/2024/01/26/65b34be0fdddfff58e8b45db.html https://elpais.com/internacional/2024-01-26/alabama-mata-con-el-experimental-metodo-de-asfixia-con-nitrogeno-a-un-condenado-a-muerte-al-que-ya-trato-de-ejecutar-en-2022.html (26/01/2024).

[136] Esto es lo que concluye el punto 5 de la Declaración sobre la conmemoración del 75º aniversario de las Naciones Unidas, que comienza señalando que los desafíos actuales guardan relación entre sí y solo pueden afrontarse mediante un multilateralismo revitalizado.

Ediciones Universidad de Salamanca | CC BY-NC-ND

2.1.4. La aportación de Naciones Unidas a la ciberseguridad en el siglo XXI

Podemos decir que, en línea con su espíritu fundacional, el compromiso de NNUU con la ciberseguridad, entendida como "la protección de activos (tangibles e intangibles) y de usuarios frente a vulnerabilidades, amenazas y riesgos" (ÁLVAREZ ROBLES, 2024, págs. 257-258), busca ofrecer a los ciudadanos un entorno confiable y seguro donde quiera que vivan y cualesquiera que sean los medios de conexión que utilizan, desde una perspectiva integral, multidimensional, consensuada y descentralizada basada en la aplicación del Derecho Internacional y el profundo respeto a los derechos humanos.

En este sentido, el Consejo Económico y Social de las Naciones Unidas (ECOSOC)[137], a la sazón responsable de los asuntos económicos, sociales, culturales y de salud, así como de los derechos humanos y las libertades fundamentales, consciente ya en el año 2011 de este problema, celebra en Nueva York un evento sobre *Seguridad cibernética y desarrollo*[138] en cuyo discurso de clausura, su presidente Sr. Lazarous Kapambwe, señala que:

> "[…] la seguridad cibernética es un problema mundial que solo puede resolverse mediante la cooperación mundial. Afecta a todas nuestras organizaciones...y las Naciones Unidas mantienen la postura de emplear sus capacidades estratégicas y analíticas para dar respuesta a estos problemas"[139].

Sin duda, una de las cuestiones que más preocupan desde el principio es la *protección de los datos personales* en el mundo virtual, donde la tensión entre la seguridad nacional y la privacidad individual no siempre se solventa de manera adecuada en atención al tipo de régimen político que gobierne en cada lugar, siendo por ello una cuestión permanentemente presente en la agenda global de NNUU[140].

Este es el ánimo que inspira el mandato que se otorga al *Relator Especial sobre el derecho a la privacidad* en la Resolución del Consejo de Derechos Humanos 28/16 sobre el derecho a la privacidad en la era digital[141] con la finalidad de crear un entorno digital

---

[137] El Consejo Económico y Social está recogido en los artículos 61 a 72 de la Carta de las Naciones Unidas. Disponible en: https://research.un.org/es/docs/ecosoc (22/02/2024).

[138] Este evento se organizó con el fin de tratar los problemas y desafíos relacionados con la seguridad y el delito cibernéticos, en colaboración con la Unión Internacional de Telecomunicaciones (UIT). Su objetivo era triple: 1) concienciar en el ámbito de la política internacional presentando un panorama de la situación y de los desafíos respecto a la seguridad cibernética y sus vínculos con el desarrollo; 2) identificar las mejores iniciativas y prácticas para crear una cultura de ciberseguridad a todos los niveles; y 3) estudiar opciones para dar una respuesta coordinada e internacional al incremento del ciberdelitos de amplio espectro.

[139] Reseña de prensa oficial. Disponible en: https://www.un.org/es/desa/seguridad-cibernetica (18/02/2024).

[140] En este sentido puede consultarse la guía de estudio 2024 de la UNAV sobre la Comisión de Desarme y Seguridad Internacional. Disponible en: https://www.unav.edu/documents/5506181/0/guia-estudio-unoda-jr.pdf (22/02/2024).

[141] Resolución aprobada por el Consejo de Derechos Humanos 28/16. El derecho a la privacidad en la era digital. Asamblea General. A/HRC/RES/28/16. 1 de abril de 2015. Disponible en: https://documents.un.org/doc/undoc/gen/g15/068/81/pdf/g1506881.pdf?token=eXb0gJGhrPqnSyVKYd&fe=true (03/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

mundial más seguro[142], y que también orienta la Hoja de Ruta para la Cooperación Digital[143], en la que el Secretario General de NNUU asume el compromiso de la Organización en el liderazgo de iniciativas, la puesta en práctica de programas y el uso de mecanismos para avanzar globalmente en las capacidades digitales desde el respeto a los valores y principios de su Carta fundacional y el Derecho Internacional. En este sentido, como señala la profesora Álvarez Robles, NNUU trata de ir más allá en su compromiso como árbitro internacional que, con el objetivo de garantizar los derechos fundamentales y libertades humanas frente a las posibles conculcaciones por parte de los Estados, trasciende el ámbito físico para actuar en el digital desde la consideración de Internet como un bien público, común y global, "como un derecho instrumental conectado en origen con las libertades de expresión e información" (ÁLVAREZ ROBLES, 2023, pág. 76).

En segundo lugar, por lo que respecta al mantenimiento de la paz y la estabilidad y seguridad internacionales, en junio de 2021, el Consejo de Seguridad de Naciones Unidas celebra su primer debate de carácter público sobre el *mantenimiento de la paz y la seguridad en el ciberespacio*[144], concluyendo que el aumento de los índices de ciberataques de distinto formato[145] -campañas desinformativas, incidentes de denegación de servicio, interrupción de servicios en red, ataques a infraestructuras críticas- constituyen una amenaza global que restringe la confianza entre los países. Para contrarrestarla, tanto la Carta de las NNUU como el Derecho Internacional con sus principios jurídicos, entre los que se encuentra el reconocimiento de la soberanía de los Estados, apuestan por un marco en el que se reconoce que estos principios ideados en clave analógica son necesariamente aplicables en el ciberespacio para asegurar un comportamiento responsable, transparente, ético y legal de todos los actores intervinientes que coadyuve a proteger los derechos y libertades de las personas, y a mantener la paz y la seguridad.

---

[142] Puede consultarse la página oficial del Relator Especial sobre el derecho a la privacidad y su mandato en https://www.ohchr.org/es/special-procedures/sr-privacy (03/03/2024)

[143] Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital. Informe del Secretario General. Asamblea General. A/74/821. 29 de mayo de 2020. Disponible en: https://documents.un.org/doc/undoc/gen/n20/102/54/pdf/n2010254.pdf?token=MzAlFTNn7EzLLZ0wkk&fe=true (03/03/2024).

[144] Puede consultarse la nota de prensa de Naciones Unidas y la cobertura mediática. Disponible en: https://news.un.org/es/story/2021/06/1493862 https://www.france24.com/es/minuto-a-minuto/20210629-el-consejo-de-seguridad-de-la-onu-debate-sobre-ciberseguridad-una-preocupaci%C3%B3n-creciente https://protecdatalatam.com/noticias/ciberseguridad-el-consejo-de-seguridad-de-la-onu-inicia-su-primer-debate-formal-sobre-ciberseguridad/ (22/02/2024).

[145] La tensión estratégica actual con la guerra en Ucrania, el enfrentamiento israelí-palestino y la acusada inestabilidad en el Sahel, las crisis humanitarias derivadas de estos conflictos y el favorecimiento de tendencias radicales y terroristas, están causando efectos directos en la seguridad internacional y, también, en la propia de los Estados. En este sentido se pronuncia el Informe Anual de Seguridad Nacional 2023, del Departamento de Seguridad Nacional de España, en el que expresamente menciona como riesgos y amenazas a la seguridad nacional las campañas de desinformación, la vulnerabilidad del ciberespacio y las amenazas a las infraestructuras críticas. Disponible en: https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2023 (27/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

La implementación de estos principios generales del Derecho la vamos a encontrar, entre otras, en la *Agenda para el Desarme*, donde se incluye el desafío de las nuevas tecnologías emergentes vinculadas con el ciberespacio, creándose al efecto un *Grupo de Expertos Gubernamentales* (GEG) sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional y un *Grupo de Trabajo de Composición Abierta* (GTCA) sobre los avances en el campo de la información y telecomunicaciones en el contexto de la seguridad internacional[146].

En este sentido, en marzo de 2021 ese GTCA sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional[147], presenta su informe final con una serie de conclusiones y recomendaciones que gira en torno a tres ideas principales:

1. Las TIC pueden ser objeto de un uso malintencionado no compatible con los principios de paz, estabilidad y seguridad que desea la comunidad internacional, por lo que la defensa de estos intereses superiores requiere de un tratamiento conjunto para alcanzar respuestas eficaces, al amparo de las normas del Derecho Internacional y la Carta de las NNUU:

> "States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. In this regard, States were called upon to avoid and refrain from taking any measures not in accordance with international law, and in particular the Charter of the United Nations. States also concluded that further common understandings need to be developed on how international law applies to State use of ICTs"[148].

---

[146] En este sentido, en diciembre de 2011 la Asamblea General aprobó la resolución A/RES/66/24 sobre *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional* en la que se requiere a un Grupo de Expertos Gubernamentales para que lleven a cabo el seguimiento y estudio de los riesgos y amenazas en el ámbito de la información y las posibles medidas para hacerles frente. A partir de este momento se presentan a la Asamblea General una serie de informes anuales en los que se da cuenta del avance de la ciberamenaza y la utilización de las tecnologías de la información y las comunicaciones, así como su afectación a los derechos humanos, las libertades fundamentales y los principios del Derecho Internacional. Disponible en: https://disarmament.unoda.org/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/
https://documents.un.org/doc/undoc/gen/n11/460/29/pdf/n1146029.pdf?token=KNBRoMvxWIIp1PUtNA&fe=true (22/02/2024).

[147] Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. General Assembly. Conference room paper. A/AC.290/2021/CRP.2. Disponible en: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (29/02/2024).

[148] IBIDEM, Apartado 34.

"Los Estados reafirman que el Derecho Internacional, y en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad y promover un entorno TIC abierto, seguro, estable, accesible y pacífico. En este sentido, se pidió a los Estados que evitaran y se abstuvieran de adoptar medidas contrarias al Derecho Internacional, y en particular de las Carta de las NNUU. Los Estados también llegaron a la conclusión de que era necesario llegar a nuevos entendimientos comunes sobre la forma de aplicar el Derecho Internacional a la utilización de las TIC por parte de los Estados" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

2. La clave para fomentar la confianza y la estabilidad internacional en el nuevo entorno tecnológico y digital es someterse voluntariamente al principio de comportamiento responsable de los Estados, conforme a lo acordado en el Resolución 70/237 de la Asamblea General de NNUU[149] sobre los avances en la esfera de la información y las telecomunicaciones, como base para ampliar las oportunidades de cooperación para el bien común de los Estados, impulsar el intercambio seguro de información a nivel internacional y fomentar la innovación y la creatividad de los desarrollos en dicho ámbito.
3. Aunque el esquema de respuesta parte de la acción conjunta, éste se construye desde el compromiso de cada Estado orientado a desarrollar capacidades propias para prevenir, detectar, defender y responder ante esta amenaza, cuya afectación a las infraestructuras críticas y servicios esenciales puede tener graves repercusiones para el normal funcionamiento de la sociedad y el bienestar de los ciudadanos, así como en la seguridad y soberanía del Estado:

> "States also concluded that ICT activity contrary to obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public, could pose a threat not only to security but also to State sovereignty, as well as economic development and livelihoods, and ultimately the safety and wellbeing of individuals"[150].

En línea con este compromiso para hacer frente a la utilización de las TIC con fines delictivos, la Asamblea General mediante la Resolución 74/247[151] crea un Comité Intergubernamental de expertos *ad hoc*, que tiene su primer periodo de sesiones en marzo de 2022, iniciándose el proceso de elaboración de una convención internacional para consensuar la respuesta a dicha amenaza.

También el Consejo de Seguridad de NNUU acepta que tiene un papel que desempeñar en la ciberseguridad internacional, tal y como queda patente en la reunión informal coorganizada por Corea del Sur y EE.UU., celebrada en abril de 2024, sobre *Evolución del panorama de las ciberamenazas y sus implicaciones para el mantenimiento de la paz y*

[149] Resolución 70/237 de la Asamblea General de NNUU aprobada el 23 de diciembre de 2015. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/70/237. Disponible en: https://www.un.org/es/ga/70/resolutions.shtml (29/02/2024).

[150] Developments in the field of information and telecommunications in the context of international security. Note by the Secretary-General. 18 March 2021. A/75/816. Disponible en: https://documents.un.org/doc/undoc/gen/n21/068/72/pdf/n2106872.pdf (01/03/2024).

"Los Estados también concluyeron que las actividades TIC contrarias a las obligaciones del Derecho Internacional que dañan intencionadamente las infraestructuras críticas o de otra forma perjudican su uso y funcionamiento para prestar servicios públicos, pueden suponer una amenaza no solo para la seguridad sino también para la soberanía de los Estados, así como para el desarrollo económico y los medios de vida e incluso la seguridad y el bienestar de las personas" (Traducción propia).

[151] Resolución aprobada por la Asamblea General el 27 de diciembre de 2019. Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Asamblea General. A/RES/74/247. 20 de enero de 2020. Disponible en: https://documents.un.org/doc/undoc/gen/n19/440/32/pdf/n1944032.pdf?token=aLMLC4D6DPQGL1vShC&fe=true (29/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la seguridad internacionales[152]. En ella, no solo se trata de la evolución y el posible impacto de la ciberdelincuencia en el orden mundial, sino que también se concluye que el Consejo de Seguridad, con sus cinco miembros permanentes liderando la clasificación de naciones con mayor nivel de madurez cibernética -uso de ciberoperaciones, establecimiento de la gobernanza digital, estrategia de ciberseguridad, etc.-, puede y debe asumir un compromiso de responsabilidad y participación ayudando a los GEG y GTCA para, por ejemplo, impulsar una mayor concienciación global en ciberseguridad, convocar revisiones anuales para tratar la naturaleza altamente cambiante de la ciberamenaza e, incluso, la participación en la investigación de ciberincidentes de alta significación, todo lo cual entra dentro de su rol de garante de la paz mundial.

En este contexto se enmarca la publicación, en mayo de 2024, de la *United States´International Cyberspace and Digital Policy Strategy: towards an innovative, secure and rights-respecting digital future*[153], cuyo eje vertebrador es el concepto de solidaridad digital entendido como:

> "[…] a willingness to work together on shared goals, to stand together, to help partners build capacity, and to provide mutual support. Digital solidarity recognizes that all who use digital technologies in a rights-respecting manner are more secure, resilient, self-determining, and prosperous when we work together to shape the international environment and innovate at the technological edge"[154].

Esta visión que presenta la estrategia estadounidense del ecosistema digital inclusivo, abierto, resiliente y seguro es una propuesta con clara inspiración en la línea avanzada por NNUU, para integrar los diferentes enfoques de gobernanza de datos, fomentar el comportamiento responsable en el ciberespacio y reforzar la capacidad digital de los socios internacionales, a partir de la cual avanzar unidos contra las ciberamenazas y los desafíos planteados por los actores maliciosos, estatales y no estatales, que utilizan el ciberespacio para sus fines criminales y amenazar la paz y la estabilidad internacionales, socavando el respecto de los derechos humanos y las libertades ciudadanas.

---

[152] Puede consultarse el contexto de esta reunión del Consejo de Seguridad y su relevante conclusión de cara al compromiso del mismo con la seguridad en el ciberespacio. Disponible en: https://www.oodaloop.com/archive/2024/04/23/the-un-security-council-has-a-role-in-international-cybersecurity/ (11/05/2024).

[153] La Estrategia Internacional de Política Digital y Ciberespacio de los EE.UU.: hacia un futuro digital innovador, seguro y respetuoso de los derechos supone un llamamiento al compromiso internacional para construir un espacio digital abierto, inclusivo, resiliente, seguro y equitativo, sobre la base de tres principios: una visión positiva de un ciberespacio seguro e inclusivo que respeta el Derecho Internacional y los derechos humanos, la integración de la ciberseguridad con el desarrollo sostenible y la innovación tecnológica, y un enfoque político global que utilice las herramientas apropiadas de la diplomacia y la gobernanza internacional en todo el ecosistema digital. Disponible en: https://www.state.gov/release-of-united-states-international-cyberspace-and-digital-policy-strategy/ (22/05/2024).

[154] La solidaridad digital es "la voluntad de trabajar juntos en objetivos compartidos, mantenerse unidos, ayudar a los socios a desarrollar capacidades y brindarnos apoyo mutuo. La solidaridad digital reconoce que todos los que utilizan las tecnologías digitales de manera respetuosa con los derechos son más seguros, resilientes, autosuficientes y prósperos cuando trabajamos juntos para dar forma al entorno internacional e innovar en la vanguardia tecnológica" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Otro paso adelante supone la aprobación el 7 de agosto de 2024 del *Proyecto de convención de las Naciones Unidas contra la ciberdelincuencia*[155], que prueba la preocupación de NNUU por el impacto de las TIC en la magnitud y consecuencias de los delitos, asi como el convencimiento de que es necesario avanzar en acuerdos de alcance mundial para proteger a la sociedad de la ciberdelincuencia, a través del desarrollo de normativa específica -jurisdiccional, procesal, penal- y el fomento de la cooperación internacional para prevenir y combatir más eficazmente esta amenaza.

Cuestión principal es delimitar el alcance de los tipos delictivos afectados, es decir, si únicamente se trata de aquellos con una naturaleza propiamente cibernética, o también incluye aquellos otros de naturaleza convencional pero que se ven facilitados en su comisión por el uso de la tecnología. Igualmente, el papel que representan los derechos humanos dentro del ámbito de aplicación del tratado. Y aquí es donde, una vez más, las posturas de los Estados se muestran enfrentadas por la distinta forma de entender las herramientas propuestas para la represión y vigilancia de la ciberdelincuencia[156], de manera que esta dialéctica parece que va a mantenerse activa toda vez que Rusia, que impulsó inicialmente en 2017 la redacción de un Tratado en el seno de las NNUU que atendiera a la cooperación internacional en la lucha contra la ciberdelincuencia, en agosto de 2024 no lo recibe con agrado, criticando su redacción y extensiva salvaguarda de derechos. Con esta situación, en noviembre de 2024, la Asamblea General aprueba -sin someter a votación- la resolución de *Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos*[157], para su firma y entrada en vigor a lo largo de 2025. En definitiva, como señala el Informe de la Dependencia Común de Inspección de Naciones Unidas[158]:

> "[…] lo que está en juego más bien es la capacidad de las organizaciones del sistema de las Naciones Unidas para cumplir sus mandatos, y también su credibilidad ante sus miembros y beneficiarios. Además, muchas categorías de personas cuyos datos custodian las organizaciones del sistema de las Naciones Unidas pueden quedar expuestas a importantes consecuencias adversas en caso de ser filtrados. Aunque los ciberataques pueden afectar de manera diferente a organizaciones con mandatos y estructuras diversas, la amenaza es real y compartida. Ninguna organización está a salvo de experimentar en alguna ocasión un incidente de ciberseguridad, independientemente de lo preparada que esté o lo vigilante que sea. Además, si se desdeñan los riesgos de que ello ocurra, el

[155] Proyecto de convención de las Naciones Unidas contra la ciberdelincuencia. Fortalecimiento de la cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves. 7 de agosto de 2024. A/AC291/L15. Disponible en: https://ciberprisma.org/wp-content/uploads/2024/08/v2405509-espanol.pdf (19/09/2024).

[156] Las dificultades del proceso de redacción tienen eco en prensa. Disponible en: https://www.hrw.org/news/2023/10/16/un-cybercrime-treaty-menace-making https://efe.com/mundo/2024-08-09/naciones-unidas-primer-tratado-ciberdelincuencia/ (20/09/2024).

[157] Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. 27 de noviembre de 2024. Asamblea General. A/79/460. Disponible en: https://documents.un.org/doc/undoc/gen/n24/372/07/pdf/n2437207.pdf (12/01/2024).

[158] Informe de la Dependencia Común de Inspección de Naciones Unidas, JIU/REP/2021/3, página III. Disponible en: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf (22/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

impacto en la reputación y las repercusiones operacionales, jurídicas y financieras pueden ser considerables".

De esta forma, podemos concluir que el enfoque multidisciplinar que NNUU utiliza para afrontar los riesgos de la ciberamenaza supone, a nuestro parecer, una evidencia más de la relevante aportación que hace a la seguridad del siglo XXI, integrando la protección de los derechos digitales –esfera individual de los ciudadanos- y la ciberseguridad –en el ámbito público de los Estados-, para traducir al nuevo lenguaje del *quinto dominio* el clásico axioma de que *sin seguridad no hay libertad*.

Esta aportación de NNUU debe ser reconocida por su amplia repercusión a nivel global, independientemente de todos los problemas que como organización arrastra, fruto de los cuales vive momentos de franco declive que reclaman, si no una refundación, sí una nueva orientación y un renovado compromiso de sus miembros, so pena de seguir desgastándola con el desprestigio y la incapacidad para asumir los compromisos que la vieron nacer.

2.2. La Organización del Tratado del Atlántico Norte

En el 2024 se celebraban los 75 años de la firma del *Tratado de Washington* por doce países del área atlántica[159], liderados por EE.UU., que buscaban la defensa conjunta de sus territorios frente a la amenaza común que, en ese momento, representaba la URSS. Catorce son los artículos que estructuran esta organización político militar intergubernamental consagrada a la seguridad de sus miembros, Estados soberanos que actúan por consenso para la toma de decisiones, y cuya esencia se vislumbra en los tres compromisos de su Preámbulo[160]: 1) alineamiento con la Carta de NNUU; 2) salvaguarda de los principios de democracia, libertad y legalidad; 3) y defensa de la paz y la estabilidad en la zona del Atlántico Norte.

Estas son las claves, a nuestro entender, para interpretar la trayectoria de la Alianza y valorar la situación actual tras más de siete décadas de continua evolución estratégica que, paradójicamente, parecen haberla devuelto a la casilla de salida, en el tablero de una Europa nuevamente en guerra.

2.2.1. 1949-1990: el equilibrio de la Guerra Fría

[159] El 4 de abril de 1949 firman el Tratado del Atlántico Norte doce países: Francia, Reino Unido, Bélgica, Países Bajos, Luxemburgo, Estados Unidos, Canadá, Portugal, Italia, Dinamarca, Islandia y Noruega. Disponible en: https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=es (03/08/2023).

[160] "Las Partes de este Tratado reafirman su fe en los propósitos y principios de la Carta de las Naciones Unidas y su deseo de vivir en paz con todos los pueblos y todos los Gobiernos. Decididos a salvar la libertad, la herencia común y la civilización de sus pueblos, basados en los principios de la democracia, las libertades individuales y el imperio de la ley. Deseosos de promover la estabilidad y el bienestar en la zona del Atlántico Norte. Resueltos a unir sus esfuerzos para la defensa colectiva y la conservación de la paz y la seguridad. Acuerdan, en consecuencia, este Tratado del Atlántico Norte:"

Ediciones Universidad de Salamanca | CC BY-NC-ND

Sobre la base de los *Tratados de Dunquerque*[161] y *Bruselas*[162], el del *Atlántico Norte* se configura como el aglutinador del bloque occidental liderado por EE.UU. para articular la defensa colectiva de Europa frente a la URSS. Ésta, por su parte, en 1955 y como reacción inmediata al ingreso de la República Federal de Alemania en la Alianza, impulsa la firma del *Pacto de Varsovia*[163] para disponer la protección del bloque oriental "frente al agresivo pacto de la OTAN" (GÖRLITZ, 1980, pág. 459), mediante la cooperación militar y el adecuado posicionamiento de las fuerzas convencionales y nucleares de los aliados de Moscú forjando lo que, en palabras de Sir Winston Churchill[164], se llamó el *Telón de Acero*.

No deja de llamar la atención el paralelismo de ambos Tratados en cuanto a la cadencia de su exposición, la estructura de su docena de artículos y el singular compromiso con la paz como medio para articular la defensa. Sirva como ejemplo el primer artículo de cada uno de ellos, donde ratifican la voluntad de resolución pacífica de las controversias internacionales, así como la *cláusula de asistencia mutua* que, también en ambos casos, remite al artículo 51 de la Carta de las Naciones Unidas:

> Tratado del Atlántico Norte
>
> "Artículo 1: Las Partes se comprometen, tal y como está establecido en la Carta de las Naciones Unidas, a resolver por medios pacíficos cualquier controversia internacional en la que pudieran verse implicadas de modo que la paz y seguridad internacionales, así como la justicia, no sean puestas en peligro, y a abstenerse en sus relaciones internacionales de recurrir a la amenaza o al empleo de la fuerza de cualquier forma que resulte incompatible con los propósitos de las Naciones Unidas.
>
> Artículo 5: Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque

[161] El Tratado de Dunquerque lo firmaron en marzo de 1947 Francia y Reino Unido con el objetivo de unir esfuerzos frente a la amenaza de un posible resurgir armado de Alemania, tal como ocurrió después de la Primera Guerra Mundial.

[162] El Tratado de Bruselas -Tratado Económico, Social, Cultural y de Defensa colectiva- por el que se constituye la Unión Europea Occidental (UEO), fue firmado en marzo de 1948 por Francia, Reino Unido, Bélgica, Países Bajos y Luxemburgo como acuerdo de cooperación y, principalmente, de defensa conjunta frente a la amenaza militar proveniente de una URSS expansionista.

[163] El Pacto de Varsovia, o Tratado de Amistad, Colaboración y Asistencia Mutua auspiciado por la URSS, se firma en Varsovia el 14 de mayo de 1955 por la República Democrática Alemana, Polonia, Bulgaria, Rumanía, Checoslovaquia, Hungría y Albania. Lo componen once artículos que, al leerlos, llevan inmediatamente a apreciar su paralelismo con el Tratado del Atlántico Norte en la cadencia de su exposición, en la estructura de sus artículos y en el compromiso con la paz para articular su defensa. Disponible en: https://www.dipublico.org/3602/pacto-de-varsovia-1955/ (03/08/2023).

[164] En el discurso titulado "Los Pilares de la Paz", pronunciado por Sir Winston Churchill en el Westminster College de Missouri (EE.UU.) el 5 de marzo de 1946, con ocasión de su investidura como Doctor Honoris Causa junto al presidente Harry Truman, expone preocupado la tendencia expansiva y proselitista de Rusia y las consecuencias que, en su opinión, pueden acarrear para Europa, concluyendo que "desde Stettin, en el Báltico, a Trieste, en el Adriático, ha caído sobre el continente un *telón de acero*. Tras él se encuentran todas las capitales de los antiguos Estados de Europa Central y Oriental". Disponible en: https://historia1imagen.cl/2007/09/11/wiston-churchill-el-telon-de-acero/ (21/07/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales".

∞ ∞∞ ∞∞ ∞

Tratado del Pacto de Varsovia:

"Artículo 1: Las Partes Contratantes se comprometen, conforme a la Carta de las Naciones Unidas, a abstenerse en sus relaciones internacionales de recurrir a la amenaza o al uso de la fuerza y a arreglar sus controversias internacionales por medios pacíficos, de tal manera que no se pongan en peligro la paz y la seguridad internacionales.

Artículo 4: En cada caso de ataque armado en Europa contra uno o varios de los Estados Partes en el Tratado, por cualquier Estado o grupo de Estados, cada Estado Parte en el Tratado, en el ejercicio de su derecho de legítima defensa individual o colectiva, conforme al artículo 51 de la Carta de las Naciones Unidas, prestará al Estado o Estados víctimas de tal ataque una inmediata asistencia, individualmente o por acuerdo con los otros Estados Partes en el Tratado, por todos los medios que considere necesarios, incluso el uso de la fuerza armada. Los Estados Partes en el Tratado se consultarán inmediatamente sobre las medidas colectivas necesarias para restablecer y mantener la paz y la seguridad internacionales. Las medidas tomadas de acuerdo con este artículo se comunicarán al Consejo de Seguridad conforme a las disposiciones de la Carta de las Naciones Unidas. Tales medidas quedarán sin efecto tan pronto el Consejo de Seguridad haya tomado la acción necesaria para el restablecimiento de la paz y la seguridad internacionales".

Queda claro el equilibrio de fuerzas simétricas que definen ambos bloques con sus respectivos Tratados, postulando un carácter defensivo basado en la responsabilidad compartida de los correspondientes aliados para dar respuesta a un eventual ataque armado contra la soberanía de los Estados que los integran, ya sea contra sus territorios o contra las fuerzas, buques o aeronaves de cualquiera de las partes que se hallen en dichos territorios.

Es en este contexto en el que la Alianza entiende necesario dar forma a las líneas maestras de su pensamiento y, para ello, concibe un tipo de documento que, a futuro, servirá para definir el equilibrio necesario en cada momento entre sus tres funciones básicas: la defensa colectiva, la seguridad cooperativa y la gestión de crisis. Nace así el *Concepto Estratégico* como herramienta esencial para concretar el ciclo de renovación a través del que organizar los medios políticos –cuerpo diplomático y grupos de trabajo- y militares –fuerzas y equipos operativos- de que dispone para responder, de manera

Ediciones Universidad de Salamanca | CC BY-NC-ND

adaptativa, a la evolución de la amenaza en el escenario internacional (GARCÍA ARNAIZ, 2017, págs. 55-58).

El primero de ellos es el *Concepto Estratégico para la Defensa del Área Noratlántica*, de enero de 1950[165] en el que, desde una perspectiva disuasoria ajustada al territorio aliado, se construye la defensa ante la amenaza vinculada a la superioridad de fuerzas convencionales soviéticas y la invasión de Europa por tierra, diseñando una estrategia de *Respuesta Inmediata* "con todo tipo de armas sin excepción, en clara alusión al arma atómica" (ADÁN GARCÍA, 2019, pág. 8).

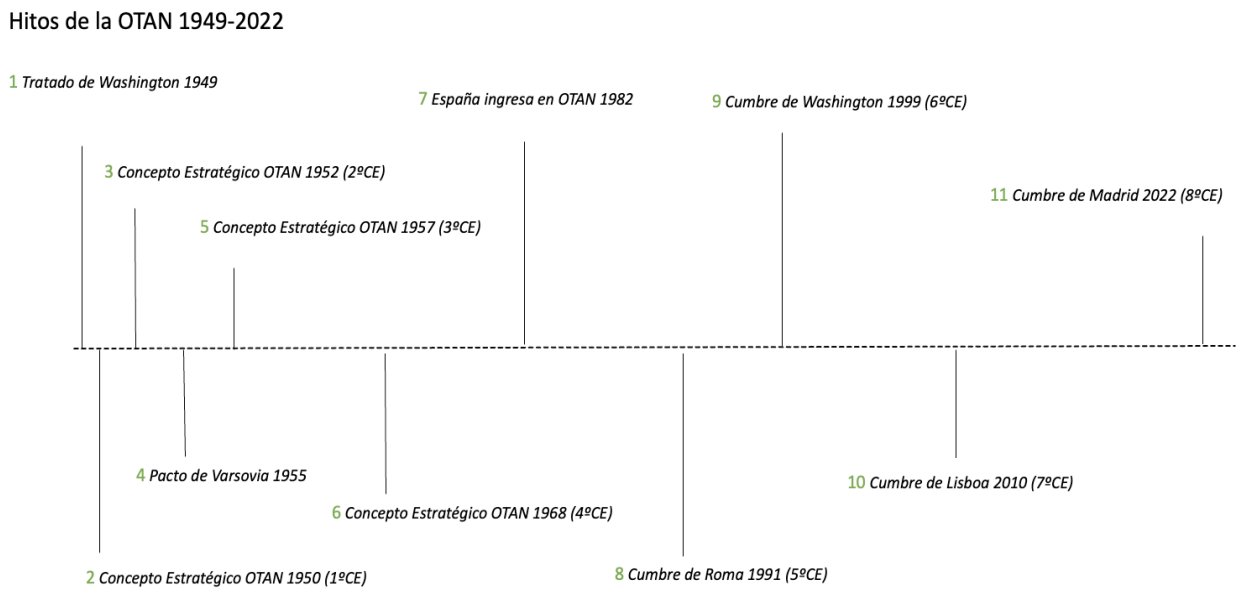


Gráfico 2.1.
Línea de tiempo de eventos y Conceptos Estratégicos de la OTAN
Fuente: propia

Apenas dos años después, a finales de 1952, se considera necesario redactar un *segundo Concepto Estratégico*[166] para definir la Estructura de Mando de la OTAN (NCS) a través del Comandante Supremo Aliado en Europa (SACEUR)[167] y el Comandante Supremo Aliado del Atlántico (SACLANT)[168], al tiempo que se instituye el puesto de Secretario General, siendo el primer nominado para ocupar el cargo Lord Hasting Lionel Ismay. Ese

[165] Hasta el año 1991 los Conceptos Estratégicos de la OTAN son documentos clasificados y, como tales, de limitada difusión y uso restringido, porque el riesgo de enfrentamiento armado entre ambos bloques era real. A partir de entonces, con el final de la Guerra Fría, pasan a ser documentos públicos en aras de una mayor transparencia de la Organización.
[166] Concepto Estratégico para la Defensa del Área del Atlántico Norte, de 3 de diciembre de 1952.
[167] SACEUR: Supreme Allied Commander Europe. Con sede actualmente en Mons (Bélgica), este puesto siempre ha sido ocupado por un Oficial de las Fuerzas Armadas de EE.UU. y, al mismo tiempo, también es el Comandante del Mando Europeo de los EE.UU., es decir, de las tropas estadounidenses acantonadas en Europa. El primero en ocupar el cargo fue el General Dwight David Eisenhower.
[168] SACLANT: Supreme Allied Commander Atlantic, con sede en Norfolk (Virginia, EE.UU.). A partir de 2002 pasa a denominarse SACT (Supreme Allied Commander Transformation).

Ediciones Universidad de Salamanca | CC BY-NC-ND

mismo año, 1952, ingresan en la Alianza Grecia y Turquía, mientras que la República Federal de Alemania lo hará en 1955.

A mediados de 1957, aún con la idea en mente de la superioridad del bloque del Este en fuerzas convencionales, y el planteamiento más probable de la amenaza en forma de ataque nuclear soviético a Europa por sorpresa, se presenta el *tercer Concepto Estratégico* que propugna la *Represalia Masiva*, insistiendo la Alianza en que "nunca empezará una guerra, pero si se inicia, estará abocada al empleo masivo de armas nucleares" (ADÁN GARCÍA, 2019, pág. 10), que serán usadas desde el primer momento.

Ese mismo año, Lord Ismay presenta un informe ejecutivo que él mismo define como "principal instrumento para la coordinación de los esfuerzos de defensa de los aliados"[169], en el que se arbitra el modelo de las infraestructuras y cuarteles generales de la organización, los planes de emergencia civil, la resolución de disputas entre Estados miembros, o la cooperación política, económica, social y cultural entre ellos. Esta línea de cooperación más allá del ámbito militar se acababa de abrir unos meses antes con el conocido como *Informe de los Tres Hombres Sabios*[170] que, en el marco de carácter político que subyace al artículo 2 del Tratado de Washington[171], pretendía impulsar esas áreas colaborativas que aún hoy perduran bajo la denominación de Programa Ciencia para la Paz y la Seguridad (SPS)[172].

Tras ocho años de existencia la organización ve la necesidad de extender su atención a las zonas de influencia propias, fuera del territorio noratlántico, puesto que también allí pueden surgir conflictos con el Bloque del Este que obliguen a los aliados a defenderse sobre el terreno (ADÁN GARCÍA, 2019, págs. 14-17). El objetivo del despliegue de bases militares en el exterior como presencia avanzada va a permitir a la OTAN la ejecución de

[169] El conocido como *Informe Lord Ismay*, primer Secretario General de la OTAN. Disponible en: https://archives.nato.int/uploads/r/null/1/3/137336/0096_Lord_Ismay_Report_North_Atlantic_Council_1957_ENG.pdf (12/08/2023).

[170] El *Three Wise Men Report*, de 13 de diciembre de 1956, fue encargado a los Ministros de Relaciones Exteriores de sus respectivos gobiernos Lester B. Pearson (Canadá), Gaetano Martino (Italia) y Halvard Lange (Noruega). Este informe inició una nueva vía para la coordinación y cooperación no militar entre los aliados. Disponible en: https://www.nato.int/cps/en/natohq/news_139363.htm (14/08/2023).

[171] El artículo 2 del Tratado establece que "Las Partes contribuirán a un mejor desarrollo de las relaciones internacionales pacíficas y amistosas reforzando sus instituciones libres, asegurando una mejor comprensión de los principios en los que se basan estas instituciones y promoviendo las condiciones adecuadas que favorezcan la estabilidad y el bienestar. Tratarán de eliminar conflictos en sus políticas económicas internacionales y estimularán la colaboración económica entre varias o todas las Partes".

[172] El *Science for Peace and Securty Progamme* (SPS) se fundó en 1958 para promover la cooperación relacionada con la seguridad civil desde la investigación científica, la innovación y el intercambio de conocimientos. Según la página web de la organización, proporciona un canal de comunicación no militar entre la comunidad científica y la OTAN para abordar los desafíos de seguridad emergentes, donde los investigadores, académicos y expertos desempeñan un papel importante para ayudar a la Alianza a identificar, comprender y responder a las vulnerabilidades, amenazas y desafíos emergentes como la ciberdefensa, la lucha contra el terrorismo o la seguridad energética y ambiental. Las iniciativas incluyen el desarrollo de tecnologías avanzadas relacionadas con la seguridad en campos como la cuántica y la inteligencia artificial (IA), y también abordan aspectos humanos y sociales de la seguridad, como la implementación de la Resolución 1325 del Consejo de Seguridad de las Naciones Unidas (RCSNU) sobre Mujeres, Paz y Seguridad. Disponible en: https://www.nato.int/cps/en/natohq/topics_85373.htm (14/08/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

estrategias que combinan la *disuasión* -persuadir al adversario de que el coste de iniciar una acción ofensiva basada en el uso de la fuerza supera al beneficio que pueda obtener con esa decisión- y la *seguridad* -persuadir a los aliados de que los beneficios de la acción militar serán mayores que los costes-.

De esta manera, jugando al equilibrio bipolar y aprovechando la debilidad de la Europa de postguerra, se va a ir conformando la esfera de influencia de EE.UU. desde la que poder actuar para aminorar sus temores y estimular sus ambiciones. Esta política, al mismo tiempo, condicionará la relación entre la OTAN y la UE, como se verá más adelante, pues el objetivo de las bases no solo es contener a las fuerzas soviéticas para garantizar la seguridad aliada impidiendo que estallara una nueva guerra, sino también "eliminar la posibilidad de que los Estados de Europa Occidental volvieran a nacionalizar sus políticas de seguridad, evitando así su capacidad de emprender acciones unilaterales" (COLOM PIELLA, y otros, 2022, pág. 15).

Mientras tanto, la intrincada década de los sesenta lleva la Guerra Fría a su cenit con dos hechos señalados: la *construcción del Muro de Berlín*, solución pactada al ultimátum que la URSS había dado para los que los aliados abandonasen la ciudad, y la *crisis de los misiles de Cuba*, que Nikita Kruschev y John F. Kennedy solucionan de manera diplomática en última instancia ante el riesgo cierto de la mutua aniquilación nuclear. Al mismo tiempo las agencias de inteligencia como la CIA[173] y la KGB[174] prosperan en un escenario en el que el objetivo es alcanzar alguna ventaja sobre el adversario utilizando cualquier método para desgastarlo o comprometerlo política o socialmente, de forma que las "campañas de desinformación antioccidentales fueron agresivas y vertiginosas, y emplearon métodos innovadores que evolucionaron con rapidez y de manera inesperada y alarmante" (RID, 2021, pág. 160) para fomentar la subversión, el temor y la agitación de los ciudadanos de ambos bandos. La relevante presencia de las campañas de desinformación durante la Guerra Fría es un elemento a tener en cuenta para cuando, en posteriores capítulos, analicemos esta amenaza en el contexto geoestratégico actual.

Para desescalar el conflicto y recuperar las posibilidades de diálogo entre ambos bloques a principios de los años setenta, los presidentes Richard Nixon y Leonid Breznev utilizaron la política de la *distensión* "en un momento de difícil retorno -con la guerra de Vietnam planteando enormes dificultades a Washington y el pulso Este-Oeste en un punto especialmente peligroso-" (ECHEVERRÍA JESÚS, 2019, pág. 217). La *distensión* es la idea fuerza que inspira tanto el Informe Harmel de 1967[175] como, un año más tarde, el *cuarto Concepto Estratégico* de la OTAN que plantea como novedad la defensa desde

[173] La Agencia Central de Inteligencia (Central Intelligence Agency - CIA) es el servicio de inteligencia exterior de los Estados Unidos, creada en 1947 y operativa hasta hoy día.

[174] El Comité para la Seguridad del Estado (KGB) fue la agencia de inteligencia de la Unión Soviética entre 1954 y 1991, año en que fue disuelta. Actualmente las labores de inteligencia, contrainteligencia y espionaje son desarrolladas por el Servicio Federal de Seguridad de la Federación de Rusia (FSB).

[175] El Informe sobre las tareas futuras de la Alianza (Informe Harmel) se presenta el 12 de diciembre de 1967 en el Consejo Atlántico de Bruselas, centrando su propuesta en la *distensión* como forma de abrir nuevas vías de comunicación con los soviéticos mediante la combinación de la defensa con el diálogo, poniendo en este sentido especial énfasis en el control del desarrollo armamentístico de ambos bloques. Disponible en: https://www.nato.int/cps/en/natohq/topics_67927.htm (22/08/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la *respuesta flexible*, donde la *disuasión* se entiende como determinación y capacidad de responder pero desde la flexibilidad para adaptar y modular la respuesta conforme a la entidad de la agresión. La *respuesta flexible* incluye un conjunto de opciones de empleo combinado de fuerzas y armas, tanto convencionales como nucleares, que puede articularse de tres maneras: 1) la *defensa directa* -responder al mismo nivel que el ataque-; 2) la *escalada deliberada* -llevar el conflicto a un punto que resulte inadmisible para el enemigo desde el punto de vista del coste y riesgo asumido-; 3) la *respuesta nuclear general* -que es la represalia masiva como última opción- (ADÁN GARCÍA, 2019, págs. 15-17).

Este cuarto Concepto Estratégico para la Defensa del Área de la Organización del Tratado del Atlántico Norte[176] es el que mayor etapa temporal cubre por cuanto permanece vigente casi veinticuatro años, desde enero de 1968 hasta noviembre de 1991, en que se celebra la Cumbre de Roma. En este periodo, concretamente en mayo de 1982, España firma el Tratado de Washington, convirtiéndose en el miembro número dieciséis de la Alianza Atlántica.

2.2.2. 1990-2001: la evolución desde la defensa colectiva a la seguridad compartida

Con el final de la Guerra Fría, propiciado por la caída del muro de Berlín en 1989 y la disolución del Pacto de Varsovia y la URSS en fechas próximas a la firma del Tratado de Reducción de Armas Estratégicas START en 1991, la OTAN considera necesaria una revisión radical de su estrategia y convoca la Cumbre de Roma en noviembre de ese mismo año.

Por primera vez el Concepto Estratégico es público y debe afrontar un nuevo escenario nunca antes contemplado en la organización: la desaparición de su *alter ego*. La nueva perspectiva que ofrece el Viejo Continente obliga a afrontar cuatro grandes riesgos que identifica de manera acertada el ex Ministro de Defensa español D. Julián García Vargas en su conferencia de clausura de la LXXXI Promoción del *Nato Defence College* de Roma. En primer lugar, el auge en Europa de nacionalismos vinculados con el fin del comunismo soviético, en una especie de proceso descolonizador que conlleva tensiones y exacerbación de los sentimientos nacionales y que suponen en cierta forma un "retorno al pasado decimonónico". En segundo lugar, compensar el vacío ideológico y de poder derivado de la disolución de la URSS en una coyuntura de crisis económica que apenas deja margen para programas de ayuda financiera a las nuevas democracias. En tercer lugar, la preocupación por el gran arsenal soviético compuesto de armamento convencional y nuclear que, fuera de control, puede alimentar conflictos en los países del Este de Europa. Y en cuarto y último lugar, el descubrimiento de crisis latentes en el entorno mediterráneo asociadas a tensiones militares, conflictos larvados, inestabilidad estructural y migraciones humanas, todo ello en un contexto cultural diferente al europeo que puede dar lugar a una "creciente incomprensión" (GARCÍA VARGAS, 1993, pág. 7).

[176] Disponible en: https://www.nato.int/docu/stratdoc/eng/a680116a.pdf (22/08/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Todo ello obliga a la OTAN a reinventarse, pasando de ser una alianza militar focalizada en la *defensa colectiva* frente a la amenaza del Este, a una comunidad de *seguridad compartida* orientada a la contención de riesgos de distinta naturaleza, con una estrategia que combina a partes iguales la distensión, la diplomacia y el control de la fuerza disuasoria.

Paradójicamente, en 1995 se desarrolla la primera operación con fuerzas militares de la OTAN de su historia, la *Operación Fuerza Deliberada*, en la que coordinados con NNUU se interviene en los Balcanes occidentales para poner fin al conflicto de Bosnia y Herzegovina, dando paso a los Acuerdos de Dayton. Cuatro años después se ejecuta la *Operación Fuerza Aliada*, esta vez sin autorización previa del Consejo de Seguridad de NNUU por el bloqueo de Rusia, para tratar de derrocar a Slobodan Milosevic y acabar con la limpieza étnica que lleva a cabo en Kosovo.

Es este un momento de debilidad de Rusia que la OTAN no está dispuesta a dejar pasar para, so pretexto de una nueva estructura de seguridad europea más inclusiva, abrirse a la incorporación de aquellos países del Este que, como Polonia, Hungría y la República Checa, miran a la Alianza como garantía de futuro en paz. Al mismo tiempo, el 27 de mayo de 1997, "tras arduas y prolongadas negociaciones", se firma en París el *Acta Fundacional sobre las Relaciones, Cooperación y Seguridad Mutuas entre la OTAN y la Federación Rusa* para, desde la reciprocidad y la transparencia, impulsar la cooperación y fortalecer la confianza bilateral sobre la que construir la unidad europea, cuyo alcance a corto plazo ya se vislumbra harto complicado pues, tras el encontronazo que supone la intervención Aliada en Kosovo, Rusia exterioriza la sensación de "enorme reto que supone dar vida al documento creado" (PAVÓN PÉREZ, 1999, pág. 230).

La Cumbre de Washington de 1999 establece una estrategia para la Alianza que atiende a cuatro prioridades: 1) el reforzamiento del vínculo transatlántico en la idea de que la seguridad de EE.UU. y Europa es un todo indivisible; 2) el impulso de las operaciones de respuesta de crisis fuera del artículo 5, como las llevadas a cabo en los Balcanes; 3) el fomento de la asociaciones y acuerdos de cooperación; 4) y, desde luego, la ampliación hacia el Este (ADÁN GARCÍA, 2019, págs. 19-20).

En otro orden de cosas, se diseña el concepto de *Combined Joint Task Force* (CJTF) para dar respuesta rápida a las necesidades de despliegue de fuerzas en las misiones que, a partir de ahora, empieza a considerar la existencia de actores no estatales en el entorno periférico de la Alianza, con capacidad para acceder y usar armamento de guerra sofisticado.

En este contexto internacional que lidera en solitario EE.UU. se evidencia, por un lado, su cada vez mayor superioridad tecnológica militar que, a través de la OTAN, instrumentaliza para las intervenciones militares fuera de área y, por otro, la ya de por sí manifiesta dependencia en el ámbito de seguridad de los aliados europeos que, entre serias divergencias, tratan de poner remedio avanzando hacia una Política Europea de Seguridad y Defensa (PESD) que, como se verá, no va a encontrar un apoyo incondicional al otro lado del Atlántico.

Ediciones Universidad de Salamanca | CC BY-NC-ND

2.2.3. 2001-2014: la adaptación a las nuevas amenazas

Los atentados terroristas del 11 de septiembre de 2001 dan pie a la invocación, por primera vez en la historia, del artículo 5 del Tratado de Washington, y la consiguiente orientación hacia una estrategia mundial de marcado carácter contraterrorista y de intervención en zonas de crisis y posconflicto. Este enfoque global requiere, precisamente, trabajar de manera conjunta en el marco de seguridad y desarrollo que las propias NNUU venían respaldando desde 1992 en su informe *Un programa de paz. Diplomacia preventiva, establecimiento de la paz y mantenimiento de la paz* y que tan poco éxito estaba cosechando a tenor de los conflictos abiertos en los albores del siglo XXI y "la progresiva huida hacia delante, en solitario, de los EE.UU. tras los atentados del 11-S" (ECHEVERRÍA JESÚS, 2019, pág. 231), con evidente desgaste para el vínculo transatlántico a raíz de la invasión de Irak por cuenta propia.

Por otro lado, esta nueva amenaza terrorista, *asimétrica, dinámica y diversificada* hace necesario implementar un esfuerzo innovador que reconsidere la estrategia, los procedimientos y las estructuras de soporte de la Alianza. Por ello, en este periodo se consolidan avances para el propósito de disuasión y defensa como la incorporación, en la Cumbre de Praga de 2002, del Mando Aliado de Transformación (SACT) con el fin de potenciar la capacidad de despliegue de fuerzas, mantener la ventaja tecnológica sobre el adversario, identificar las áreas clave de los futuros cambios estratégicos y liderar la capacidad de transformación de la Alianza como base de su capacidad operativa (HORCADA RUBIO, 2017, págs. 91-92). En este mismo sentido, en 2007 se crea el Centro de Fusión de Inteligencia de la OTAN (NIFC)[177] como estructura de inteligencia para apoyar la planificación y ejecución de operaciones, y en 2008 el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE)[178], como respuesta a los ciberataques que un año antes sufre Estonia por parte de Rusia y que evidencian dos realidades que van a transitar paralelas en adelante: por un lado, la rentabilidad de los ataques en el ciberespacio y, por otro, el retorno de Rusia al escenario de la confrontación política. En este sentido, la OTAN reacciona con prontitud ante un evidente cambio de paradigma en la naturaleza de la amenaza.

A esto último contribuye de manera decisiva la política de *puertas abiertas* de la OTAN que le lleva a pasar de 16 a 28 miembros entre 1999 y 2009, "con el objetivo de extender el paraguas de seguridad de la Alianza a casi todo el continente, pero sin considerar la aportación estratégica y militar de dichos países" (DÍAZ RODRÍGUEZ, 2020, pág. 19). Así, en 2004 ingresan Bulgaria, Eslovaquia, Eslovenia, Letonia, Lituania, Estonia y Rumanía, y en 2009 lo hacen Croacia y Albania. Esta ampliación a Estados balcánicos y otros próximos al antaño ámbito de influencia de la Unión Soviética tiene un impacto negativo en las relaciones con Rusia que, sintiéndose rodeada por la OTAN, reacciona. Paradójicamente, la propia política expansiva noratlántica actúa como elemento incentivador de su principal enemigo, entumecido hasta entonces.

[177] Ubicado en Molesworth (Reino Unido). Disponible en: https://web.ifc.bices.org/ (24/08/2023).
[178] Ubicado en Tallinn (Estonia). Disponible en: https://ccdcoe.org/ (24/08/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Este resurgimiento de Rusia como amenaza para Europa obedece, al mismo tiempo ,al ideario político de su presidente Vladimir Putin que, en la Conferencia de Seguridad de Múnich[179] de 2007, reprocha el liderazgo unipolar que ha ejercido EE.UU. desde los años noventa y el expansionismo provocador de la OTAN que, en su opinión, socava la confianza mutua y contribuye a alimentar la carrera armamentista[180].

En este contexto, en abril de 2008, se celebra la cumbre de la OTAN en Bucarest donde, entre otras cuestiones, se trata el posible ingreso de Georgia y Ucrania a la organización. Esto implica una *escalada de la tensión* que lleva a Rusia a cerrar filas con Abjasia y Osetia del Sur, regiones prorrusas y autoproclamadas independientes de Georgia, lo que sumado a diversos incidentes y al aumento de la presencia de tropas de uno y otro bando desencadena el conflicto que, finalmente, se cierra en muy poco tiempo con un plan de paz auspiciado por Francia, que comporta la vuelta al *statu quo* original en la zona y, con ello, el afianzamiento de la influencia y el control de Rusia sobre las regiones georgianas independentistas.

En este desafío político y militar ruso al orden internacional, el Kremlin ya hace alarde de su avanzado desempeño en operaciones híbridas y en el ciberespacio, y deja clara su intención de reivindicar el papel estabilizador y mediador en la región del Cáucaso, corredor estratégico para el gas y el petróleo del mar Caspio y Asia Central.

Aun con todo, "las relaciones OTAN-Rusia pronto volvieron a la normalidad" (AGUIRRE DE CÁRCER Y GARCÍA DEL ARENAL, 2017, pág. 28) y el *Concepto Estratégico* que se presenta en la Cumbre de Lisboa de noviembre de 2010 se queda, en nuestra opinión, muy lejos de acertar en la definición de la amenaza, en base a los tres pilares en que se fundamenta.

El primero de ellos es la *defensa colectiva*, "aunque expresamente reconoce que no considera a ningún país como adversario" (ADÁN GARCÍA, 2019, pág. 24), la cual pivota sobre las capacidades nucleares y convencionales que permitirán a la OTAN atender de manera simultánea varias operaciones principales y de menor tamaño, dentro y fuera de su territorio. El segundo pilar es la *gestión de crisis*, que exige disponer de capacidades multifunción -militares, políticas, civiles- para gestionar de forma integral los conflictos. Y el tercero es la *seguridad cooperativa* como modelo para exportar seguridad a todas las áreas de influencia de la Alianza.

Sin embargo, el Concepto Estratégico de Lisboa del año 2010 no ve a China como un posible adversario estratégico, a pesar de que EE.UU. ya mira en 2009 hacia Asia con preocupación (FERNÁNDEZ FERREÑO, 2022, págs. 3-4), y tampoco valora la amenaza de Rusia, a la que la OTAN continúa apreciando como compañera por cuanto:

[179] La Conferencia de Seguridad de Múnich se celebra anualmente en el mes de febrero en dicha ciudad alemana para debatir, en el espíritu de su eslogan "Paz a través del diálogo", los temas internacionales vinculados a la acción exterior, la seguridad y la defensa. En 2007 se celebró la XLIII Conferencia con la participación de alrededor de 250 personalidades de cerca de 40 países. Disponible en: https://securityconference.org/en/ (24/08/2023).

[180] Discurso del presidente Vladimir Putin en la Conferencia de Seguridad de Múnich de 10 de febrero de 2007. Disponible en: https://equilibriumglobal.com/wp-content/uploads/2018/01/Vladimir-Putin-Conferencia-Seguridad-Munich-2007.pdf (24/08/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] que la relación entre ambos es de importancia estratégica al contribuir a la paz, seguridad y estabilidad. Sigue apostando por una reciprocidad en temas de seguridad y pretende mejorar la cooperación en asuntos de defensa antimisil, contra piratería, contra narcóticos y contra terrorismo" (ADÁN GARCÍA, 2019, pág. 25).

Incomprensiblemente, los aliados hacen oídos sordos a Rusia que alza potente su voz, no consideran los nuevos retos que se van fraguando en la zona de Asia-Pacífico, se distraen en la gestión de crisis -de otros- y, con notoria insensibilidad al peligro, relegan la defensa de la zona noratlántica a un segundo plano y se centran en los flancos. A esta misma conclusión parece llegar la Directiva española de Defensa Nacional de 2012[181] cuando dice que, aun siendo la Alianza Atlántica:

> "[…] el vínculo de seguridad y defensa colectiva más apropiado para España […]. Es cierto, sin embargo, que la aprobación en 2010 de un nuevo concepto estratégico no ha cerrado de forma definitiva la reflexión sobre la orientación y los retos estratégicos a que se enfrenta la Alianza, reflexión que debe continuar y producir conclusiones sólidas que repercutan positivamente en la cohesión de las decisiones que la Alianza tome".

A su favor, sin embargo, debe señalarse que el Concepto Estratégico de 2010 identifica el ciberespacio como entorno de riesgo para la prosperidad y la seguridad euroatlántica, poniendo el acento en las capacidades que la Alianza y sus miembros deben desarrollar para prevenir, detectar, defenderse y recuperarse de los ciberataques que pudieran sufrir en sus infraestructuras o sistemas. Como consecuencia:

> "[…] la Alianza creó en agosto de 2010 la División de Desafíos Emergentes de Seguridad (ESCD), cuya finalidad era hacer frente a todos aquellos riesgos y amenazas que no respondían al apelativo de tradicionales, como eran los cibernéticos. Al mismo tiempo, se incorporaron las capacidades de ciberdefensa a su Comité de Planeamiento y Política de Defensa, que pasó a hacer recomendaciones a los aliados sobre asuntos de ciberseguridad" (FUENTE COBO, 2022, pág. 87).

No obstante, en nuestra opinión, esta es la estrategia de la OTAN que, con mucho, más alejada nace de la realidad geopolítica y estratégica e, irónicamente, es la segunda que más tiempo ha permanecido en vigor, pues no se sustituye hasta la Cumbre de Madrid de junio de 2022.

2.2.4. 2014-2024: el resurgir del desafío ruso

A partir del mensaje reivindicador lanzado por Putin en Múnich en 2007 y la evidencia puesta de manifiesto en Georgia de que Rusia ha vuelto para quedarse, la política exterior de Moscú se desarrolla conforme al proyecto expansionista trazado por su

[181] Directiva de Defensa Nacional 2012: por una defensa necesaria, por una defensa responsable. Presidencia del Gobierno. Madrid. Julio de 2012. Página 3. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2012.pdf (24/08/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

presidente, lo cual sirve para, en un golpe de realidad, devolver a la OTAN el motivo de su existencia: la defensa conjunta de sus territorios frente a la amenaza rusa.

En este recorrido, el siguiente hito lo marca la inestabilidad generada en Ucrania a finales de 2013 cuando su presidente Yanukovich, rusófilo, rechaza la firma del Acuerdo de Asociación que se venía negociando con la UE desde 2007 y que, tras distintos episodios violentos durante las manifestaciones del *Euromaidán* en Kiev y enfrentamientos con la oposición, conlleva la salida del país del presidente[182] y su sustitución por un gobierno provisional que convoca elecciones en mayo de 2014. Este contexto de interinidad es aprovechado por grupos prorrusos de Crimea para proponer un referéndum separatista que confirme la adhesión de la península y de la ciudad de Sebastopol a la Federación de Rusia, lo que da la oportunidad al Kremlin de desplegar tropas sobre el terreno con el pretexto de restablecer la paz y la tranquilidad hasta que se normalice la situación, que acaba con la proclamación de la República de Crimea y su reconocimiento por Moscú[183]. Esto supone la violación, entre otros, del Memorándum de Budapest sobre Garantías de Seguridad de 1994.

Días después las milicias prorrusas de las regiones de Donetsk y Lugansk inician una sublevación armada para independizarse de Ucrania, con soporte de tropas uniformadas *sin distintivos* y otras tácticas de guerra híbrida por parte del Kremlin:

> "A ojos del mundo, se trataba de "fuerzas de autodefensa" surgidas entre la población de la península. El personal, uniformado con el nuevo uniforme de camuflaje ruso "flora digital", de estilo pixelado en dos tonos de verde y uno de marrón, no lucía insignias nacionales y pasaron a ser conocidos como los "hombrecillos verdes", mientras que en Rusia se les denominó *gente amable*. La falta de insignias permitió mantener la farsa de que no se trataba de personal militar ruso y, por tanto, Ucrania no podía esgrimir un *casus belli* ante el invasor" (PÉREZ TRIANA, 2023, pág. 145).

Pero los desafíos para la seguridad internacional que trae consigo el 2014 no acaban ahí. En Irak el DAESH se apodera de Mosul y Tikrit y controla las fronteras con Siria, ocupando amplias zonas de Raqqa y Deir-Ezzor, lo cual le facilita el acceso a recursos petrolíferos y al control de las redes de crimen organizado que operan sobre el territorio, obteniendo

[182] El presidente Yanukovich trataba de encontrar la forma de compaginar el Acuerdo de Asociación entre Ucrania y la UE con las negociaciones que, al mismo tiempo, mantenía con Rusia para encontrar un modelo de cooperación con la unión aduanera que ésta tenía con Bielorrusia y Kazajistán desde el 2010. Con ese fin, presionado por Rusia, suspendió la firma del Acuerdo con la UE y propuso la creación de una comisión que iniciase las negociaciones para alcanzar un acuerdo de libre comercio entre Ucrania, Rusia y la UE, lo que le habría permitido jugar las dos bazas: entrar en el selecto grupo europeo y mantenerse próximo a Rusia. Esta maniobra política de Yanukovich desencadena a finales del 2013 las manifestaciones y disturbios del *Euromaidán* en Kiev -con decenas de muertos-, que finalmente obligan al presidente a huir del país hacia Rusia en febrero del 2014. Disponible en: https://www.lavanguardia.com/internacional/20140222/54401609478/ucrania-yanukovich-elecciones.html
https://www.elmundo.es/internacional/2014/02/20/5305d599268e3ecd738b4573.html
https://world.time.com/2014/02/22/ukraines-president-flees-protestors-capture-kiev/ (19/09/2023).

[183] Crisis en Ucrania: condenado el referéndum "ilegal" de Crimea. BBC News 6 marzo 2014. Disponible en: https://www.bbc.com/news/world-europe-26475508 (19/09/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de esta manera abundantes ingresos con los que financiar actividades terroristas en Oriente Medio, Norte de África, el Sahel y los países occidentales (AGUIRRE DE CÁRCER Y GARCÍA DEL ARENAL, 2017, pág. 17), donde se cometen atentados por parte de combatientes terroristas extranjeros y células yihadista nacionales conectadas a través del liderazgo global del autoproclamado Califato Islámico del DAESH.

La Alianza ya no puede desoír los sonidos de sables en sus fronteras. La defensa colectiva del área Noratlántica vuelve a ser prioridad, el marco cooperativo de la OTAN con Rusia queda en suspenso, el flanco sur se resiente y necesita una proyección aliada de estabilidad para contrarrestar los efectos de la lacra terrorista y, junto con la mejora de la disponibilidad de la fuerza, es necesario revisar con urgencia las capacidades para operar en escenarios de guerra híbrida[184].

Todo ello hace que la Cumbre de Gales, de septiembre de 2014, sea necesaria para tapar las vías de agua que amenazan con hundir definitivamente la nave tras la deriva de Lisboa y poder hacer frente a los nuevos retos planteados con, entre otras, medidas de adaptación militar[185], el compromiso de los aliados para "dedicar al menos un 2% del PIB a gastos anuales de defensa y de estos, al menos un 20% para la adquisición de nuevos equipos, incluyendo investigación y desarrollo" (AGUIRRE DE CÁRCER Y GARCÍA DEL ARENAL, 2017, pág. 24), así como la permanencia de tropas OTAN en Afganistán para apoyar la consolidación del Gobierno del país.

Asimismo se acuerda la creación de la Coalición Internacional contra DAESH bajo el auspicio de las NNUU y liderada por EE.UU., para contrarrestar la estrategia expansiva de la organización terrorista y aliviar la presión en los territorios ocupados de Irak y Siria, de manera que permitan el avance del ejército iraquí para recuperar las posiciones y defender Bagdad.

Apenas trascurridos dos años, en julio de 2016, se celebra una nueva Cumbre en Varsovia en la que la organización define dos líneas de actuación fundamentales para el nuevo *enfoque de respuesta 360º*: el *refuerzo de la disuasión y defensa* mediante el despliegue persistente de fuerzas OTAN en el frente Este[186] y, en segundo lugar, la *proyección de estabilidad* para impulsar las capacidades de socios como Ucrania o Georgia, reforzar los programas de asistencia, asesoramiento y entrenamiento de Fuerzas Armadas en Irak, Siria o Libia y desarrollar las actividades de apoyo a la coalición internacional contra DAESH (AGUIRRE DE CÁRCER Y GARCÍA DEL ARENAL, 2017, págs. 36-40). Cuestión fundamental que se aborda también en esta Cumbre es, dentro de la

[184] Conscientes de la amenaza que los conflictos híbridos suponen, en 2014 se crea el NATO Strategic Communications Centre of Excellence (NATO StratCom COE), responsable del análisis de las narrativas desinformativas, operaciones de información de grupos radicales o terroristas, evaluación de impacto de la inteligencia artificial en redes sociales, análisis de estrategias contranarrativas, etc. Disponible en: https://stratcomcoe.org/ (19/09/2023).

[185] En Gales se aprueba el Plan de Acción para la Preparación (Response Action Plan –RAP) con un enfoque de respuesta 360º ante la cada vez mayor amenaza proveniente de Rusia y, al mismo tiempo, los riesgos asociados a la inestabilidad en Oriente Medio, el Sahel y el Norte de África, pero también para contribuir desde la OTAN a la lucha contra el terrorismo internacional. Para hacer operativo este enfoque 360º se crea la Fuerza Conjunta de Muy Alta Disponibilidad (VJTF).

[186] Se establecieron fuerzas OTAN en Polonia, Letonia, Lituania, Estonia, Rumanía y Bulgaria.

Ediciones Universidad de Salamanca | CC BY-NC-ND

doctrina militar de la OTAN, el *reconocimiento del ciberespacio como el quinto dominio*, lo que supone el inicio del desarrollo de Unidades militares específicas para combatir en este nuevo ámbito de operaciones. El ciberespacio es reconocido, definitivamente, como escenario de confrontación permanente entre los aspirantes al poder hegemónico.

Para aumentar la capacidad de respuesta rápida mejorando la movilidad de la fuerza y agilizar el proceso de toma de decisiones, se aprueba la *Iniciativa de preparación* (NRI)[187] en la Cumbre de Bruselas de 2018, con lo que la OTAN vuelve a dar prioridad al artículo 5 del Tratado de Washington –disuasión y defensa colectiva- en detrimento de la denominada *gestión de crisis* (FUENTE COBO, 2022, págs. 41-42).

En la Cumbre de Londres de 2019, al fin, ya asoma China en el visor de objetivos críticos por su capacidad tecnológica, su expansión económica, su agresiva política exterior y el incremento de su fuerza militar y de su capacidad nuclear. Mientras tanto, continúa la política de expansión de la Alianza y, en 2017, Montenegro ratifica el Tratado de Washington y, en 2020, Macedonia del Norte, lo que no hace sino agravar aún más la percepción soviética de amenaza que, desde su punto de vista, conlleva esta política de "puertas abiertas" que mantiene la OTAN.

En este contexto de tensión, a mediados de 2021, Rusia comienza a concentrar efectivos en las proximidades de la frontera con Ucrania y, en septiembre, lleva a cabo las maniobras militares Zapad-21 de manera conjunta con Bielorrusia[188], que conllevan un despliegue a gran escala de unidades, equipos, medios aéreos y buques de guerra en el entorno del Mar Báltico y las fronteras con Ucrania, Polonia y Lituania lo que, con el paso del tiempo, se ha interpretado como un ensayo de la invasión que se hace efectiva el 24 de febrero de 2022, cuando las fuerzas rusas penetran por la frontera Este de Ucrania en lo que Moscú define como *operación militar especial*[189], con el probable objetivo de

[187] La Iniciativa de Preparación (NATO Readiness Initiative –NRI) también es conocida como "los cuatro treinta" porque exige a los Estados miembros mantener operativos 30 batallones mecanizados, 30 buques y 30 escuadrones aéreos listos para ser empleados por la estructura de mando de la OTAN en los 30 días posteriores a la activación de la demanda.

[188] Estas "maniobras militares estratégicas" ZAPAD (Oeste/Occidente) se realizan regularmente desde 2009 cada cuatro años. En la ZAPAD-21 participaron unos 200.000 efectivos, más de 80 aviones y helicópteros de combate, unos 290 carros de combate, 240 piezas de artillería y una quincena de buques. Disponible en: https://informnapalm.org/es/comienzo-de-las-maniobras-oeste-2021-y-el-traslado-de-los-cazas-rusos-su-30-sm-a-belarus/ (19/09/2023).

[189] Referirse al conflicto con Ucrania como una *operación militar especial* permite a Putin manejar hacia el pueblo ruso la narrativa de que se trata de una *operación quirúrgica*, algo con un impacto limitado en el ámbito interno, sin afectación a la vida normal de la mayoría de los rusos. Sin embargo, más de dos años después, en marzo de 2024, el portavoz del Kremlin, Dmitry Peskov, cambia la retórica oficial y reconoce que dicha ofensiva es una guerra *de facto* que le exige a Rusia cada vez mayor implicación a resultas del soporte y la ayuda que la UE y EE.UU. están aportando a Ucrania. Este cambio de estrategia de Putin, recién *reelegido* presidente por otros seis años, busca justificar la escalada de la narrativa hacia el *conflicto* con Occidente, el hecho de que la invasión de Ucrania se haya alargado en el tiempo poniendo en tela de juicio la propia efectividad de las tropas rusas, así como la posibilidad cada vez más real de otro reclutamiento forzoso entre su población. Disponible en: https://elpais.com/internacional/2024-03-22/el-kremlin-reconoce-que-su-operacion-militar-especial-contra-ucrania-es-una-guerra.html https://www.elperiodico.com/es/internacional/20240323/rusia-cambiando-lenguaje-guerra-dv-99869724 (27/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

decapitar al gobierno ucraniano para sustituirlo en el poder, iniciándose de esta manera el mayor conflicto bélico en suelo europeo desde la Segunda Guerra Mundial.

No obstante, conforme al informe de Microsoft titulado *Defending Ukraine: Early Lessons from the Cyber War*[190], la invasión rusa se inicia el día de antes con un ciberataque masivo contra los servidores de servicios críticos de Ucrania, lo que forma parte de una *estrategia híbrida* previamente definida por el Kremlin que, junto al elemento de *guerra convencional*, suma al menos tres frentes distintos pero coordinados: los ciberataques, las operaciones de influencia y la penetración de redes de comunicación. En este mismo sentido, un año y medio después de la invasión se confirma que el ataque al satélite KA-SAT del día 23 de febrero de 2022, que provee servicios de comunicaciones satelitales a Ucrania, es producto de un malware introducido por hackers rusos en los servidores de VIASAT, la empresa administradora del sistema[191], poniendo de relieve una vez más la relevancia de las operaciones cibernéticas para los generales moscovitas. El siguiente paso de esta estrategia en el ciberespacio, una vez iniciadas las operaciones convencionales, es la evolución que lleva a los hackers rusos a abandonar los ataques disruptivos para enfocarse en el espionaje y la recopilación de datos de los sectores críticos ucranianos que puedan aportar ventaja táctica a las fuerzas de ocupación.

Los primeros meses del conflicto nos permiten identificar varias fases, a través de las cuales se puede vislumbrar la evolución de la estrategia rusa. La primera de ellas, que trascurre desde febrero a abril del 2022, se resume en la frustración del pretendido golpe de mano de Putin y la puesta en marcha de una campaña de atrición para que Ucrania acepte una salida negociada al conflicto según los términos del Kremlin. Este fracaso motiva la redefinición de los objetivos de Moscú y el comienzo de una segunda fase, que se mantiene hasta septiembre de 2022, que supone la concentración de esfuerzos en el Sur y el Este de Ucrania para integrar los óblast de Jersón, Zaporiya, Donestsk y Lugansk a la Federación Rusa[192], con la idea de garantizar la continuidad geográfica con Crimea y dificultar a Ucrania la salida al Mar Negro. La tercera fase comienza con la ofensiva ucraniana de Járkov, que supone el desmoronamiento del frente ruso y la recuperación de más de 8.000 km^2 que obligan a Rusia a la movilización parcial de 300.000 reservistas y la retirada de Jersón.

A partir de este momento Rusia pierde el liderazgo del conflicto, de manera que se dilata la toma de Bajmut hasta mayo de 2023 -la que debería haber sido el símbolo de la ofensiva de invierno rusa- y en junio saltan las desavenencias entre el Ministerio de Defensa y la compañía militar privada Wagner que, al mando de su líder Yevgueni

[190] Informe, de fecha 22 de junio de 2022, de Microsoft. Disponible en: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (19/09/2023).

[191] Esta información la difunde la propia compañía VIASAT en una nota de prensa ofrecida durante la 26ª edición de la Conferencia de Ciberseguridad Black Hat, celebrada en agosto de 2023 en Las Vegas (EE.UU.), donde se explica que el ataque constó de dos fases, una primera previa a la invasión para dejar inoperantes los módems de comunicaciones, y una segunda de carácter persistente para, en una estrategia de denegación de servicio, colapsar los servidores corporativos. Disponible en: https://cyberscoop.com/viasat-ka-hack-black-hat/ (20/09/2023).

[192] Moscú anexionó *de iure* estos cuatro óblast el 5 de octubre de 2022, aunque la comunidad internacional no lo ha respaldado por la quiebra del Derecho Internacional que supone explícitamente.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Prigozhin, en respuesta a la orden ministerial de integrar todas las unidades de combatientes voluntarios en Ucrania dentro de la estructura del Ejército ruso, llega a marchar en olor de multitudes hacia Moscú tomando las ciudades de Rostov del Don y Vorónezh, abriéndose con ello un nuevo frente -esta vez interno y que amenaza a la propia supervivencia política de Putin- que crea nuevos dilemas estratégicos al Kremlin, entre ellos qué hacer con los mercenarios sublevados y cómo recuperar la imagen pública de unidad y lealtad que tanto necesitan el ministro de Defensa ruso Shoigú y el jefe del Estado Mayor de la Defensa, el General Guerásimov (COLOM PIELLA, 2023, págs. 6-7).

En agosto, las demandas internacionales de un alto el fuego llevan a la reunión de Yedá, en Arabia Saudí, a representantes de más de treinta países con la pretensión del inicio de las conversaciones de paz sin la presencia de Rusia, aunque con la asistencia de países afines como China, India o Brasil. La *Fórmula para la Paz* propuesta por el presidente ucraniano Zelenski tiene buena acogida y supone el inicio de un acuerdo para constituir grupos de trabajo en torno al programa de paz trazado, pero sin valor añadido alguno por la ausencia de los representantes de Moscú[193].

Con la perspectiva de un final de año 2023 con un frente estancado, la OTAN apuesta por escenificar la necesidad de mantener la ayuda militar a Kiev a través de reuniones periódicas en distintos formatos[194], con el objetivo de reafirmar la eficacia del respaldo aportado por los aliados a Ucrania y hacer que Rusia, en teoría más débil política, militar y económicamente, retroceda. Sin embargo, la realidad parece indicar que el estancamiento del conflicto contraviene el apoyo político a Kiev por parte de Washington y pone en tela de juicio su capacidad de resistencia, con un partido republicano bloqueando paquetes de ayudas económicas y una sociedad en creciente oposición a mantener la financiación del país eslavo.

El invierno de 2023 parece confirmar la estrategia rusa de congelar el conflicto con el objetivo de destruir el tejido económico de Ucrania y desgastar psicológicamente a su población como primer paso para convertirla en un Estado fallido, al tiempo que desequilibra la unidad de acción en el soporte militar a Kiev por parte de EE.UU. y la

[193] En la Cumbre de Yedá el presidente ucraniano Volodímir Zelenski expuso su plan de diez puntos para la paz, entre los que se encontraba el respeto a la integridad territorial de Ucrania y la total retirada de las tropas rusas, incluidos los territorios anexados, así como la liberación de todos los prisioneros y la puesta en marcha de un tribunal penal internacional para juzgar los crímenes de guerra y lesa humanidad cometidos por los invasores. La prensa internacional dio amplia cobertura. Disponible en: https://europapress.es/internacional/noticia-reunion-yeda-coincide-plan-paz-respete-soberania-integridad-territorial-ucrania-20230805225247.html (22/09/2023).

[194] Reuniones como las llevadas a cabo por los ministros de Defensa aliados el 11 de octubre y el 29 de noviembre en la sede de la OTAN en Bruselas, o las celebradas por el grupo Ramstein también a mediados de octubre. La visibilidad de estas acciones tiene reflejo en prensa internacional. Disponible en: https://www.europapress.es/internacional/noticia-zelenski-viaja-sorpresa-belgica-participar-reunion-grupo-ramstein-otan-20231011083314.html
https://www.defensa.gob.es/Galerias/gabinete/red/2023/11/RED410.pdf
https://www.swissinfo.ch/spa/ucrania-guerra-otan_la-otan-contin%C3%BAa-su-apoyo-a-ucrania-y-avisa-de-que-rusia-hipoteca-su-futuro-a-china/49016748 (08/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

UE[195], que vislumbra un panorama preocupante si Ucrania pierde la guerra. De hecho, a mediados de febrero de 2024 el debate sobre la situación real del frente es público al tiempo que se trata de entender las razones del fracaso de la contraofensiva de verano ucraniana, que lleva a Zelenski a plantearse la sustitución del extraordinariamente popular jefe de las Fuerzas Armadas, Valery Zaluzhmi, prueba de la profunda división interna alimentada por la creciente convicción de que Europa y, fundamentalmente, EE.UU., han dejado de creer que Kiev pueda recuperar el territorio perdido frente a Rusia. Esta duda se acrecienta con la retirada de Avdivka y su entrega a las tropas del Kremlin en vísperas de conmemorarse el segundo aniversario de la invasión, lo que supone para los rusos el principal trofeo de campaña y la mayor victoria moral desde la toma de Bajmut[196], cuestión ampliamente aprovechada por el ecosistema propagandístico prorruso para tratar de consolidar la percepción del desfallecimiento ucraniano y la voluntad inquebrantable del Kremlin para alcanzar sus objetivos.

En mayo de 2024, tras el comienzo del nuevo mandato presidencial de Vladimir Putin y el cambio de su ministro de Defensa, Serguei Shoigu, el conflicto en suelo ucraniano experimenta un giro propiciado por la intensificación de las acciones del ejército ruso sobre la región de Jarkov, en una zona que parecía consolidada por Ucrania, lo que implica un cambio de tendencia favorable a Moscú. Esta cuestión enciende las alertas tanto en Kiev como en el corazón de Europa y la OTAN por las consecuencias que pudiera conllevar. Aun siendo cierto que el desgaste militar afecta a ambos contendientes, parece más grave para el bando ucraniano, muy afectado por el largo paréntesis sufrido en el envío de material por parte de Occidente y por el propio agotamiento de los combatientes, hecho que se constata por la decisión del Ministerio de Justicia ucraniano de habilitar el reclutamiento de presos y la rebaja firmada por Zelenski de la edad mínima de reclutamiento de ciudadanos, de 27 a 25 años, de cara a afrontar la campaña de verano en el frente que, sin duda, se presenta crítica.

Con la campaña de verano Ucrania consigue uno de sus más ansiados objetivos: llevar la guerra al territorio del invasor hasta un nivel inédito hasta el momento[197]. El 6 de

[195] Ucrania se esfuerza para que la ayuda de occidente no decaiga; Moscú pone sus ojos en el G7. FRANCE24, 6 diciembre 2023. Disponible en: https://www.france24.com/es/europa/20231206-ucrania-se-esfuerza-para-que-la-ayuda-de-occidente-no-decaiga-mosc%C3%BA-pone-sus-ojos-sobre-el-g7 (27/12/2023).

[196] La retirada ucraniana de Avdivka tiene amplio seguimiento internacional no solo porque se trata de la entrega a Rusia de uno de los primeros territorios ocupados, sino por el contexto de duda de la continuidad del apoyo internacional a la guerra. Amplia cobertura por prensa internacional. Disponible en: https://elpais.com/internacional/2024-02-17/ucrania-se-retira-de-avdiivka-en-la-mayor-victoria-rusa-en-un-ano.html
https://www.france24.com/es/europa/20240217-ucrania-anuncia-su-retiro-de-avdiivka-una-ciudad-estrat%C3%A9gica-en-la-guerra-contra-rusia
https://www.elperiodico.com/es/internacional/20240217/directo-guerra-rusia-ucrania-ultimas-noticias-conflicto-97242304 (18/02/2024).

[197] Amplia repercusión en prensa de la ofensiva ucraniana. Disponible en: https://www.bbc.com/mundo/articles/c0l8znxl8w8o
https://www.france24.com/es/europa/20240819-ucrania-ampl-su-ofensiva-en-kursk-mientras-rusia-asedia-zonas-de-donetsk-y-obliga-a-evacuaciones
https://elpais.com/internacional/2024-08-20/ucrania-abre-un-segundo-flanco-de-ataque-en-territorio-ruso.html (27/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

agosto el ejército ucraniano inicia el ataque a la provincia rusa de Kursk y toma el control de una veintena de poblaciones, liderando la narrativa con el recurso a la imagen bíblica de la gesta de David frente a Goliat el filisteo, instrumentalizando la alegoría del débil que inflige daño al poderoso. Al mismo tiempo, con este movimiento Ucrania busca mejorar su posición a la hora de negociar el fin del conflicto y obligar a Putin a mover ficha en su política interna, por el desgaste de imagen institucional y personal sufrida ante la evidencia de las bajas rusas y la *entrada en casa* de la guerra. Todo ello supone un punto de inflexión por cuanto no solo alienta al avance ucraniano y al compromiso de los aliados con su causa, sino que también deteriora la imagen del ejército ruso sacando a relucir sus carencias para defender la retaguardia. Como respuesta, Moscú retoma su estrategia de ataque a las infraestructuras energéticas del país ocupado, interrumpiendo el suministro de servicios esenciales como clara advertencia de las penurias que habrá de pasar la población civil a medida que se acerque el invierno, sempiterno aliado del Kremlin.

A finales de septiembre, Volodímir Zelensky presiona a Washington para que flexibilice las restricciones sobre el uso de misiles de largo alcance para atacar a Rusia, al tiempo que impulsa la vía diplomática y presenta un *Plan de Victoria* a los candidatos presidenciales estadounidenses, Trump y Harris, buscando preparar cualquiera de los escenarios que pudiera deparar el duelo en las urnas del 5 de noviembre de 2024[198] y, en especial, desactivar en la medida de lo posible las oscuras perspectivas de futuro para Ucrania en caso de que ganase las elecciones el republicano, que podría buscar un *final rápido* al conflicto. Semanas después el líder ucraniano hace lo propio con los aliados europeos, prosiguiendo la estrategia de crear lo que Kiev considera unas condiciones apropiadas para un final justo de la guerra contra Moscú[199].

Sin embargo, conforme se acerca el final de 2024, se precipitan las perspectivas de una negociación forzada con la aceptación implícita de pérdida territorial para Kiev, motivada por el lento pero determinado avance ruso en los frentes de batalla de Odesa, Jerson y Zaporiyia, la reafirmación diplomática del Kremlin ejerciendo como anfitrión en la XVI cumbre de los BRICS en Kazán[200], la reelección de Donald Trump como Presidente

[198] Amplia repercusión en prensa. Disponible en: https://es.euronews.com/my-europe/2024/09/27/zelenski-se-reune-con-trump-en-nueva-york-para-presentarle-su-plan-de-victoria https://www.bbc.com/mundo/articles/cp952pypj37o (08/10/2024).

[199] Amplia repercusión en prensa. Disponible en: https://es.euronews.com/my-europe/2024/10/11/volodimir-zelenski-presenta-a-sus-aliados-el-plan-de-victoria-de-ucrania-en-su-gira-por-eu https://www.europapress.es/internacional/noticia-zelenski-presenta-londres-plan-victoria-medio-demandas-armas-mas-potentes-20241010145912.html https://www.elcorreo.com/internacional/europa/zelenski-presenta-plan-victoria-fugaz-viaje-europeo-20241010165338-ntrc.html (11/10/2024).

[200] La XVI cumbre de los BRICS, celebrada en Kazán (Rusia) del 22 al 24 de octubre de 2024, congrega a más de 30 países que representan el 45,5 % de la población mundial, el 43,34% de la producción mundial de petróleo y casi el 36% del PIB mundial. En esta ocasión, además, cuenta con la presencia del Secretario General de NNUU, Antonio Guterres, lo cual revela la fortaleza diplomática de Moscú, dando impulso al mismo tiempo a esta alianza de países, alternativa al modelo global occidental que, entre otras cuestiones, amenaza la actual configuración comercial de sistema de pagos en las relaciones internacionales con su modelo de Brics Pay, ajena al referente del dólar y la unilateralidad impuesta por EE.UU. Disponible en: https://efe.com/mundo/2024-10-23/cumbre-de-los-brics-kazan-rusia/

Ediciones Universidad de Salamanca | CC BY-NC-ND

de EE.UU.[201] y el propio desgaste de la población ucraniana que, cada vez más, ve a Rusia como un enemigo demasiado fuerte al que causar daños de entidad suficiente como para hacerle perder la guerra[202]. De hecho, la reunión de Trump con Zelensky en diciembre de 2024, con ocasión de la reapertura oficial de Notre Dame de París, se traduce en una flexibilización del discurso del mandatario ucraniano respecto a Rusia, mientras el estadounidense solicita un alto el fuego inmediato y negociaciones entre las partes, a lo que parecería abierto el Kremlin sobre la base del reconocimiento de la nueva realidad territorial que se manejaba en los Acuerdos de Estambul, de marzo de 2022[203].

La nueva investidura presidencial de Donald Trump el 20 de enero de 2025 conlleva, entre otros, un drástico giro de la política internacional de los EE.UU. con efectos inmediatos en la guerra ruso ucraniana y, por ende, en el papel de la UE en dicho conflicto. La reunión que, apenas un mes después, mantiene Volodímir Zelenski en el despacho oval de la Casa Blanca con su máximo dignatario y el vicepresidente J.D. Vance, se desarrolla en un entorno de enfrentamiento y calculada tensión que lleva al presidente ucraniano a suspender el pretendido acuerdo sobre minerales críticos que EE.UU. pone sobre la mesa de negociaciones para alcanzar la, de repente, ansiada paz que, a todas vistas, va más allá del cese de las hostilidades[204]. La mirada geopolítica experta alcanza a ver que el futuro acuerdo de paz en Ucrania que quiere el presidente Donald Trump no se limita al alto el fuego entre las partes, sino que pretende redefinir el equilibrio estratégico global para, tal vez ansiando rememorar tiempos pretéritos,

https://legrandcontinent.eu/es/2024/10/22/comienza-la-cumbre-anual-de-los-brics-en-kazan-en-rusia/ (17/11/2024).

[201] La victoria de Trump abre un abanico de incertidumbres en el Viejo Continente porque, como dejó entrever en su anterior mandato, el líder estadounidense pretende reducir su intervención en el conflicto entre Moscú y Kiev, lo que obliga a la Unión a definirse individualmente en su compromiso con la defensa de Ucrania. Además, durante su campaña electoral, el candidato republicano se comprometió a poner fin a la guerra buscando una salida negociada que, sin duda, habrá de llevar anejas concesiones territoriales por parte de Ucrania a Rusia, muy probablemente en las regiones del Donbás y Crimea.

[202] Según una encuesta publicada en octubre de 2024 por el Instituto Internacional de Sociología de Kiev (KI IS), entre diciembre de 2023 y septiembre de 2024, en todas las regiones de Ucrania, salvo en la zona occidental más alejada del frente ruso, hubo menos personas que creían en la posibilidad de éxito en la guerra. En concreto, el mayor descenso de ucranianos que confían en ganar la guerra se observa en la zona oriental, donde en diciembre de 2023 el 79% creía en la posibilidad de éxito, y en septiembre de 2024 baja hasta el 67%. Al mismo tiempo, en esta zona, el 24% de los ucranianos cree que Rusia es demasiado fuerte para ser vencida sin el apoyo occidental. Disponible en: https://www.kiis.com.ua/?lang=eng&cat=reports&id=1438&page=1 (17/11/2024).

[203] En estos Acuerdos de 2022 el presidente Putin condicionaba la paz, entre otras cuestiones, a que Ucrania no se uniese a la OTAN y redujese su arsenal nuclear como garantía de seguridad de las fronteras rusas. Disponible en:https://urgente24.com/mundo/acuerdos-estambul-el-plan-ruso-frenar-la-guerra-ucrania-n580406
https://mondiplo.com/la-pista-de-estambul
https://diario-octubre.com/2024/06/18/el-new-york-times-publica-el-tratado-de-paz-firmado-en-2022-por-ucrania-y-rusia/ (14/12/2024).

[204] Repercusión en prensa internacional de esta entrevista entre Zelenski y Trump que puede consultarse en: https://www.rtve.es/noticias/20250228/trump-zelenski-encuentro-casa-blanca/16471009.shtml
https://www.bbc.com/mundo/articles/clyd11np8p7o
https://www.elespanol.com/mundo/20250228/video-momento-tenso-trump-zelenski-discuten-gritos-casa-blanca-planeta/927657740_0.html (14/03/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

compartir la influencia sobre Ucrania con el Kremlin, que estaría encantado de reconfigurar la arquitectura de seguridad del Viejo Continente sobre la base de unas relaciones bilaterales con EE.UU. más fuertes gracias a acuerdos en otras áreas de interés mutuo. En definitiva, llegar a una paz negociada en Europa pero sin Europa.

Mientras el Kremlin intensifica sus ataques en Donetsk y Odessa y recupera terreno en la región rusa de Kursk, el alto mando ucraniano se encuentra en una encrucijada de difícil solución por cuanto el abandono de estas posiciones perjudicaría la posición de Kiev en la mesa negociadora del alto el fuego que, el 11 de marzo, se reúne en Yeda (Arabia Saudí)[205], bajo la supervisión del Secretario de Estado estadounidense Marco Rubio, y el asesor de Seguridad Nacional Mike Waltz. Estos proponen un alto el fuego provisional inmediato de treinta días, prorrogable de mutuo acuerdo entre las partes, pero sujeto a la aceptación e implementación simultánea por parte de la Federación Rusa, la cual se muestra inicialmente ambigua al ofrecimiento para, de alguna forma, reforzar también su postura de negociación.

Este complejo y delicado posicionamiento en el tablero internacional obliga al resto de jugadores a mover sus fichas. Por ello se convoca en París, el mismo día 11 de marzo, a los jefes militares de treinta y cuatro países de la UE y de la Alianza para definir el posicionamiento aliado en la resolución del conflicto[206]. Tres días después, el Secretario General de la OTAN, Mark Rutte, debe lidiar en la Casa Blanca[207] con la maniobra envolvente de Trump construida sobre su pretendida anexión de Groenlandia y la crítica al gasto en defensa de los, por ahora, aliados europeos como condición *sine qua non* para su apoyo militar.

---

[205] Reflejo en prensa de la referida mesa de negociación del alto el fuego en Ucrania disponible en: https://legrandcontinent.eu/es/2025/03/11/propuesta-de-alto-el-fuego-inmediato-en-ucrania-el-texto-completo-de-la-declaracion-conjunta-con-estados-unidos/
https://www.rtve.es/noticias/20250311/eeuu-ucrania-arabia-saudi-negociaciones-paz/16485603.shtml
https://www.elperiodico.com/es/internacional/20250310/ucrania-alto-fuego-parcial-rusia-negociaciones-eeuu-arabia-saudi-115148191 (14/03/2025).

[206] A esta reunión en París asisten los representantes de Albania, Alemania, Australia, Austria, Bélgica, Bulgaria, Canadá, Chipre, Croacia, Dinamarca, España, Estonia, Finlandia, Grecia, Hungría, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Macedonia, Montenegro, Noruega, Nueva Zelanda, Holanda, Polonia, Portugal, República Checa, Rumania, Eslovaquia, Eslovenia, Suecia y Turquía. La prensa internacional se hace eco de esta reunión. Disponible en: https://elpais.com/internacional/2025-03-11/macron-reune-en-paris-a-31-jefes-militares-de-paises-dispuestos-a-implicarse-en-una-paz-en-ucrania.html
https://www.france24.com/es/europa/20250311-par%C3%ADs-30-naciones-de-europa-y-la-otan-debaten-sobre-la-defensa-y-la-paz-en-ucrania
https://www.france24.com/es/europa/20250311-macron-urge-a-sus-aliados-a-definir-garant%C3%ADas-de-seguridad-cre%C3%ADbles-para-ucrania-en-cumbre-de-par%C3%ADs
https://www.ansalatina.com/americalatina/noticia/union_europea/2025/03/11/paris-primer-paso-para-garantias-seguridad-en-kiev_e439b8ae-bec6-4e69-926f-28eaab84aab3.html (16/03/2024).

[207] Reflejo en prensa de la reunión del presidente Trump con el Secretario General de la OTAN Mark Rutte, el 14 de marzo de 2025. Disponible en: https://www.infobae.com/america/mundo/2025/03/13/el-jefe-de-la-otan-se-reunio-con-trump-en-la-casa-blanca-y-se-mostro-cauto-al-hablar-de-gastos-en-defensa-y-groenlandia/
https://es.euronews.com/2025/03/14/rutte-ser-reune-con-trump-en-washington-y-este-vuelve-a-insistir-con-la-anexion-de-groenla (14/03/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

En este contexto de aceleración vertiginosa para dar solución al conflicto, las diplomacias estadounidense y rusa acuerdan una conversación telefónica entre los mandatarios de ambos países para comenzar a sentar las bases de un alto el fuego temporal entre Moscú y Kiev[208] que podrían constituir el primer paso hacia la paz. Las derivadas geopolíticas del acercamiento entre EE.UU. y la Federación de Rusia son profundas por cuanto revelan una interpretación utilitarista de las relaciones bilaterales con potencial para redefinir el sistema de alianzas establecido, lo cual obliga a la UE a reconsiderar su autonomía estratégica estrechamente vinculada a su capacidad de defensa y a su papel como actor internacional relevante. Sin embargo, las prisas de Donald Trump por alcanzar una salida pactada a la guerra no coinciden con el *tempo* con que Putin interpreta su agresión a Ucrania. Después de más de tres años de conflicto el tiempo corre a favor del Kremlin que, conocedor de esta ventaja, va a negociar desde una posición firme para imponer su objetivo primigenio: paz por territorio. Prueba de ello son las exigencias de Putin sobre el cese de toda ayuda militar a Ucrania y su no entrada en la OTAN como punto de partida para detener, temporalmente, los ataques contra la infraestructura energética ucraniana. Una vez más, parece confirmarse que las prisas no son buenas consejeras.

2.2.5. El Concepto Estratégico de Madrid

El Informe OTAN 2030 encargado por Jens Stoltenberg a principios de 2021 tenía tres objetivos: la readaptación de la Alianza al escenario de competición entre potencias, la necesidad de dar respuesta a los desafíos globales y, desde luego, atender a las ciberamenazas y estrategias híbridas consustanciales al actual contexto internacional (COLOMINA, 2022, pág. 88).

Partiendo de este trabajo previo realizado, la Cumbre de Madrid de junio de 2022 asume como reto principal el reforzamiento del vínculo transatlántico y sus valores[209] para, de nuevo entre competidores sistémicos, garantizar la defensa colectiva de sus socios con un *enfoque 360º* articulado sobre tres pilares: la disuasión y defensa, la prevención y gestión de crisis, y la seguridad cooperativa. Sin duda, ello ha coadyuvado a que el catálogo de retos que contempla el Concepto Estratégico de Madrid[210] sea, esta vez sí, plenamente acertado por cuanto enumera las *principales amenazas globales para la Alianza* a corto, medio y largo plazo y advierte la interconexión entre ellas, definiendo desde el inicio un área euroatlántica que *no está en paz*.

---

[208] La llamada entre Trump y Putin para acordar un alto el fuego y comenzar a sentar las bases de una salida negociada al conflicto se produce el martes 18 de marzo de 2025. El seguimiento en prensa internacional es de amplia cobertura. Puede consultarse en: https://www.eldiario.es/internacional/trump-busca-final-rapido-guerra-ucrania-putin-no-prisa_1_12153752.html
https://www.nytimes.com/es/2025/03/20/espanol/mundo/trump-putin-llamada-ucrania.html
https://www.bbc.com/mundo/articles/ce30e1qndveo (22/03/2025).

[209] Recordemos que el espíritu original de la OTAN se vincula con tres grandes objetivos: el alineamiento con la Carta de las Naciones Unidas, la salvaguarda de los principios de democracia, libertad y legalidad, y la defensa de la paz y la estabilidad en la zona del Atlántico Norte.

[210] Nuevo Concepto Estratégico de la OTAN (Madrid, 29 de junio de 2022). Disponible en: https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf (22/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

La primera de estas amenazas, la más importante y directa para la OTAN, es la Federación de Rusia a la que ya no se considera como socia. El enfrentamiento de su sistema autocrático contra los principios de la democracia, sus tácticas híbridas que constantemente tratan de socavar los valores occidentales y su agresiva política exterior son las claves de este señalamiento. No obstante, pese a ser considerada una amenaza y siguiendo los valores de la Alianza, se trata de mantener abiertos diferentes canales de comunicación con Moscú. Ello ayuda, por un lado, a buscar la paz y el respeto al Derecho Internacional, seriamente conculcado con la invasión rusa de Ucrania, y de otro, a evitar el discurso del victimismo ruso y su autoexclusión.

A continuación, la segunda amenaza sistémica se centra en el terrorismo internacional, la cual incide de manera más directa en la seguridad de los ciudadanos, interactuando con los problemas de violencia, demográficos, climáticos, institucionales, económicos y políticos que presenta el Flanco Sur[211], cuya inestabilidad afecta a escala global a la seguridad humana y de los propios Estados.

La tercera amenaza para la Alianza es la República Popular China como nuevo rival sistémico que, mediante el empleo de todas las herramientas políticas, económicas y militares a su alcance -entre las que se incluyen las operaciones híbridas-, trata de controlar sectores tecnológicos e industriales críticos para dominar las redes de suministro de productos esenciales. A esto hay que añadir su asociación estratégica con Rusia, en cuyo contexto se enmarca el desarrollo de tecnologías innovadoras que, en ocasiones, parten de la ventaja obtenida a través del espionaje industrial[212].

En cuarto lugar se señala al ciberespacio, como objeto de disputa permanente, y la inversión en desarrollo e innovación que los adversarios de la Alianza están realizando en la búsqueda de la primacía tecnológica. También se hace una referencia a la actual crisis del control de armamentos, desarme y no proliferación, señalando directamente la violación de obligaciones y compromisos por parte de Rusia, Irán, Corea del Norte, Siria y China, que siguen desarrollando programas nucleares, ampliando sus arsenales y mejorando sus sistemas de lanzamiento.

La última de las amenazas es la referida al cambio climático que, por primera vez, tiene cabida en un Concepto Estratégico augurando profundos impactos en la Alianza por su afectación directa al modo de operar las Fuerzas Armadas, al efecto multiplicador de crisis, al carácter de agente acelerador de conflictos geopolíticos y las evidentes catástrofes medioambientales que causa con devastadores efectos sobre la población.

[211] Norte de África, Sahel y Oriente Medio.

[212] En este contexto cabe citar el *milagroso* salto tecnológico que China ha conseguido con su cazabombardero de quinta generación, el J-20 *Mighty Dragon*, para cuyo desarrollo no ha necesitado transitar por el paso intermedio de los cazas de cuarta generación tipo F-18 o los Eurofighter. De hecho, la similitud con los F-22 *Raptor* y F-35 *Lightning II* estadounidenses de quinta generación es apreciable incluso para el ojo no experto. Disponible en:https://www.larazon.es/internacional/increible-historia-familia-china-que-logro-espiar-aviones-combate-f35-eeuu_20231227658c61b8a4afb00001d07822.html https://www.diariolasamericas.com/economia/china-crea-aviones-combate-tecnologia-robada-eeuu-n5332195 (27/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Frente a este elenco de desafíos se presenta la estrategia de *disuasión y defensa* como primera línea del enfoque 360º, a través del cual poder articular una respuesta ante cualquier amenaza *como queramos, cuando queramos y en el dominio que elijamos*[213]. La OTAN vuelve a utilizar el recurso de la defensa adelantada -fuerzas multidominio y combinadas- y la defensa integrada mediante la implantación de un *nuevo modelo de fuerzas* -fuerzas de tierra, mar y aire tanto desplegadas como de refuerzo- para su disponibilidad operativa, con una estructura de mando y control integrados, y el compromiso de alineación de los planes de defensa de sus aliados con los planes regionales que el SACEUR elabora para responder a la amenaza actual.

Con el objetivo de garantizar el uso seguro y el acceso sin restricciones al espacio ultraterrestre y al ciberespacio, así como la respuesta ante cualquier amenaza o ataque en dichos entornos, se plantean varias *líneas de acción* del enfoque 360º:

1. La primera de ellas pivota sobre las tres caras de un triángulo. La primera se encarga de señalar como objetivos críticos la innovación y el aumento de la inversión en la transformación digital, la ciberdefensa y la protección de redes e infraestructuras críticas para preservar la ventaja tecnológica y militar, en un escenario internacional de crecientes sabotajes a infraestructuras críticas que exigen, por parte de la OTAN, una respuesta inmediata sobre la base del intercambio de inteligencia[214] frente a ataques a servicios esenciales de comunicaciones, como los perpetrados contra cables submarinos de fibra óptica[215], que se están convirtiendo en la amenaza más acuciante contra la seguridad de los aliados. En segundo lugar, en base a la consideración de que el Derecho Internacional es de aplicación en el ciberespacio[216] y en el espacio, entender que cualquier actividad maliciosa u operación hostil en estos dominios puede alcanzar el nivel de *ataque armad*o y, como tal, justificar que se invoque el artículo 5 del Tratado de Washington. Idéntica consideración se contempla

[213] Vid. Supra. Apartado 1.1.2.

[214] En este sentido se pronuncia el Secretario General, Mark Rutte, en la reunión de diciembre de 2024 de los ministros de Asuntos Exteriores de la OTAN, respecto al intercambio de inteligencia, la mejor protección de las infraestructuras críticas y la potenciación de la ciberdefensa para contrarrestar las actividades hostiles rusas. Disponible en: https://www.nato.int/cps/en/natohq/news_231006.htm (14/12/2024).

[215] Puede consultarse la referencia en prensa de estos daños. Disponible en:
https://efe.com/economia/2024-11-19/danos-cables-submarinos-telecomunicaciones-baltico/
https://www.dw.com/es/cables-da%C3%B1ados-en-el-b%C3%A1ltico-guerra-h%C3%ADbrida-en-el-fondo-del-mar/a-70853517
https://www.swissinfo.ch/spa/investigan-una-aver%C3%ADa-en-cable-de-telecomunicaciones-submarino-entre-finlandia-y-alemania/88210823 (14/12/2024).

[216] En este sentido puede consultarse el *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, elaborado por un grupo de expertos internacionales en colaboración con el NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), y que conforma actualmente la base de la doctrina existente al respecto. La edición de 2017 (Manual Tallinn 2.0) contiene 154 reglas con las que se da respuesta a 20 cuestiones de interés relacionadas con el ciberespacio y el Derecho Internacional: la soberanía, la diligencia debida, la jurisdicción, el derecho de responsabilidad internacional, las operaciones cibernéticas no reguladas *per se* por el Derecho Internacional, el Derecho Internacional de los derechos humanos, el derecho diplomático y consular, el derecho del mar, el derecho del aire, el derecho del espacio, el Derecho Internacional de las telecomunicaciones, las operaciones de paz, la prohibición de intervención, el uso de la fuerza, el derecho general de los conflictos armados, la conducción de hostilidades, algunas personas, objetos y actividades, la ocupación y la neutralidad.

Ediciones Universidad de Salamanca | CC BY-NC-ND

también respecto a las operaciones híbridas contra los aliados. La última cara de este triángulo se refiere a la capacidad nuclear de la OTAN, sobre la que se mantiene el argumentario original que respalda su existencia como garantía de paz y de seguridad, base de la disuasión creíble y elemento de estabilidad estratégica frente al resto de potencias con semejante potencial.

2. La segunda línea de acción del enfoque 360º es la *prevención y gestión de crisis* que puedan afectar a la seguridad aliada, y que supone mantener las operaciones multinacionales para estabilizar conflictos, luchar contra el terrorismo o afrontar situaciones de prevención y ayuda humanitaria, para lo que la OTAN se coordinará con organizaciones como NNUU, la UE, la Organización para la Seguridad y Cooperación en Europa (OSCE), la Unión Africana y otras similares.
3. El Concepto Estratégico de Madrid fija la tercera línea de acción del enfoque 360º en la *seguridad cooperativa* afirmando, en lo que consideramos que continúa siendo una huida hacia adelante, que *la ampliación de la OTAN ha sido* un *éxito histórico.* En consonancia, mantiene la política de puertas abiertas bajo unas condiciones que no siempre se han cumplido: ha de tratarse de Estados democráticos europeos, que compartan los valores aliados, dispuestos y capaces de asumir las responsabilidades y obligaciones derivadas del ingreso y, no menos importante, que su adhesión contribuya a la seguridad común del resto de miembros. En una referencia expresa a Bosnia Herzegovina, Georgia y Ucrania, se compromete la Alianza a apoyar su incorporación y a intensificar el diálogo político y la cooperación en ese sentido.

Por lo que respecta al reforzamiento de lazos con estructuras regionales, se alude específicamente a la importancia de la UE como *socio único y esencial* para la OTAN, incidiendo en el profundo vínculo entre ambas y el carácter complementario de sus funciones, creando espacio para reconocer el valor de la Política Exterior y de Seguridad Común de la UE (PESC) y su positiva contribución a la seguridad transatlántica y global[217], no sin dejar de evocar el aumento del presupuesto de defensa como parte esencial del compromiso para la financiación común de las infraestructuras, las capacidades y las fuerzas de la Alianza. Actualmente la OTAN mantiene su estrategia de relaciones con organizaciones regionales de seguridad y defensa como el *Diálogo Mediterráneo*[218] y la *Iniciativa de Cooperación de Estambul*[219], piezas clave de estabilidad en el entorno geográfico de interés compartido, además de los denominados *Partners around the*

[217] Como veremos más adelante, tanto la OTAN como su principal componente, los EE.UU., interpretaron inicialmente como una amenaza para el vínculo transatlántico el desarrollo de la PESC, pero la evolución de la misma ha demostrado que la UE tiene aún mucho camino por delante para consolidar una defensa militar autónoma dirigida por su propia estrategia común. Además, el nuevo foco de atención de EE.UU., y de la OTAN, que mira a China y al Indo-Pacífico, impone una economía de esfuerzos y recursos que da la bienvenida a una mayor implicación de Europa en su propia seguridad, como oportunidad para compartir costes y responsabilidades en el mantenimiento del flanco euro-atlántico.

[218] El Diálogo Mediterráneo está compuesto por Jordania, Israel, Egipto, Marruecos, Argelia, Túnez y Mauritania.

[219] La Iniciativa de Cooperación de Estambul integra a Kuwait, Bahréin, Qatar y Emiratos Árabes Unidos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

World[220] para la intervención en operaciones aliadas y la participación en ejercicios y programas de formación.

Finalmente, como clave del éxito futuro de la OTAN para seguir manteniendo *nuestra paz, nuestra libertad y nuestra prosperidad* se apuesta por el discurso tradicional basado en la continuidad del vínculo transatlántico y el compromiso común y equitativo de los aliados, al tiempo que se hace una mención específica a la resiliencia a nivel nacional y de toda la Alianza frente a las actuales amenazas para "resistir, responder y recuperarnos rápidamente de los *shocks* y de las disrupciones estratégicas"[221].

A la luz de los acontecimientos que se han producido con posterioridad, entre ellos la Cumbre de la OTAN en Vilna (Lituania) en julio de 2023, cabe concluir que el vínculo transatlántico se ha revitalizado y ha encontrado en el apoyo a Ucrania frente a la invasión rusa un factor impulsor y de consenso, a través del cual se ha conseguido no solo estrechar lazos entre Europa y EE.UU. sino, también, atraer "a nuevos miembros, como los neutrales Suecia y Finlandia, que han corrido a acogerse bajo su paraguas", e incluso ampliar el rango de partenariado con Oriente Medio, el Sahel y Norte de África, y reforzarlo con la UE (ARTEAGA & SIMÓN, 2022).

De hecho, los planes regionales de la OTAN presentados en Vilna suponen la mayor reorganización de la Alianza desde el final de la Guerra Fría y un gran paso adelante en la comunicación estratégica para llegar a la población civil y tratar de ganar su apoyo, elemento imprescindible para mantener un compromiso a largo plazo en Ucrania que ponga freno al denuedo expansivo del Kremlin (ARTEAGA & SIMÓN, 2023).

2.2.6. Balance y situación actual tras 75 años de OTAN: ¿anacronismo o pilar del equilibrio de fuerzas?

Qué duda cabe que la única manera de mantener vigente un proyecto de la envergadura y el calado de la OTAN requiere un esfuerzo de adaptación continuo a la realidad de la amenaza para reorientar la estrategia con la que alcanzar el objetivo que la justifica, que no es otro que procurar la defensa conjunta de sus miembros como uno solo.

A tenor de los hechos, durante la Guerra Fría, la Alianza cumplió su cometido dando estabilidad y seguridad al área noratlántica contrarrestando de manera equilibrada al oponente soviético, frente al que bastó la disuasión. Sin embargo, en nuestra opinión, con el cambio de siglo la OTAN pierde gran parte de las referencias que venían guiando su rumbo y, desde entonces, su estrategia abandona la gestión anticipativa para tornarse eminentemente reactiva y expansiva, dando la impresión de estar superada por el escenario altamente cambiante que ha supuesto la era digital y la asimetría de los conflictos que la acompañan.

[220] Entre estos países podemos citar a Australia, Colombia, Japón, Corea del Sur o Nueva Zelanda, entre otros.
[221] Nuevo Concepto Estratégico de la OTAN, Op.Cit. página 11.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Para analizar el posible origen de esta deriva debemos recordar que el Tratado de Washington define su pilar central organizativo a través del artículo 4, que establece la consulta y el consenso en los acuerdos como modo de adoptar las decisiones y para lo cual, lógicamente, precisa de la cohesión de los aliados en torno a los principios y valores que componen el acervo de las democracias occidentales, patrón común de los doce miembros fundacionales. Si se agrieta esta columna vertebradora toda la estructura corre grave riesgo de colapso, pues será imposible acordar objetivos comunes que guíen la estrategia de actuación futura de la OTAN. Y aquí radica el *quid* de la cuestión.

La realidad es que, en el contexto internacional actual, la Alianza afronta un gran reto para mantener la afinidad de criterio de sus socios a la hora de consensuar sus actuaciones. Varias circunstancias coadyuvan a esta situación, siendo la primera de ellas las nuevas amenazas híbridas que han supuesto para las democracias un continuo frente de ataque, articulado a través de injerencias extranjeras que tratan de socavar sus instituciones y generar dudas sobre la legitimidad de sus procesos, polarizando el debate social y político interno -génesis del odio y de la radicalización en los ciudadanos- y, como tal, actuando como vía de entrada para postulados nacionalistas y extremistas que dan pábulo a las autocracias.

En segundo lugar, el hecho de que los propios Estados evolucionan en sus políticas de manera autónoma e independiente, conforme a sus intereses nacionales y en un contexto de circunstancias históricas no siempre resueltas de manera satisfactoria que pueden afectar a sus decisiones, pudiendo llevarlos a defender posturas no compartidas por el resto de aliados en un momento determinado.

En tercer lugar, las consecuencias derivadas de la línea expansionista de la Alianza, iniciada en el año 1999, hacia países históricamente vinculados al Pacto de Varsovia, algunos de los cuáles han transitado desde el comunismo para llegar a ser miembros de un escogido club en el que aún no se sienten plenamente cómodos con todos los socios, con los que comparten valores pero con los que difieren en la perspectiva con la que miran el mundo en que conviven.

Y en cuarto y último lugar, la que podríamos denominar la *paradoja de Europa*, hija favorita de la Alianza que, conforme va creciendo y definiendo su identidad, quiere alcanzar su propia cuota de *autonomía estratégica* con la que reivindicarse como proveedor de seguridad, por lo que ve a la OTAN "como una organización necesaria y útil, pero a la vez, como una incómoda expresión de la hegemonía norteamericana en asuntos de seguridad y defensa colectiva" (VILANOVA, 2022, pág. 124) lo cual, a su vez, genera recelos en EE.UU., cuya superioridad militar y económica pretende hacer valer para decidir unilateralmente cómo y cuándo los intereses aliados deben imbricarse con los suyos propios. Clara expresión de esta pulsión europea que busca su autonomía defensiva mientras sigue viendo en la OTAN a su fiel compañera de viaje, es el *Plan ReArm Europe* incardinado en el *Joint White Paper for European Defence - Readiness 2030*[222], presentado en marzo de 2025 como la respuesta de la Unión al cambio de

[222] Joint White Paper for European Defence - Readiness 2030. Brussels, 19.3.2025. JOIN(2025) 120 final. Disponible en: https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf (23/03/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

paradigma en el contexto geopolítico que suponen la invasión rusa de Ucrania y la relección de Donald Trump como Presidente de los EE.UU., con su política revisionista de alianzas y principios de comportamiento en el orden internacional. Así, mientras la administración Trump exige a la UE mayor inversión en su propia defensa, ésta confía en la OTAN para el desarrollo conjunto y colaborativo de capacidades, como forma para obtener de manera rápida y efectiva la interoperabilidad de equipos, medios y sistemas de combate, dando por sentado que:

> "NATO remains the cornerstone of collective defence of its members in Europe. EU-NATO cooperation is an indispensable pillar for the development of the EU's security and defence dimension. The EU's unique tools of regulatory power and financial instruments help the 23 EU Member States in NATO to achieve their capability targets"[223].

Son estas circunstancias las que, a nuestro entender, pueden explicar la ralentización en la toma de decisiones en el seno de la OTAN, lo que la obliga a una permanente carrera para tratar de adelantarse al futuro pero que, producto de esa lentitud determinada por la evidente falta de cohesión interna, la lastran y la mantienen frenada en un presente que le obliga a reaccionar prácticamente en tiempo real, lo que perjudica su capacidad de disuasión y de respuesta.

Como ejemplo de ello puede citarse a Turquía, cuya ofensiva en el Norte de Siria en octubre de 2019 contra las Fuerzas Democráticas Sirias por su vinculación con el independentista Partido de los Trabajadores del Kurdistán (PKK), deja clara la falta de coordinación dentro de la OTAN, aviso de un Tayyip Erdogan que, en mayo de 2023, inicia una tercera legislatura con una deriva autoritaria y nacionalista que hace que su país se parezca "poco a la Turquía de 1952, cuando ingresó en la Alianza como parte de la política de contención de EE.UU.", y cuyas "rivalidades territoriales con Grecia complican más las relaciones intra-OTAN y las relaciones UE-Turquía" (DÍAZ RODRÍGUEZ, 2020, pág. 18), cuestiones de nuevo evidenciadas por el veto turco al ingreso en la Alianza de Suecia y Finlandia, justificado por las supuestas relaciones de estos países nórdicos con el independentismo kurdo del PKK y sus elementos armados en Siria, conversaciones que llevan incluso a poner encima de la mesa la condición de que Bruselas reanude las negociaciones con Turquía para su entrada en la Unión[224]. Finalmente, en abril de 2023 se confirma el ingreso de Finlandia en la organización y, en la cumbre aliada celebrada en Lituania en julio, Erdogan levanta el veto al ingreso de

[223] "La OTAN sigue siendo la piedra angular de la defensa colectiva de sus miembros en Europa. La cooperación UE-OTAN es un pilar indispensable para el desarrollo de la dimensión de seguridad y defensa de la UE. Las herramientas referidas al poder regulador y los instrumentos financieros de la Unión ayudan a sus 23 Estados Miembros integrados en la OTAN a alcanzar sus objetivos de capacidad" (traducción propia). IBIDEM, página 19.

[224] El presidente turco Tayyip Erdogan declaró en vísperas de la apertura de la cumbre: "Primero allanaremos el camino para la adhesión de Turquía a la Unión Europea, y después allanaremos el camino para Suecia". Puede consultarse la noticia en prensa. Disponible en: https://es.euronews.com/2023/07/10/erdogan-apoyara-el-ingreso-de-suecia-en-la-otan-si-la-ue-reanuda-negociaciones-con-turquia (20/09/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Suecia[225], no sin quedar en evidencia una vez más la cada vez mayor dificultad para alcanzar consensos y poner en marcha iniciativas conjuntas dentro de la OTAN.

Pero lejos de firmar una visión pesimista del estado de salud de la Alianza, consideramos que, a día de hoy, sigue siendo un caso de éxito basado en la capacidad de disuasión y defensa que ofrece en base a la adecuada combinación de la potencia nuclear, la fuerza convencional y el soporte táctico de los misiles, aunque padece de algunas dolencias que perjudican su naturaleza original, que ha perdurado todos estos años debido "en gran parte al hecho de que es la organización central de seguridad de unos países occidentales con valores y presupuestos filosóficos comunes" (HUNTINGTON, 1997, pág. 154).

Una vez efectuado el diagnóstico corresponde la propuesta de acciones que puedan facilitar a la OTAN la recuperación de esa visión de futuro que, desde los principios y valores compartidos por todos sus integrantes, representa la clave para la seguridad euroatlántica frente a las actuales amenazas y desafíos provenientes de todos los dominios operacionales -tierra, mar, aire, espacio y ciberespacio- que generan escenarios altamente demandantes de capacidades, competencias y recursos.

En este sentido, la primera consideración debe hacerse con respecto a la guerra de Ucrania a la que, entre todos, hay que darle una solución que permita recuperar la paz y la estabilidad cuanto antes en el territorio. En este punto, la coalición internacional que, liderada por la OTAN, ha mantenido a Ucrania con vida mediante la entrega de armas, el entrenamiento de sus fuerzas y la ayuda económica y logística, es probable que, llegado el momento, comience a favorecer un acuerdo negociado con Rusia porque un conflicto enquistado en Europa no lo quiere nadie, a pesar de las repetidas declaraciones de los principales líderes occidentales de apoyo *inquebrantable y continuo* a Ucrania[226]. La cohesión mostrada por EE.UU. y sus aliados europeos hasta la llegada a la Casa Blanca de Donald Trump, resulta esencial tanto para tratar de alcanzar la derrota militar de Rusia como, ante la perspectiva de las consecuencias derivadas para la estabilidad y seguridad de la región, la búsqueda de posibles soluciones negociadas que devuelvan la situación al *statu quo* inicial, aunque la península de Crimea se antoja como la gran línea roja del conflicto, por lo que cualquier intento de retornarla a Ucrania motivaría una escalada vertical inmediata del enfrentamiento. En cualquier caso, la coalición internacional no dispone de tantos recursos como para forzar un cambio de

[225] Finalmente, el Parlamento de Hungría ratifica el 26 de febrero de 2024 la entrada de Suecia como nuevo miembro de la OTAN, superándose de esta forma el último obstáculo para hacer efectiva la expansión de la Alianza a los dos países nórdicos, Finlandia –que ingresó en abril de 2023- y Suecia. Puede consultarse la relevancia de la noticia en la prensa internacional. Disponible en: https://www.nytimes.com/es/2024/02/27/espanol/suecia-otan-hungria.html https://elpais.com/internacional/2024-02-26/hungria-ratifica-la-adhesion-de-suecia-a-la-otan.html https://es.euronews.com/video/2024/02/26/el-parlamento-hungaro-ratifica-el-ingreso-de-suecia-en-la-otan (27/02/2024).

[226] El 10 de enero de 2023, la UE y la OTAN hacen una Declaración Conjunta en la que expresamente reiteran el "apoyo inquebrantable y continuo a la independencia, la soberanía y la integridad territorial de Ucrania dentro de sus fronteras reconocidas a escala internacional". Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/ (29/09/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

situación, a pesar del consenso mostrado en la reunión del G7 celebrada en Hiroshima en 2023[227], donde se corrobora la posición de China como competidor sistémico de Occidente del que no se espera un paso adelante para avalar unas hipotéticas negociaciones de paz, pese a que la capacidad de palanca que Pekín tiene con Moscú puede acabar siendo fundamental para alcanzar el acuerdo definitivo, lo que certificaría definitivamente la *desoccidentalización* del escenario mundial. En este contexto, los aliados europeos deben mostrarse como referentes para impulsar la salida al conflicto que, no olvidemos, se desarrolla en su ámbito geográfico de actuación. Sin embargo, el retorno a la presidencia de los EE.UU. de Donald Trump en enero de 2025 lejos de suponer un elemento de armonía dentro de la política de la Alianza, supone un cambio de paradigma en las alianzas internacionales previamente establecidas donde juegan un papel fundamental las ambiciones estadounidenses sobre el territorio de Groenlandia[228] o las denominadas *tierras raras* de Ucrania[229]. Prueba de ello ofrece su vicepresidente, J.D. Vance, en la Conferencia de Seguridad de Munich de febrero, planteando a posibilidad de buscar un acuerdo negociado para la guerra al margen de los europeos y presentando cono poco realista la pretensión de Ucrania de ingresar en la OTAN[230].

La segunda de las propuestas atañe a los nuevos escenarios de confrontación -ciberespacio y espacio ultraterrestre- donde la OTAN puede jugar una baza muy relevante como plataforma conjunta avanzada a través de la que articular el intercambio de lecciones aprendidas entre los aliados y, a mayores, de información con la que generar inteligencia que, posteriormente, pueda ser explotada para afrontar las amenazas comunes en base a la interoperabilidad de fuerzas y procedimientos estandarizados de sus unidades. Sin duda, a ello contribuye el avance substancial que supone el Concepto Estratégico de Madrid en cuanto a la equiparación de las operaciones hostiles contra los aliados en estos nuevos dominios ultraterrestre y ciberespacial, con respecto a los ataques armados en los entornos convencionales, y la

[227] La Cumbre del G7 de Hiroshima (Japón) se celebró del 19 al 21 de mayo de 2023, siendo la agresión de Rusia a Ucrania una de las cuestiones principales a tratar. Comunicado de prensa oficial disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/05/20/g7-hiroshima-leaders-communique/ (29/09/2023).

[228] Las pretensiones territoriales de EE.UU. sobre Groenlandia tienen amplio seguimiento en prensa internacional. Disponible en: https://www.bbc.com/mundo/articles/cqx8xgy2yryo https://elpais.com/internacional/2025-03-23/trump-desata-la-ira-de-groenlandia-al-enviar-una-delegacion-al-pais-encabezada-por-la-segunda-dama.html https://www.bbc.com/mundo/articles/c14jm544x87o (25/03/2025).

[229] La incorporación de las tierras raras ucranianas como parte de los factores determinantes de la negociación de la paz con Rusia, a través de la mediación de EE.UU., tiene amplio seguimiento en la prensa internacional. Disponible en: https://elpais.com/internacional/2025-02-12/trump-quiere-las-tierras-raras-de-ucrania-y-zelenski-esta-dipuesto-a-darselas.html https://es.euronews.com/my-europe/2025/02/28/esta-intentando-trump-dejar-fuera-a-la-ue-para-apoderarse-de-la-riqueza-mineral-de-ucrania https://www.youtube.com/watch?v=hW61fmf2FZM (25/03/2025).

[230] La Conferencia de Seguridad de Munich, celebrada del 14 al 16 de febrero de 2025, tiene amplio seguimiento en prensa. Disponible en: https://es.euronews.com/my-europe/2025/02/16/las-7-citas-que-debe-recordar-de-la-conferencia-de-seguridad-de-munich https://www.bbc.com/mundo/articles/cp8kg6r2wdjo https://legrandcontinent.eu/es/2025/02/14/cambio-de-regimen-el-discurso-completo-de-j-d-vance-en-munich/ (16/02/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

consecuente posibilidad de invocar el artículo 5 del Tratado del Atlántico Norte para la defensa común.

La tercera consideración supone afianzar el compromiso de los aliados para asumir la parte alícuota de inversión en defensa, dado que:

> "[…] existe una verdadera necesidad de invertir más para proteger a nuestras sociedades y es que el coste de la seguridad no es medible en cifras. Eso sí, habrá que garantizar que el incremento presupuestario se destina a adquirir las capacidades que son necesarias y que se estará dispuesto a utilizarlas cuando sea necesario (algo que no siempre ocurre). En definitiva, las tres Cs inglesas de *Cash, Capabilities, Commitments* (dinero, capacidades y compromiso) deben constituir un todo" (GÓMEZ CASTRO, 2017, pág. 13).

Para mantener su capacidad de disuasión y de defensa la OTAN necesita mantener operativos y actualizados una importante cantidad de recursos, así como la ventaja tecnológica de sus componentes, lo cual precisa el soporte del conocimiento y del desarrollo investigativo aplicado a la defensa, y esta es una forma de generar valor a futuro que puede liderar la OTAN, en línea con proyectos como la iniciativa DIANA[231] o su *Centro de Seguridad Cibernética*[232]. Ambas cuestiones requieren un esfuerzo de inversión de todos los socios con el que, verdaderamente, no siempre se ha cumplido. En este sentido, la invasión de Ucrania ha supuesto un eficaz revulsivo, principalmente para los socios europeos que, cada vez más, son conscientes de la necesidad de avanzar en su *autonomía estratégica* y, con ello, lanzar un mensaje a los EE.UU. de firmeza respecto a la idea de desligar la defensa aliada del compromiso económico que pueda adoptar Donald Trump a partir de enero de 2025.

La cuarta propuesta se refiere a la mejora de la citada capacidad de disuasión de la OTAN sobre la base no solo de sus fuerzas de defensa y de la inversión presupuestaria, sino de la cohesión euroatlántica, para lo cual será imprescindible responder con agilidad a cualquier señal de desacoplamiento entre las prioridades de los aliados. Fundamental para ello será dejar de crecer a expensas de rebajar los requisitos de acceso. La OTAN nunca ha sido una organización sustentada por la *cantidad de sus miembros*, sino por la *calidad de los valores y las capacidades militares* de aquellos, es decir, una organización política orientada a la defensa de sus socios. Por esta razón, la Alianza debe seguir manteniendo su carácter euroatlántico, vinculado a ese territorio y a ese contexto cultural e ideológico en el que nació, aunque en el actual marco geopolítico mundial,

[231] El Acelerador de Innovación de Defensa para el Atlántico Norte (DIANA) es la iniciativa de la OTAN presentada en la Cumbre de Bruselas de 2021, en el marco de la Agenda OTAN 2030, para potenciar el desarrollo económico, militar y tecnológico de los aliados frente a la competencia rusa y china, y que se fundamenta en la unión del esfuerzo en innovación entre el sector privado, del no gubernamental y del académico, y los especialistas en defensa públicos y privados, para aprovechar al máximo el potencial de las tecnologías de doble uso emergentes y disruptivas. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/bot__74.pdf (29/09/2023).

[232] El NATO´s Cyber Security Centre (Centro de Seguridad Cibernética de la OTAN) es el responsable de la prevención, detección y respuesta frente a los ataques a la infraestructura de red y sistemas críticos de la organización. Una de sus principales responsabilidades es la ciberseguridad de la NATO Communications and Information Agency – NCI Agency (Agencia de Información y Comunicaciones de la OTAN). Disponible en: https://www.ncia.nato.int/what-we-do/cyber-security.html (29/09/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

donde las crisis y los conflictos tienen consecuencias a nivel global, la defensa de los aliados precisa hoy día ampliar su ámbito de influencia a través de acuerdos cooperativos con socios de Europa del Este, de África, de América Central y del Sur, de Oriente Medio y Asia, entre otros, con el propósito de crear un elenco de *beneficios de seguridad mutuos* que se correspondan con los intereses estratégicos de la OTAN, *pero sin que esta red cooperativa pase a integrarse como países miembros de la Alianza*. En este mismo sentido, se debe mejorar la cooperación con foros internacionales, actores no estatales, organizaciones no gubernamentales y asociaciones regionales cuyos intereses puedan coincidir con los definidos por los aliados para preservar su seguridad.

Por último, muy en relación con la anterior, proponemos aprovechar la ocasión que brinda el Concepto Estratégico de Madrid para recuperar la capacidad de antaño de *anticiparse* a la situación geopolítica del presente y, mirando al medio y largo plazo, lograr que la OTAN genere valor para los aliados a través del impulso decidido de su *carácter político y el mecanismo consultivo*, consagrados en los artículos 2 y 4, respectivamente, del Tratado de Washington[233], para hacer de la organización "el principal foro de concertación euroatlántico" (COLOMINA, 2022, pág. 89) y buscar el consenso frente a estrategias expansionistas como las de China, nuevo competidor sistémico con especial querencia en las infraestructuras críticas[234] y en el desarrollo de tecnologías disruptivas y emergentes. Y todo ello pasa por disponer de una apropiada capacidad de reacción y toma de decisiones, de unas fuerzas adecuadamente disponibles, de la capacidad de despliegue donde sea necesario y, finalmente, de compartir una misma agenda aliada de intereses.

2.2.7. La aportación de la OTAN a la ciberseguridad en el siglo XXI

Una vez repasada la historia de la más famosa organización político militar intergubernamental consagrada a la defensa de sus miembros y pensando en identificar su principal aportación en el actual contexto internacional, caracterizado por los desafíos globales y las amenazas en el nuevo dominio del ciberespacio, tenemos que referirnos obligatoriamente a su enfoque de seguridad 360º que permite gestionar los tres planos de acción que la conforman:

1. El enfoque preventivo para la adaptación al permanente cambio de la amenaza, con el objetivo de poder afrontarla cualquiera que sea su naturaleza y gestionar la situación de crisis que conlleva.

[233] El artículo 2 del Tratado establece que "Las Partes contribuirán a un mejor desarrollo de las relaciones internacionales pacíficas y amistosas reforzando sus instituciones libres, asegurando una mejor comprensión de los principios en los que se basan estas instituciones y promoviendo las condiciones adecuadas que favorezcan la estabilidad y el bienestar. Tratarán de eliminar conflictos en sus políticas económicas internacionales y estimularán la colaboración económica entre varias o todas las Partes".
Por su parte, el artículo 4 señala que "Las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada".

[234] Un claro ejemplo de esta estrategia geopolítica es la Nueva Ruta de la Seda (*One Belt, One Road Initiative*), uno de los pilares de consolidación de China como superpotencia, mediante su conexión por tierra -ferrocarril- y por mar -puertos- con el objetivo de asegurar el acceso del país a los suministros de energía y materiales necesarios para impulsar su capacidad política y el crecimiento económico de su industria, facilitando la conexión con Europa, Asia, África y Rusia.

Ediciones Universidad de Salamanca | CC BY-NC-ND

2. La operativización de la disuasión como fase defensiva previa a la acción ofensiva colectiva, invocable a través de su artículo 5.
3. La gestión cooperativa de la seguridad de sus miembros para mantener activos el vínculo transatlántico y sus valores originarios: alineamiento con la Carta de las Naciones Unidas, salvaguarda de los principios de democracia, libertad y legalidad, y defensa de la paz y la estabilidad en la zona del Atlántico Norte

Este enfoque holístico de la seguridad implica necesariamente el compromiso con las operaciones en cualquier ámbito, destacando el ámbito de la ciberseguridad por sus implicaciones estratégicas, donde juega un papel protagónico la Agencia de Información y Comunicaciones de la OTAN (NCI Agency)[235] con funciones, entre otras, de coordinación de los Equipos Nacionales de Respuesta a Emergencias Informáticas (N-CERT), la dirección de la Asociación CIS3, responsable de garantizar la interoperabilidad de los sistemas aliados para operar de manera conjunta en misiones de la Alianza, y el mantenimiento del Centro de Servicios Móviles Integrado de la OTAN (NIMSC) de apoyo a las redes de comunicaciones seguras para las operaciones en cualquiera de los dominios físicos y el ciberespacio.

Pero la visión integral de la seguridad de los aliados también comporta una gestión activa de las capacidades operativas en el ciberespacio que se comienza a construir en el Concepto Estratégico de 2010, donde ya se identifica la gravedad de la ciberamenaza:

> "Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks"[236].

Desde entonces la Alianza ha sido muy consciente de la necesidad de proteger sus infraestructuras y de avanzar en la consecución de capacidades y competencias tecnológicas con las que operar en el ciberespacio para defenderse activamente y con tanta eficacia como en el resto de dominios físicos, estrategia respaldada por "el reconocimiento por parte de los aliados de que el Derecho Internacional era de aplicación en el ciberespacio" (FUENTE COBO, 2022, pág. 88). Fruto de este esfuerzo sostenido, actualmente la OTAN dispone de una visión integral de ciberdefensa articulada en torno a un eje principal, que es *la disuasión activa en todo el espectro de la amenaza, en cualquier ámbito o dominio, tanto en tiempo de paz como de conflicto, y a nivel político o militar*. Con ello la Alianza muestra su alerta ante la ciberamenaza

[235] Puede consultarse la página oficial de NCIA. Disponible en: https://www.ncia.nato.int/ (22/02/2024).

[236] "Los ciberataques son cada vez más frecuentes, organizados y costosos en cuanto a los daños causados a las administraciones gubernamentales, las empresas, las economías y potencialmente también a las redes de transporte y suministro y otras infraestructuras críticas; pueden alcanzar un umbral que amenace la prosperidad, la seguridad y la estabilidad nacional y Euroatlántica. Los militares y servicios de inteligencia extranjeros, la delincuencia organizada, los grupos terroristas y/o extremistas pueden ser la fuente de dichos ciberataques" (Traducción propia). Concepto Estratégico para la Defensa y la Seguridad de los Miembros de la OTAN. Lisboa 19-20 de noviembre de 2010. Consideración número 12. Página 11.

Ediciones Universidad de Salamanca | CC BY-NC-ND

pero, también, su firme determinación de considerar las estrategias híbridas como "un arma por derecho propio" (FUENTE COBO, 2022, pág. 89).

En esta idea, en mayo de 2008 se constituye el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) por iniciativa de Estonia, cuyo presidente define como "world-class think tank and training institution that is valued partner for NATO, Allies, and the international community"[237] (SCHMITT, 2017, p. XXIII), que actualmente cuenta con 28 países miembros -tanto aliados como socios ajenos- unidos por el objetivo de afrontar la ciberamenaza desde un enfoque interdisciplinar en el que tienen cabida la tecnología, la estrategia, las operaciones y el marco legal. Dos de sus más relevantes aportaciones son el conocido como *Manual de Tallinn* y el ejercicio de entrenamiento de ciberdefensa *Locked Shields*.

Respecto al *Manual de Tallinn sobre el Derecho Internacional aplicable a las ciberoperaciones* es la iniciativa de investigación[238] más emblemática del CCDCOE que, a través de 154 Reglas distribuidas en cuatro grandes apartados[239], aborda las cuestiones clave que definen las relaciones entre Estados en el ciberespacio desde la perspectiva del Derecho Internacional y en las que, entre otras, se afrontan temas como la soberanía, la jurisdicción, el uso de la fuerza o los derechos humanos en el nuevo dominio. Se trata de un texto *no vinculante* que atiende al principio del comportamiento responsable de los Estados como base para regular las ciberoperaciones y tratar de establecer un marco normativo acordado que evite la sustanciación del viejo brocardo latino *inter arma enim silent leges*[240].

Pero el CCDCOE redacta otro tipo de documentos como el titulado *Russia´s Strategy in Cyberspace*, desarrollado conjuntamente con el Centro de Excelencia de Comunicaciones Estratégicas de la OTAN (StratCom COE), en el que se analiza específicamente la permanente amenaza que suponen las operaciones ofensivas del Kremlin, donde la *confrontación informativa* frente a EE.UU. y Europa adquiere cada día más relevancia y en la que las ciberoperaciones son utilizadas junto con otros medios militares y no militares para alcanzar sus objetivos estratégicos[241].

En cuanto al *Locked Shields*, se trata de un ejercicio anual de ciberdefensa en formato *Blue Team vs. Red Team*, coordinado por el CCDCOE y orientado al entrenamiento de las capacidades de análisis y respuesta por parte de los equipos que representan a los países

[237] "Centro de estudios e institución de formación de ámbito mundial que es un socio valioso para la OTAN, los Aliados y la comunidad internacional" (Traducción propia).

[238] El equipo de trabajo encargado de la elaboración de dicho Manual estaba compuesto por un grupo de expertos internacionales bajo la dirección del profesor Michael N. Schmitt, con perfiles variados y complementarios: expertos legales, expertos técnicos y observadores sin derecho a voto. Además, otros como colaboradores, supervisores jurídicos y técnicos, e investigadores jurídicos.

[239] El Manual de Tallinn 2.0, edición de 2017, tiene 4 partes: 1. Derecho Internacional general y ciberespacio; 2. Regímenes especiales de Derecho Internacional y ciberespacio; 3. Paz y seguridad internacionales y actividades cibernéticas; 4. El derecho de los conflictos armados cibernéticos.

[240] "Las leyes guardan silencio entre las armas" (traducción propia).

[241] Russia´s Strategy in Cyberspace. NATO Strategic Communications Centre of Excellence & NATO Cooperative Cyber Defence Centre of Excellence. June 2021. Página 4. Disponible en: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf (05/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

participantes -*National Blue Teams*-, frente a un ciberincidente simulado en un escenario realista y con tecnologías aplicadas de vanguardia en el que el *Red Team* ataca a un sistema esencial o infraestructura crítica concreta, compitiendo por dar una respuesta adecuada, eficiente y en el menor tiempo posible en los diferentes planos que se ven afectados: el estratégico, el técnico, el legal y el mediático. El principal objetivo de este ejercicio es practicar y, al mismo tiempo, evaluar las capacidades de los equipos participantes para prevenir, detectar, evaluar y responder frente a ciberataques a gran escala. También sirve para formar a los decisores políticos, a los asesores jurídicos y a los responsables de comunicación en los aspectos estratégicos y técnicos de este tipo de incidentes. El equipo que representa a España[242] -*Spanish Blue Team*- está liderado por el Mando Conjunto del Ciberespacio (MCCE) y en él se integran expertos con diferentes perfiles de las diferentes instituciones con competencias en el ámbito de la ciberseguridad, tanto públicas como privadas[243], que de esta forma entrenan procedimientos de reacción y comparten experiencias y lecciones aprendidas.

Este modelo cooperativo e integral de seguridad que se construye sobre la organización de una alianza defensiva, la armonización de capacidades de sus miembros y la apertura del foco de atención hacia las zonas de influencia propias, determina un nueva manera de entender la seguridad en el orden internacional basado en el compromiso y la suma de fuerzas que, en pleno siglo XXI, sigue vigente y ha servido de guía a otra organización internacional de carácter supranacional, la Unión Europea, para dar forma a su proyecto de defensa común que establece incluso una cláusula de asistencia mutua similar a la noratlántica y que, siguiendo su patrón, combina las operaciones militares y las misiones civiles para favorecer la estabilidad y el mantenimiento de la paz mundial bajo el mandato de las NNUU y el auspicio del Derecho Internacional. Con sus aciertos y errores a lo largo de sus casi 75 años de existencia, la OTAN ha contribuido al equilibrio entre los rivales geopolíticos que pretenden la hegemonía en la esfera mundial y, a día de hoy, tras haber superado el cambio de modelo que trajo consigo el final de la Guerra Fría y el nacimiento de un nuevo entorno digital que ha abierto la puerta a riesgos y amenazas globales nunca antes conocidos, permanece vigente sin haber encontrado aún sustituto. No es poca cosa.

2.3. Conclusiones: la adaptación como parte del secreto para llegar a los 80 años de edad

A lo largo de la primera parte de este Capítulo 2 hemos señalado que una de las debilidades de las NNUU está en el alcance de los consensos requeridos para la toma de

[242] España es socio fundador del CCDCOE y forma parte de su Comité de Dirección, y lleva participando en el ejercicio Locked Shields desde 2010 con un equipo Blue Team compuesto por personal experto de las distintas áreas de especialidad como el aseguramiento de las infraestructuras, la defensa de sistemas y redes, el mantenimiento de servicios, la respuesta forense y la garantía de disponibilidad, confidencialidad e integridad de la información para el apoyo a la toma de decisiones.

[243] Entre otros participan expertos del Centro Criptológico Nacional, de la Fiscalía del Estado, del Departamento de Seguridad Nacional, de las Fuerzas y Cuerpos de Seguridad del Estado, del INCIBE, del mundo académico y del empresarial (Telefónica, INDRA, Iberdrola, entre otros). Puede consultarse la nota de prensa del Ministerio de Defensa sobre el ejercicio Locked Shields 2023. Disponible en: https://emad.defensa.gob.es/prensa/noticias/2023/04/Listado/230425-ni-mcce-locked-shield.html (01/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

decisiones y la consiguiente adopción de medidas que, de acuerdo al contexto geopolítico de cada momento, no siempre van a ir a favor de los intereses de todos los Estados miembros. Ello nos obliga a cuestionar la efectividad de su configuración gravemente afectada por la paralización que conlleva el anacrónico derecho al veto de sus miembros permanentes que, cada vez que lo emplean, centrados en la lucha por la hegemonía y la prevalencia de sus intereses, aprietan un poco más el nudo de la soga que condena a aquella a la muerte por asfixia, poniendo de manifiesto su incapacidad para alcanzar su principal objetivo: mantener la paz y la seguridad internacionales mediante la aplicación de medidas colectivas consensuadas por sus integrantes de acuerdo con los principios de la justicia y del Derecho Internacional.

Obligados por la realidad también debemos reconocer que la grieta que horada el principio de respeto a los derechos humanos es más profunda de lo que nos gustaría confesar, pero conflictos como los abiertos en el primer cuarto del siglo XXI, tanto en Europa como en Oriente Próximo, nos devuelven imágenes que la Carta de San Francisco quería, precisamente, evitar que volvieran a producirse.

Y tampoco es menos cierto que la posible actuación irresponsable de algunos de sus empleados, como la que ocupó la investigación dentro de la Agencia de Naciones Unidas para los Refugiados Palestinos (UNRWA) por su supuesta participación en los ataques de Hamás contra Israel del 7 de octubre de 2023[244], no vienen sino a socavar un poco más la credibilidad de la institución y a dañar otro de sus pilares fundacionales, como es la contribución a la solución de problemas internacionales de carácter humanitario y el impulso del respeto a los derechos humanos y las libertades fundamentales.

Sin embargo, esa misma realidad también nos brinda otra evidencia: la profunda repercusión de la perspectiva integral de la seguridad que desde 1994 comienza a construir NNUU sobre el concepto de la *seguridad humana*, íntimamente ligada a la *triple esfera de la libertad para vivir sin temor, sin miseria y con dignidad*. Esta visión supuso *de facto* la apertura a nuevas dimensiones nunca antes exploradas sobre la seguridad, hasta entonces principalmente focalizada en el Estado, así como la consideración de la gestión anticipativa como clave para prevenir la amenaza a las personas antes de que se llegue a producir el daño en cualquiera de esas tres esferas -paz, desarrollo o dignidad-.

[244] Dicha noticia tuvo amplio seguimiento en la prensa internacional y supuso que cerca de 20 Estados suspendiesen temporalmente sus aportaciones económicas a la UNRWA, entre ellos EE.UU., Canadá, UK, Francia, Alemania, Italia, Países Bajos, Austria, Finlandia, Rumanía, Estonia, Letonia, Lituania, Japón o Australia, entre otros. Finalmente, no se pudo llegar a demostrar tal participación en los atentados. Puede consultarse relevancia en prensa nacional e internacional. Disponible en: https://www.europapress.es/internacional/noticia-principales-responsables-onu-temen-efectos-catastroficos-suspension-ayuda-unrwa-20240131105430.html
https://www.elconfidencial.com/mundo/2024-01-29/guerra-israel-Hamás-gaza-directo-hoy_3819502/
https://www.france24.com/es/medio-oriente/20240126-unrwa-investiga-presunta-colaboraci%C3%B3n-de-su-personal-en-ataques-del-7-de-octubre-ee-uu-suspende-financiaci%C3%B3n
https://www.lavanguardia.com/internacional/20240126/9506787/onu-investiga-miembros-agencia-ayuda-palestina-implicados-presuntamente-ataque-Hamás-israel-7-octubre.html (02/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

A partir de entonces, y con hitos intermedios como la Resolución 66/290 aprobada por la Asamblea General en septiembre de 2012[245], *la seguridad humana se revela como clave transversal para la interpretación a escala global de las posibles respuestas centradas en las personas para los nuevos desafíos del siglo XXI*, que tiene su adaptación particular mediante los desarrollos nacionales que orienta la propia NNUU a través de su Manual de Seguridad Humana de 2016[246], donde se pone de manifiesto que *la seguridad humana tiene implicación nacional y no reemplaza a la seguridad estatal, sino que la complementa*, junto con el respeto a la integridad territorial y la no injerencia en cuestiones de jurisdicción interna de los Estados.

En consonancia con lo anterior y producto de la evolución del escenario mundial en el que aparecen nuevos actores que reclaman, en el marco de la seguridad multidimensional y multinivel, mayor papel para implicarse en la resolución de problemas vinculados con el desarrollo económico de las zonas más desprotegidas, el respeto de los derechos humanos, la defensa del medio ambiente y otras cuestiones de carácter global, NNUU presenta en 2015 la *Agenda 2030*[247] apostando por los ODS como factores de desarrollo que, junto con el respeto a los derechos humanos y el impulso de la paz, la comunidad internacional reconoce como pilares comunes de la pretendida nueva manera de entender la seguridad, integral y holística, que no puede perfeccionarse sino con la acción conjunta de todos esos actores y siempre desde el enfoque orientado a la persona como sujeto principal de la intervención, donde las *estructuras de gobierno dejan de ser el fin para convertirse en el medio* con el que conseguirlo.

Finalmente, como prueba de la adaptación a la transformación técnica y digital del nuevo siglo y la determinación por seguir cumpliendo su cometido en el nuevo dominio, debemos referirnos a la perspectiva de la *ciberseguridad aplicada a las Naciones Unidas* que, consciente del aumento sin precedentes de la ciberamenaza y del uso con fines delictivos de las TIC y las graves repercusiones que puede suponer, se postula como el marco de referencia e interlocución internacional. Para ello propone un modelo basado en el diálogo y la participación desde el que construir el consenso necesario entre todos los actores intervinientes -Estados, organizaciones intergubernamentales y regionales, sociedad civil, sector privado, academia, comunidad técnica-, con el objetivo de promover la paz, la seguridad, la cooperación y la confianza internacionales. La consecución de estos objetivos, que son intrínsecos a la esencia misma de la Organización, coadyuva a promover la seguridad internacional a través de, entre otras cuestiones, la *reducción de la brecha digital* que sigue siendo una prioridad urgente para

[245] Resolución aprobada por la Asamblea General el 10 de septiembre de 2012, A/RES/66/290, de 25 de octubre de 2012, sobre el Seguimiento del párrafo 143, relativo a la seguridad humana, del Documento Final de la Cumbre Mundial de 2005. Disponible en: https://www.un.org/humansecurity/wp-content/uploads/2022/06/N1147622.pdf (22/02/2024).

[246] Manual de Seguridad Humana. Un enfoque integrado para la consecución de los Objetivos de Desarrollo Sostenible y los ámbitos de acción prioritarios de la comunidad internacional y el sistema de las Naciones Unidas. Disponible en: https://www.un.org/humansecurity/wp-content/uploads/2023/02/HS-handbook-Spanish.pdf (22/02/2024).

[247] Resolución aprobada por la Asamblea General el 25 de septiembre de 2015, A/RES/70/01, de 21 de octubre de 2015, "Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible". Disponible en: https://unctad.org/system/files/official-document/ares70d1_es.pdf (22/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la comunidad internacional[248]. De esta forma, NNUU orienta su estrategia a un marco de protección que supera el propio de las TIC para atender a la gestión del riesgo institucional, la planificación de la continuidad de las actividades y la integridad y seguridad de toda su organización.

En cuanto a la que hoy por hoy es la alianza militar más exitosa de la historia, la OTAN, su naturaleza queda inicialmente resumida en la célebre frase de su primer secretario general, Lord Hastings Lionel Ismay, que comentaba que ésta se había creado *para mantener a los rusos fuera, a los americanos dentro y a los alemanes debajo*. Pero esto habría de cambiar por cuanto que ninguna organización o estructura internacional puede mantenerse ajena al permanentemente cambiante contexto en el que participa, so pena de ir quedando relegada hasta, definitivamente, acabar desapareciendo por su misma anacronía e ineficiencia. Es por ello que la Alianza Atlántica, empujada por el final de la Guerra Fría, se viera obligada a reinventarse dejando de focalizar su acción en la *defensa colectiva* frente a la extinta URSS para convertirse en una comunidad de *seguridad compartida* a través de la cual afrontar una nueva amenaza asimétrica y multidimensional, como la que evidenciaron los atentados terroristas del 11 de septiembre de 2001, que exige respuestas complejas donde, entre otras, la diplomacia y las estrategias híbridas juegan un papel prominente junto al clásico efecto disuasorio de la fuerza cinética.

Paradójicamente, la política expansiva de la Alianza de principios del siglo XXI para extender su cobertura de seguridad a todo el continente europeo, integrando bajo su escudo protector a gran parte de los antiguos componentes del Telón de Acero, será pieza clave en el resurgir de Rusia como principal amenaza al orden internacional, haciendo alarde de sus capacidades en el ciberespacio y en el desempeño de operaciones híbridas.

Es por ello que en la Cumbre de Madrid de 2022 se defina una nueva estrategia de disuasión y defensa de la OTAN basada en la *seguridad cooperativa* que, desde un enfoque 360º, pretende dotar a los aliados de la capacidad de respuesta ante cualquier amenaza *como quieran, cuando quieran y en el dominio que elijan*. Estos riesgos globales y multidimensionales se identifican, entre otras, con las políticas expansionistas de Rusia y China, el terrorismo internacional, el ciberespacio y el cambio climático.

Este ideario de alta capacitación operativa en cualquier dominio de enfrentamiento conlleva, *per se*, un compromiso con la estructura de gestión, de soporte técnico y de combate en el *ciberespacio, en el que la Alianza considera directamente aplicable el Derecho Internacional vigente* para la resolución de las controversias que las relaciones *inter pares* siempre generan. El esfuerzo realizado en este sentido se ampara con la consideración de la *amenaza híbrida como un arma más* en el elenco de las disponibles para respaldar su capacidad de disuasión y defensa.

Será por todo ello conveniente que la OTAN recuerde que su objetivo original y sus valores no han cambiado; lo que ha cambiado es el enfoque que debe dar a la defensa

[248] Recordemos que ello quedó ya reflejado en la Declaración del Milenio del año 2000, tal y como explicamos en el Capítulo primero, apartado 1.3.3.

Ediciones Universidad de Salamanca | CC BY-NC-ND

de los aliados de manera que consiga disuadir a los potenciales adversarios utilizando cualquiera de sus múltiples capacidades, en cualquier momento y en cualquier entorno. Todo lo que no sea esto será prolongar la deriva iniciada con el nuevo siglo. A ello puede ayudar el relevo de Jens Stoltenberg como Secretario General a partir del 1 de octubre de 2024 por Mark Rutte[249], ex primer ministro de Países Bajos, que a lo largo de su carrera política ha demostrado una gran capacidad de consenso. Dicha cualidad se antoja necesaria para poder liderar una Organización con 32 miembros que, por diversas razones, observan el desafío de la guerra de Ucrania a través de cristales diferentes, aunque Rutte haya comenzado su mandato con una línea de acción firme y continuista en cuanto a la necesidad de mantener el apoyo a Kiev, afirmando su derecho a defenderse incluso atacando objetivos legítimos en territorio ruso. Habrá que esperar a ver los efectos que sobre este planteamiento aliado tiene el regreso a la Casa Blanca del republicano Donald Trump y sus ambiciones territoriales sobre Groenlandia, o su propuesta de negociación con Rusia para alcanzar un acuerdo de paz en Ucrania al margen de la Unión Europea.

[249] Puede consultarse referencia en prensa nacional e internacional. Disponible en: https://es.euronews.com/my-europe/2024/06/26/ya-es-oficial-la-otan-tiene-un-nuevo-lider-mark-rutte-secretario-general
https://www.rtve.es/noticias/20240626/aliados-otan-eligen-primer-ministro-neerlandes-mark-rutte-como-nuevo-secretario-general/16162944.shtml (23/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 3. LA SEGURIDAD EUROPEA: REPLANTEAMIENTO DE LA ESTRATEGIA Y REAFIRMACIÓN DE VALORES EN EL CIBERESPACIO

Al igual que al presentar la OTAN debe comenzarse reconociéndole el mérito de ser la alianza militar más exitosa de la historia, cuando nos referimos a la Unión Europea (UE) es preciso destacar que, también, es única en su género.

Y esto es así por cuanto se trata de "la única organización internacional de carácter supranacional que funciona hasta la fecha, en la que sus Estados miembros han consentido en ceder parcelas de sus soberanías en distintos ámbitos" (ECHEVERRÍA JESÚS, 2019, pág. 245), como medio para alcanzar unos objetivos comunes[250] en permanente evolución -mejoras políticas y sociales, crecimiento económico, seguridad y defensa, influencia internacional-, a la vez que se comparten unos valores superiores[251], esenciales para comprenderla: la dignidad humana, la libertad, la democracia, la igualdad, el Estado de Derecho y el respeto a los derechos humanos, incluidos los derechos de las personas pertenecientes a las minorías.

La combinación de estos valores fundamentales y ambiciosos objetivos es lo que acarrea la necesidad de trascender el encaje de la UE como organización internacional, a pesar de serlo por su origen, y acuñar la nueva dimensión de la *supranacionalidad* que, como señala el profesor Díez-Picazo, lo es en un doble sentido, normativo y decisional:

> "La Unión Europea es supranacional en un doble sentido: en sentido normativo, porque muchas de sus normas vinculan directamente a las autoridades nacionales y a los particulares; y en un sentido decisional, porque la aprobación de dichas normas no está necesariamente sometida a la regla de la unanimidad –la tendencia ha venido siendo la de reducir progresivamente las materias en que se exige la decisión unánime- y porque en el procedimiento participan actores distintos de los representantes de los Gobiernos. El cuadro de las instituciones políticas de la Unión Europea, en efecto, no se reduce sólo al Consejo, sino que comprende también la Comisión y el Parlamento Europeo4. La supranacionalidad ha alcanzado tal grado de desarrollo que puede decirse, sin reservas, que la Unión Europea ejerce verdadero poder político" (DÍEZ-PICAZO, 2008, pág. 5).

No obstante, otra parte de la doctrina como la profesora Mangas Martín, no presumen ese carácter supranacional, *quasi* federal, argumentando que de ningún modo anima a

[250] El artículo 3 del Tratado de la Unión Europea estipula como objetivos genéricos, entre otros, la paz, sus valores y el bienestar de sus pueblos, la configuración de un espacio de libertad, seguridad y justicia, la libre circulación de sus ciudadanos y sus actividades económicas, la protección social, la no discriminación y la igualdad de género, así como la cohesión y solidaridad entre los Estados miembros.

[251] El artículo 2 del Tratado de la Unión Europea recoge estos valores comunes a sus Estados miembros: "La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Estos valores son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres".

Ediciones Universidad de Salamanca | CC BY-NC-ND

la Unión Europea el propósito de sustituir a los Estados soberanos, los cuales, de hecho, conforme al artículo 1 de su Tratado constitutivo[252], permanecen como tales independientes aunque vinculados por la cesión de competencias concretas y limitadas a la Unión. Como explica la profesora Mangas Martín:

> "La UE no es un Estado federal, aunque sólo sea por el hecho de que ni tan siquiera es un Estado. Es una organización internacional intergubernamental, ciertamente muy distinta a las Organizaciones clásicas; es una organización internacional original, única. La UE es un ente jurídico-internacional y político atípico; esta asociación de Estados soberanos no tiene en el horizonte sustituir a los Estados soberanos" (MANGAS MARTÍN & LIÑÁN NOGUERAS, 2016, pág. 63).

Nosotros, alineados con quienes ven en la UE un *mecanismo supranacional de integración*, creemos que la Unión trasciende la naturaleza jurídica y política de una organización internacional para convertirse, como defiende el profesor Coello de Portugal, en:

> "Un Estado en construcción en la antesala de su unificación política con la clara intención de convertirse en un Estado soberano, fruto de la acción concertada y racional de un poder constituyente supranacional progresivo y silente.
> Por todo ello, la Unión respondería a la naturaleza de un Estado en construcción al que preferentemente resultan aplicables las normas y principios propios del Derecho constitucional, antes que los principios propios del Derecho internacional público, salvo cuando la Unión Europea se relaciona con terceros en el marco de la sociedad internacional" (COELLO DE PORTUGAL, 2024, págs. 92-93)

Pero además de esta original naturaleza de la Unión, que ha comportado hasta el momento un caso de éxito global, es menester enfatizar el hecho de que comparte con las NNUU el honor de haber merecido el Premio Nobel de la Paz, porque "durante más de seis décadas, ha contribuido al avance de la paz y la reconciliación, la democracia y los derechos humanos en Europa"[253], lo cual habla de la identidad de los valores y principios que las inspiran y complementan. A ello coadyuva la diversidad geográfica, cultural, religiosa y política del Continente, esencia heterogénea e integradora que, al mismo tiempo, ha sustentado el "crecimiento económico y el progreso por primera vez en la historia de la humanidad" (MOLINAS & RAMÍREZ MAZARREDO, 2017).

Es decir, la integración de la UE continúa siendo un proyecto singular y abierto que, a día de hoy, aglutina a veintisiete países soberanos europeos convencidos de unos valores que gravitan sobre la dignidad humana, la libertad, la democracia, la igualdad, los derechos humanos y el Estado de Derecho, los cuales les llevan a comprometerse

[252] El artículo 1 del Tratado de la Unión Europea dispone que "Por el presente Tratado, las ALTAS PARTES CONTRATANTES constituyen entre sí una UNIÓN EUROPEA, en lo sucesivo denominada «Unión», a la que los Estados miembros atribuyen competencias para alcanzar sus objetivos comunes".

[253] En el año 2012 el Comité del Nobel subrayó la contribución de la UE a la transformación del continente europeo en un entorno pacífico, próspero y democrático. Puede consultarse en la página web del Premio Nobel y en la página web del Parlamento Europeo. Disponibles en: https://www.nobelprize.org/prizes/peace/2012/summary/ https://www.europarl.europa.eu/news/es/headlines/eu-affairs/20121012STO53551/la-union-europea-premio-nobel-de-la-paz-2012 (29/09/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

con unos mismos principios[254] que rigen su forma de proceder para la consecución de aquellos objetivos que justifican su existencia como "sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres"[255].

Esta es la auténtica clave sobre la que se sustenta la Unión en cuanto forma de organización política, consciente de su responsabilidad como punto de equilibrio en un complejo entorno multipolar, de competidores sistémicos ávidos de incrementar su poder, que mira al futuro desde una perspectiva global y colaborativa, fiel a sus valores y principios, como apuesta para continuar avanzando en su propia unidad y fortaleza.

Todo ello no significa que llegar hasta aquí haya sido *peccata minuta* ni, tampoco, que el día a día de la Unión para aglutinar voluntades sea cosa fácil, lo que demuestra que, casi ochenta años después de su fundación, sea acertada la reflexión del filósofo francés Bernard-Henri Lévy: "Europa no es un lugar, sino una idea".

3.1. El inopinado proceso constitutivo de la Unión Europea

Las enquistadas relaciones franco alemanas del siglo XIX estuvieron alimentadas por la permanente lucha de ambas potencias por sustentar una posición de prestigio y poder ante el resto de países vecinos, determinando las consecuencias de esta pugna, que tuvo su zenit en la Guerra Franco Prusiana de 1870[256], el belicoso destino de la Europa de la primera mitad del siglo XX, asolada por dos guerras mundiales[257] que devastan su

[254] El artículo 6 del Tratado de la Unión Europea determina que: "1) La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados. Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones.
2) La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados.
3) Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales".

[255] Artículo 2 Tratado de la Unión Europea.

[256] La Guerra franco prusiana de 1870-1871 supuso la ruina de Napoleón III y la llave para que Otto von Bismark abriera otra vez la ilusión con el nuevo Imperio Alemán –el conocido como II Reich- que amplió sus fronteras, potenció su industria, impulsó su economía y se fortaleció militarmente hasta su hundimiento por la derrota sufrida en la Primera Guerra Mundial frente a la Triple Entente conformada por Francia, Rusia y Reino Unido, que a su vez supuso el comienzo del hastío social del pueblo alemán que daría entrada al nacionalismo radical, caldo de cultivo del nazismo y preludio de la Segunda Gran Guerra.

[257] A modo de resumen, la I Guerra Mundial (1914-1918) supone el declive de las potencias europeas y la aparición de las dos nuevas referencias globales: EE.UU. y la URSS. Tras la guerra se crea la Sociedad de las Naciones con el Tratado de Versalles para, en teoría, fomentar la cooperación entras las naciones y garantizar la paz y la seguridad. Por su parte, la II Guerra Mundial (1939-1945) trae consigo el afán europeista que aúna la búsqueda de la paz y de una solución económica y defensiva, que impulsará la firma de grandes tratados para alcanzar dichos objetivos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

población, destruyen sus infraestructuras y ciudades, desmoronan el tejido industrial y finiquitan su potencia económica y comercial. Europa queda reducida a escombros y los europeos que sobreviven lo hacen como víctimas aterradas en una posguerra de miseria, hambre y destrucción como nunca antes se había visto.

La necesidad de encontrar la paz es la causa que impulsa, en el periodo comprendido entre 1945 y 1951, la firma concatenada de cuatro grandes acuerdos que marcan la historia de la Edad Contemporánea: la Carta de las Naciones Unidas en 1945, el Tratado de Bruselas origen de la Unión Europea Occidental (UEO) en 1948, el Tratado del Atlántico Norte en 1949, y el Tratado de París con el que se funda la Comunidad Europea del Carbón y del Acero (CECA)[258] en 1951, primera etapa del proceso de construcción de la UE que tiene su continuidad con la firma del Tratado de Roma en 1957, que instaura dos nuevas comunidades, la Comunidad Europea de la Energía Atómica (EURATOM), con el propósito de favorecer las condiciones para crear una industria y un mercado común nuclear en el territorio de sus miembros, y la Comunidad Económica Europea (CEE), con el esperanzado objetivo de converger en las políticas económicas de los Estados firmantes a través de la libre circulación de mercancías, servicios, personas y capitales.

Para que el ambicioso proyecto de paz y recuperación de Europa salga adelante es clave que Francia y Alemania superen su ancestral enfrentamiento y que se comprometan a hacer juntos el camino. De ahí la relevancia de que el Tratado de París sea firmado inicialmente por estos dos países junto con Italia, Bélgica, Países Bajos y Luxemburgo[259] "resueltos a sentar las bases de una unión cada vez más estrecha entre los pueblos europeos"[260] partiendo de la estrategia de favorecer la cooperación económica y la interdependencia comercial como paso previo para alcanzar, paulatinamente, mayores cotas de unidad política que evitasen a futuro una nueva confrontación militar. Desde el primer momento se confiere entidad jurídica al proyecto integrador europeo y se le dota de una serie de instituciones supranacionales[261] que obligan a los Estados miembros (EEMM) a pequeñas cesiones de competencias en materias concretas como, por ejemplo, la gestión de los aranceles aduaneros.

[258] El Tratado de París, constitutivo de la Comunidad Europea del Carbón y del Acero (CECA) fue firmado el 18 de abril de 1951 entre Francia, la República Federal de Alemania, Italia, Bélgica, Países Bajos y Luxemburgo, pretendía contribuir a la expansión económica, al empleo y a la mejora del nivel de vida en ese incipiente mercado común organizado en torno a la libertad de circulación del carbón y del acero y el libre acceso a las fuentes de producción, supervisado por una estructura institucional en cuyo vértice estaba la Alta Autoridad, encargada de velar por el respeto a las normas de competencia y la transparencia de precios. Junto a ella una Asamblea, un Consejo y un Tribunal de Justicia. Estas instituciones fueron las predecesoras de la Comisión Europea, el Parlamento Europeo, el Consejo de la UE y el Tribunal de Justicia de la UE, respectivamente. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:xy0022 (17/10/2023).

[259] De ellos, Francia, Bélgica, Países Bajos y Luxemburgo firman los cuatro grandes acuerdos referidos entre 1945 y 1951 como miembros fundadores.

[260] Célebre sentencia con la que inicia el Prólogo del Tratado de Roma, de 25 de marzo de 1957.

[261] Las principales instituciones creadas por el Tratado de Roma, de 26 de marzo de 1957, son el Consejo de Ministros -actual *Consejo de la UE*-, la Comisión, la Asamblea parlamentaria -actual *Parlamento Europeo*-, el Tribunal de Justicia y el Comité Económico y Social. Disponible en: https://www.europarl.europa.eu/about-parliament/es/in-the-past/the-parliament-and-the-treaties/treaty-of-rome (17/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por ello, con un evidente carácter utilitarista, los padres fundadores del proyecto unificador europeo -Robert Schumann[262], Jean Monnet, Alcide de Gaspieri, Konrad Adenauer y Paul-Henri Spaak– parten del convencimiento de que la integración únicamente puede afrontarse desde la perspectiva de una propuesta política de carácter inclusivo y abierta a todos los Estados democráticos del Viejo Continente, con dos líneas principales: centrarse en trabajar sobre la base de coaligar intereses económicos y comerciales, y rebajar el nivel de las cuestiones relativas a la defensa de sus miembros para no complicar el camino a transitar. Y este es el espíritu del Tratado de París de 1951, proyectado a su vez en el Tratado de Roma de 1957[263], que atesora toda la grandeza de estos estadistas quienes, sobre la base de una destrucción total y el rencor acumulado que ello conlleva, supieron tender la mano a Alemania para alzar el proyecto de "una unión cada vez más estrecha entre los pueblos europeos"[264].

El Tratado de Bruselas de 1965 marca el siguiente paso, constituyéndose las Comunidades Europeas a partir de la fusión de los órganos ejecutivos de la CECA, el EURATOM y la CEE, quedando a partir de entonces un Consejo y una Comisión únicos. A partir de entonces vamos a asistir a un proceso de integración -mediante los distintos Tratados de Adhesión- y de revisión de los tratados constitutivos de la Unión hasta llegar a los actuales -Tratado de la Unión Europea (TUA) y Tratado de Funcionamiento de la Unión Europea (TFUE)-.

En 1973 firman su adhesión Dinamarca, Irlanda y el Reino Unido[265], en 1981 lo hace Grecia, y en 1986 España[266] y Portugal. Es la Europa de los doce que, mediante las

[262] El Ministro francés de Asuntos Exteriores Robert Schuman pronunció el 9 de mayo de 1950 la célebre Declaración que lleva su nombre, en la que proponía la creación de una Comunidad Europea del Carbón y del Acero -CECA-, integrada inicialmente por Francia, Alemania Occidental, Italia, Países Bajos, Bélgica y Luxemburgo, origen del entramado institucional que, con el tiempo, llegaría a ser la Unión Europea. Disponible en: https://european-union.europa.eu/principles-countries-history/history-eu/1945-59/schuman-declaration-may-1950_es (17/10/2023).

[263] Después de los Tratados de Roma surgieron dos visiones sobre el proceso de integración europeo: de un lado, el intergubernamentalismo, que se enfoca en los acuerdos europeos como medio para que los Estados nación cooperen entre sí en aquellos asuntos de su interés sin que la soberanía nacional se vea socavada; y de otro, el supranacionalismo, que entiende que los Estados no retienen el control total de los desarrollos normativos europeos y sus consecuencias, es decir, pueden verse obligados a realizar actos en contra de su voluntad o sus preferencias, lo que implica una pérdida de soberanía nacional. En este sentido, el Tribunal de Justicia de la Comunidades Europeas (TJCE) se pronunció en el caso Van Gend en Loos (febrero de 1963) reconociendo la autonomía del ordenamiento jurídico de la Unión, consagrando el principio básico del *efecto directo del Derecho de la UE*, por cuanto genera obligaciones para los Estados miembros y, también, derechos para los particulares, por lo que estos pueden invocar directamente dichos derechos ante los Tribunales nacionales y europeos, independientemente de que los cuerpos normativos nacionales lo recojan. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/the-direct-effect-of-european-union-law.html (21/10/2023).

[264] Preámbulo del Tratado constitutivo de la Comunidad Económica Europea, firmado en Roma el 25 de marzo de 1957, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:11957E/TXT (21/10/2023).

[265] El 23 de junio de 2016 el Reino Unido celebró un referéndum sobre su pertenencia a la UE, donde un 52% votó a favor de abandonarla frente al 48% partidario de mantenerse en ella. El 30 de enero de 2020 se ratificó el Acuerdo de Retirada, conforme al artículo 50 del Tratado de la UE. Este proceso se conoce popularmente como *Brexit* (acrónimo de *Britain* -Gran Bretaña- y de *exit* -salida-).

[266] El camino para la integración de España en la UE comienza en febrero de 1962 con la carta de Fernando Castiella, Ministro de Asuntos Exteriores de España, a Maurice Couve de Murville, Presidente del Consejo

Ediciones Universidad de Salamanca | CC BY-NC-ND

reformas que comprende el Acta Única Europea[267], en vigor desde el 1 de julio de 1987, pone en marcha el mercado único interior, un espacio sin fronteras interiores y con libertad de circulación para personas, mercancías, servicios y capitales, elementos clave para dicha estrategia de cohesión económica y social. Asimismo, introduce el artículo 30 sobre la cooperación europea en materia de política exterior, sentando las bases para el desarrollo progresivo de una capacidad de acción conjunta con objetivos comunes, e institucionalizando las reuniones de los Ministros de Asuntos Exteriores en el marco de la Cooperación Política Europea. Esta representación formal de la de la coordinación de posiciones sobre los aspectos políticos y económicos de la seguridad europea no hace sino poner de relieve el convencimiento de los EEMM de que una cooperación más estrecha contribuirá al desarrollo de la identidad europea en materia de política exterior. Tres años después cae el muro de Berlín y se unifica Alemania tras más de 40 años dividida, adhiriéndose a las Comunidades Europeas la parte oriental en octubre de 1990.

En febrero de 1992 se firma en Maastricht el Tratado de la Unión Europea[268], piedra angular del proyecto unificador por cuanto supone un punto de inflexión en su evolución

---

de Ministros de la CEE, en la que solicita la apertura de negociaciones para examinar una posible vinculación de España con la CEE. Disponible en: https://www.cvce.eu/content/publication/2010/2/25/7e6802dc-c3e7-4715-9c68-b49224a171f7/publishable_es.pdf (22/10/2023).

En 1964, el Informe Birkelbach, documento de referencia en el marco de las deliberaciones del Consejo sobre la respuesta que se dará a la solicitud de asociación de España a la CEE, señala los aspectos políticos e institucionales de dicha asociación y posterior adhesión de España a la UE. Disponible en: https://www.cvce.eu/obj/informe_de_willi_birkelbach_sobre_los_aspectos_politicos_e_institucionales_de_la_adhesion_o_de_la_asociacion_a_la_comunidad_19_de_diciembre_de_1961-es-2d53201e-09db-43ee-9f80-552812d39c03.html (22/10/2023).

La primera fase del proceso es el Acuerdo Preferencial de octubre de 1970, por el que España se asocia con la CEE y se consiguen los tratos comerciales favorables. La segunda fase es la solicitud de adhesión el 28 de julio de 1977, seguida de las primeras elecciones en junio de 1977, el decidido apoyo del Parlamento y de la población, el dictamen favorable a la adhesión por parte de la Comisión de noviembre de 1978, y la apertura de negociaciones formales en 1979. Finalmente, la adhesión mediante la celebración del Consejo Europeo de Fontainebleau, celebrado en junio de 1984, donde Mitterrand anuncia el ingreso de España y Portugal en la CEE a partir del 1 de enero de 1986, y la firma del Tratado y Acta de Adhesión a la Comunidad el 12 de junio de 1985. Todo ello ratificado por la Ley Orgánica 10/1985, de autorización para la adhesión de España a las Comunidades Europeas.

A este respecto, cabe destacar la relevancia del artículo 93 CE que dispone que "mediante ley orgánica se podrá autorizar la celebración de tratados por los que se atribuya a una organización o institución internacional el ejercicio de competencias derivadas de la Constitución. Corresponde a las Cortes Generales o al Gobierno, según los casos, la garantía del cumplimiento de estos tratados y de las resoluciones emanadas de los organismos internacionales o supranacionales titulares de la cesión", el cual da carta de naturaleza a la celebración de tratados internacionales y a la incorporación al ordenamiento jurídico interno de las órdenes supraestatales.

[267] El Acta Única Europea fue firmada en Luxemburgo el 17/02/1986 y en La Haya el 28/02/1986, entrando en vigor el 1/07/1987. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:11986U/TXT (21/10/2023).

[268] El Tratado de Maastricht fue firmado en Maastricht el 7 de febrero de 1992 y entró en vigor el 1 de noviembre de 1993. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:11992M/TXT (21/10/2023).

El Tratado de Maastricht es de una gran importancia en el marco constitucional español por cuanto que, de las tres reformas que ha tenido nuestra Carta Magna, dos de ellas guardan relación con este Tratado. Así, en la Declaración 1/1992, de 1 de julio (BOE núm. 177, de 24 de julio de 1992), el Tribunal

Ediciones Universidad de Salamanca | CC BY-NC-ND

al trascender el inicial objetivo económico europeo y dotarle de una firme vocación política sentando las bases para la futura moneda única, instaurando la ciudadanía europea asociada a la libre circulación y residencia en el territorio de los EEMM y formalizando la estructura de funcionamiento de la UE sobre tres pilares. Esta distribución organizativa define un *Primer Pilar* de integración política y económica comunitaria, que recoge los Tratados como base de las competencias supranacionales transferidas por los Estados, y otros dos nuevos pilares que se sustentan en la cooperación intergubernamental, siendo el *Segundo Pilar* el relativo a la cooperación en Política Exterior y de Seguridad Común (PESC), y el *Tercer Pilar*, correspondiente a la cooperación en el ámbito de la Justicia y de los Asuntos de Interior (JAI). Esta estructura de los tres pilares se mantendrá hasta la entrada en vigor del Tratado de Lisboa en 2009, en el que por fin se define la *personalidad jurídica única* de la Unión.

En 1995, tras la adhesión de Austria, Finlandia y Suecia, entra en vigor el *acervo Schengen* que suprime las fronteras interiores entre sus siete países firmantes con el propósito de fomentar la libre circulación de personas, mercancías, servicios y capitales[269], a cuyo logro viene a contribuir la introducción de la moneda común para los doce países que inicialmente se incorporan a la zona euro.

Constitucional concluye la necesidad de reformar la CE, concretamente el artículo 13.2, introduciendo el término "y pasivo" en cuanto al derecho de sufragio en las elecciones municipales españolas, para ajustarlo al art. 8 B, apartado 1 del Tratado de la CEE, en la redacción dada por el art. G B, apartado 10 del TUE., cuyo texto indica que "Todo ciudadano de la Unión que resida en un Estado miembro del que no sea nacional tendrá derecho a ser elector y elegible en las elecciones municipales del Estado miembro en el que resida, en las mismas condiciones que los nacionales de dicho Estado. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/6944#:~:text=%221.,los%20nacionales%20de%20dicho%20Estado.
https://www.boe.es/buscar/doc.php?id=BOE-A-1992-20403
https://app.congreso.es/consti/constitucion/reforma/primera_reforma.htm (21/10/2023).
La segunda reforma, de 27 de septiembre de 2011, afecta al art. 135 CE con el objetivo de posibilitar el cumplimiento de los compromisos asumidos por España al integrarse en la CEE, marco en el cual la estabilidad presupuestaria adquiere un valor estructural y condicionante de la capacidad de actuación financiera y presupuestaria de las Administraciones Públicas. Se concibe así la estabilidad presupuestaria como esencial para el mantenimiento y desarrollo del Estado Social que se proclama en el artículo 1.1 CE, por lo que se opta por incluirlo en la Carta Magna y darle a la referida estabilidad presupuestaria el máximo nivel normativo posible dentro de nuestro ordenamiento jurídico. Disponible en: https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=135&tipo=2
https://www.congreso.es/docu/constituciones/1978/art135_1978.pdf (21/10/2023).

[269] El Acuerdo de Schengen se firmó el 14 de junio de 1985 por Bélgica, Países Bajos, Luxemburgo, Francia y Alemania para reforzar la solidaridad entre sus pueblos eliminando los obstáculos para la libre circulación en las fronteras comunes de sus nacionales, mercancías y servicios. Cinco años más tarde, el 14 de junio de 1990, los mismos Estados firman el Convenio de Aplicación del Acuerdo de Schengen para la supresión gradual de los controles en las fronteras interiores, concretando definiciones, procedimientos y condiciones de circulación de los extranjeros, entre otros. El 25 de junio de 1991 lo ratifican España y Portugal. Su aplicación efectiva comenzó en marzo de 1995 cuando los siete países rescindieron los controles en sus fronteras comunes. Actualmente forman parte del Espacio Schengen los 27 países de que conforman la UE, con la particularidad de Rumanía y Bulgaria en cuanto al cruce de fronteras por tierra, y otros 4 que no pertenecen a ella: Noruega, Islandia, Suiza y Liechtenstein.
Puede consultarse el Acervo de Schengen en el Diario Oficial de las Comunidades Europeas DO núm. L239, de 22 de septiembre de 2000. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:2000:239:TOC (21/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Hitos de la UE 1948-2022

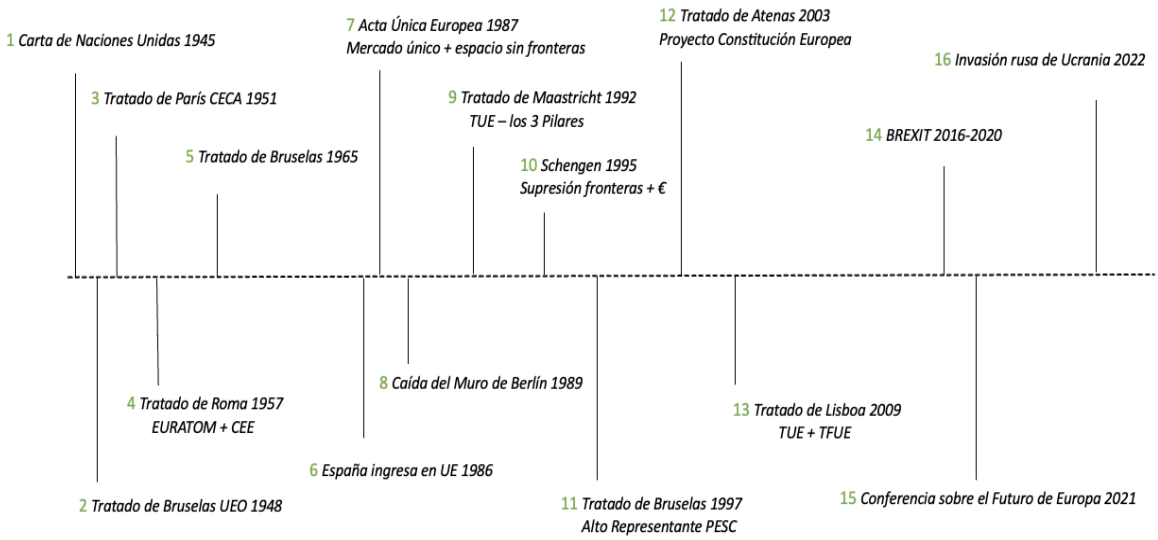


Gráfico 3.1.
Fuente: propia

El Tratado de Ámsterdam[270] de 1997 da entrada a una de las señas de identidad de la Unión, creando la posibilidad de la *cooperación reforzada* entre aquellos Estados miembros que cumplan una serie de requisitos, a través de las instituciones y de los procedimientos de la UE y siempre que el Consejo considere que los objetivos de éstas no pueden alcanzarse, en un plazo razonable, mediante la aplicación de las disposiciones pertinentes de los Tratados. Asimismo, en Ámsterdam se instaura el cargo de *Alto Representante de la Política Exterior y de Seguridad Común*[271] y unos meses después, en el Consejo Europeo de Helsinki, al tiempo que se prepara el proceso de ampliación necesaria "para la estabilidad y prosperidad del continente europeo"[272], se le empieza a dar forma a dicha Política reconociendo que el Consejo de Seguridad de las NNUU "es el primer responsable del mantenimiento de la paz y seguridad internacionales"[273] para, seguidamente, mostrar la determinación de crear una capacidad de decisión autónoma y de asumir operaciones militares propias en respuesta a crisis internacionales,

[270] El Tratado de Ámsterdam por el que se modifican el Tratado de la Unión Europea, los Tratados constitutivos de las Comunidades Europeas y determinados actos conexos, fue firmado en Ámsterdam el 2 de octubre de 1997 y entró en vigor el 1 de mayo de 1999. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:1997:340:FULL (21/10/2023).

[271] El artículo J.8.3 del Tratado de Ámsterdam señala que "La Presidencia contará con la asistencia del Secretario General del Consejo, que ejercerá las funciones de Alto Representante de la política exterior y de seguridad común".

[272] El punto 3 de las Conclusiones de la Presidencia del Consejo Europeo de Helsinki, celebrado el 10 y 11 de diciembre de 1999, señala que "El Consejo Europeo ha corroborado la importancia del proceso de ampliación que se inició en Luxemburgo en diciembre de 1997 para la estabilidad y prosperidad de todo el continente europeo. Un proceso de ampliación eficaz y digno de crédito ha de tener continuidad".

[273] El punto 26 establece que "La Unión contribuirá a la paz y seguridad internacionales de conformidad con los principios de la Carta de las Naciones Unidas. La Unión reconoce que el Consejo de Seguridad de las Naciones Unidas es el primer responsable del mantenimiento de la paz y seguridad internacionales".

Ediciones Universidad de Salamanca | CC BY-NC-ND

respetando el vínculo transatlántico con la OTAN y sin que estas capacidades conlleven la creación de un ejército europeo[274]. Al mismo tiempo, en el ámbito del Tercer Pilar, por un lado se acuerda como objetivo de la Unión "ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia elaborando una acción en común entre los Estados miembros en los ámbitos de la cooperación policial y judicial"[275], dando mayor profundidad y sustituyendo la referencia que Maastricht hace a Justicia y Asuntos de Interior, y por otro, se integra el acervo de Schengen en el marco de la UE[276].

En 2003 se firma el Tratado de Atenas[277] consolidándose la mayor ampliación de la UE hasta la fecha con la adhesión de República Checa, Hungría, Polonia, Eslovaquia, Eslovenia, Lituania, Letonia, Estonia, Chipre y Malta. Son tiempos de expansión que se tratan de aprovechar para lanzar la idea de acordar un *texto constitucional* que sustituya a los tratados fundacionales de la Unión. Pero la inercia que parecía haberse conseguido se detiene de golpe. Tras el rechazo al proyecto de Constitución para Europa por parte de dos de los países fundadores, Francia y Países Bajos, en sus respectivos referéndums de ratificación en 2005[278], la UE sufre una de sus mayores crisis de identidad, quedando

[274] El punto 27 indica que "El Consejo Europeo ha destacado su determinación de crear una capacidad de decisión autónoma y, en aquellas operaciones militares en las que no participe la OTAN en su conjunto, la capacidad de iniciar y llevar a cabo operaciones militares dirigidas por la UE en respuesta a crisis internacionales. Este procedimiento, que evitará duplicaciones innecesarias, no implica la creación de un ejército europeo".

[275] El Tratado de Ámsterdam por el que se modifica el Tratado de la Unión Europea, los Tratados constitutivos de las Comunidades Europeas y determinados actos conexos, firmado en Ámsterdam el 2 de octubre de 1997, en el marco de las Disposiciones relativas a la cooperación policial y judicial en materia penal, en el artículo K.1 determina que: "Sin perjuicio de las competencias de la Comunidad Europea, el objetivo de la Unión será ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia elaborando una acción en común entre los Estados miembros en los ámbitos de la cooperación policial y judicial en materia penal y mediante la prevención y la lucha contra el racismo y la xenofobia. Este objetivo habrá de lograrse mediante la prevención y la lucha contra la delincuencia, organizada o no, en particular el terrorismo, la trata de seres humanos y los delitos contra los niños, el tráfico ilícito de drogas y de armas, la corrupción y el fraude, a través de:

- — una mayor cooperación entre las fuerzas policiales, las autoridades aduaneras y otras autoridades competentes de los Estados miembros, ya sea directamente o a través de la Oficina Europea de Policía (Europol), de conformidad con lo dispuesto en los artículos K.2 y K.4 ;
- — una mayor cooperación entre las autoridades judiciales y otras autoridades competentes de los Estados miembros, de conformidad con lo dispuesto en las letras a) a d) del artículo K.3 y en el artículo K.4;
- — la aproximación, cuando proceda, de las normas de los Estados miembros en materia penal, de conformidad con lo dispuesto en la letra e) del artículo K.3".

Puede consultarse en el Diario Oficial de las Comunidades Europeas DO núm. C340, de 10 de noviembre de 1997. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:1997:340:TOC (21/10/2023).

[276] Protocolos anejos al Tratado de la Unión Europea y al Tratado Constitutivo de la Comunidad Europea. Puede consultarse en el Diario Oficial de las Comunidades Europeas DO núm. C340, de 10 de noviembre de 1997. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:1997:340:TOC (21/10/2023).

[277] El Tratado de Atenas fue firmado el 16 de abril de 2003 en Atenas y entró en vigor el 1 de mayo de 2004. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=OJ%3AL%3A2003%3A236%3ATOC (22/10/2023).

[278] El proyecto de elaboración de una constitución para los ciudadanos europeos comenzó a elaborarse a partir de la decisión del Consejo Europeo de Laeken en diciembre de 2001 de organizar una Convención

Ediciones Universidad de Salamanca | CC BY-NC-ND

desorientada por el mensaje recibido de estos resultados y las posturas contrarias de otros Estados miembros que ponen en entredicho el futuro del proyecto integrador, ante la evidencia de que "el número de los escépticos se ha incrementado notablemente, pero lo más trascendente quizá sea que resulta difícil establecer la posición en la que se encuentran los que supuestamente no lo son" (GARCÍA VALDECASAS, 2005), lo cual viene a ratificar la idea de que el nivel de madurez real de la Unión en ese momento demanda una estrategia de consolidación, de afirmación de ideas y valores conjuntos, todo lo contrario a la recién consumada ampliación que, como es el caso, no siempre funciona como herramienta de política exterior.

Aun así, dos años después parte de los elementos más importantes del fallido proyecto constitucional se integran en la relevante modificación de base que se acuerda en Lisboa en diciembre de 2007. El Tratado de Lisboa[279] entra en vigor el 1 de diciembre de 2009 y supone un punto de inflexión por cuanto que, por primera vez, se distinguen *tres tipos de competencias de la Unión* -las exclusivas, las compartidas y las de apoyo[280]- y se le otorga *personalidad jurídica propia*[281], lo que le permite firmar acuerdos internacionales en los ámbitos de competencia que tiene atribuidos y, al tiempo, asumir la responsabilidad del avance del proceso integrador. Asimismo, suprime la estructura competencial de los tres pilares y configura un *nuevo marco institucional*[282] buscando la mejora de la eficacia y transparencia que permitan alcanzar sus objetivos y defender sus intereses a través de un nuevo sistema de adopción de decisiones por mayorías y

que reflexionase con todas las partes interesadas sobre el futuro de la UE. Las cuatro cuestiones más importantes en este sentido se concretaron en estudiar un mejor reparto de competencias de las instituciones de la Unión, la simplificación de sus instrumentos de actuación, la consecución de un mayor grado de democracia, transparencia y eficacia y, finalmente, la redacción de una Constitución para Europa, con la que se pretendía reemplazar los tratados existentes hasta el momento. El proyecto de Tratado Constitucional se firmó en Roma en octubre de 2004 y, en enero de 2005, el Parlamento Europeo aprobó una resolución en la que recomendaba a los Estados miembros que sus ciudadanos lo ratificaran en plebiscito. En España se celebró el referéndum consultivo el 20 de febrero de 2005, obteniendo el sí, cosa que no ocurrió el 29 de mayo y el 1 de junio en dos de los países fundadores, Francia y Países Bajos respectivamente, donde se rechazó.

[279] Su denominación es Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, por cuanto da lugar a los dos Tratados actuales, el Tratado de la Unión Europea (TUE), y el de Funcionamiento de la Unión Europea (TFUE), desapareciendo el término *Comunidad* que es sustituido por el de *Unión*, tal y como se recoge en el artículo 1 del TUE al referirse a que "la Unión sustituirá y sucederá a la Comunidad Europea". Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12007L/TXT (22/10/2023).

[280] Es esta cuestión relevante para entender el principio de que la UE no tiene soberanía y que sus competencias son las atribuidas específicamente por los Estados miembros, que continúan siendo sus titulares como auténticos representantes de los diferentes pueblos soberanos que les respaldan. Es este el denominado principio de atribución de competencias que recoge el TUE. Conforme a ello, las competencias exclusivas de la Unión quedan definidas en el artículo 3 TFUE, las compartidas en el artículo 4 TFUE y las de apoyo en el artículo 6 TFUE, y este es el marco de actuación en el que la Unión puede actuar.

[281] El artículo 47 TUE estipula que "La Unión tiene personalidad jurídica".

[282] El artículo 13 del TUE indica que las instituciones de la Unión son el Parlamento Europeo, el Consejo Europeo, el Consejo, la Comisión Europea, el Tribunal de Justicia de la Unión Europea, el Banco Central Europeo y el Tribunal de Cuentas.

Ediciones Universidad de Salamanca | CC BY-NC-ND

articulando herramientas como la *Cooperación Estructurada Permanente* (PESCO)[283] y la figura del *Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad*[284], responsable de elaborar la *Política Exterior y de Seguridad Común de la Unión* (PESC) y la *Política Común de Seguridad y Defensa* (PCSD). En cuanto al espacio de libertad, seguridad y justicia trasciende su anterior naturaleza intergubernamental para integrarse en el marco comunitario como competencia compartida[285], siendo desarrollado en el ahora denominado *Tratado de Funcionamiento de la Unión Europea* (TFUE)[286].

Desde la entrada en vigor del Tratado de Lisboa en 2009 hasta la actualidad la Unión ha tenido que afrontar varios retos sin precedentes como dos crisis económicas a nivel global, la salida del Reino Unido con el *Brexit*[287], la pandemia del COVID-19, la adhesión de la península de Crimea a la Federación de Rusia y su posterior invasión de Ucrania, entre otros dramas humanitarios[288] y conflictos en el límite de sus fronteras. La gestión de estas amenazas pone nuevamente de relieve carencias en el modelo de toma de decisiones y de eficiencia del sistema de gobernanza vigente, que lleva a la Unión a poner en marcha en marzo de 2021 la Conferencia sobre el Futuro de Europa[289], la cual concluye con la presentación de cuarenta y nueve propuestas que implican modificaciones de los Tratados. A partir de estas iniciativas planteadas, el 9 de junio de 2022 el Parlamento Europeo aprueba la Resolución sobre la convocatoria de una

[283] La Cooperación Estructurada Permanente se recoge en los artículos 42.6 y 46 TUE y permite a los Estados miembros que lo deseen y dispongan de unas determinadas capacidades militares, desarrollar misiones suministrando unidades de combate que operen conjuntamente.

[284] De acuerdo al artículo 18 TUE, el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad preside el Consejo de Asuntos Exteriores y es Vicepresidente de la Comisión, contando para el desempeño de sus funciones con el apoyo del Servicio Europeo de Acción Exterior (SEAE) y de la Agencia Europea de Defensa (EDA).

[285] El artículo 4.2.j del TUE recoge que "Las competencias compartidas entre la Unión y los Estados miembros se aplicarán a los siguientes ámbitos principales: j) el espacio de libertad, seguridad y justicia".

[286] Se desarrolla en el Título V Espacio de Libertad, Seguridad y Justicia, entre los artículos 67 a 89 del TFUE.

[287] El 23 de junio de 2016 el Reino Unido celebró un referéndum sobre su pertenencia a la UE, donde un 52% votó a favor de abandonarla frente al 48% partidario de mantenerse en ella. El 30 de enero de 2020 se ratificó el Acuerdo de Retirada, conforme al artículo 50 del Tratado de la UE. Este proceso se conoce popularmente como *Brexit* (acrónimo de *Britain* -Gran Bretaña- y de *exit* -salida-).

[288] El 3 de octubre de 2013 murieron más de 300 migrantes tras el naufragio de una embarcación con alrededor de 500 personas en las costas de la isla italiana de Lampedusa, desgraciado suceso que supuso una poderosa llamada de atención sobre la inalterable situación de pobreza en África y el consecuente intento de sus ciudadanos de intentar mejorar sus vidas migrando a Europa, mayormente cayendo en manos de las redes de crimen organizado que manejan las redes de trata de seres humanos.
Puede verse la repercusión en prensa. Disponible en: https://www.bbc.com/mundo/noticias/2013/10/131003_lampedusa_migrantes_cuerno_africa_cch.amp (21/10/2023).

[289] La Conferencia sobre el Futuro de Europa es una iniciativa conjunta de la Comisión, el Parlamento y el Consejo para, a través de diálogos y deliberaciones con ciudadanas y ciudadanos de toda Europa organizados por temas, escuchar las opiniones sobre lo que debe ser el futuro de la Unión. Este proceso consultivo y de intercambio de ideas finaliza el 9 de mayo de 2022, con la presentación de un informe final con 49 propuestas y 326 medidas para articularlas. Disponible en: https://www.consilium.europa.eu/es/policies/conference-on-the-future-of-europe/ (22/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

convención para la revisión de los Tratados[290] al objeto de garantizar mayor eficacia frente a las crisis en la que se acuerda, entre otras cuestiones, reforzar la capacidad de actuación de la Unión mediante la reforma de sus procedimientos de votación prescindiendo de la unanimidad en la PESC, la adaptación de las competencias atribuidas a la Unión, la incorporación a sus políticas de parámetros ecológicos y de transición digital, y el reforzamiento de la protección de sus valores fundamentales para responder a las necesidades planteadas por los Estados miembros y sus ciudadanos.

A renglón seguido, y en el marco geoestratégico derivado de la guerra de Rusia contra Ucrania, el Consejo Europeo comienza a plantearse el desafío de su potencial expansión hacia el Este[291] recurriendo otra vez a la ampliación como "uno de los instrumentos de política exterior de la UE más acertados", por cuanto "cada nueva tanda de adhesiones ha venido acompañada de reformas institucionales y nuevos ámbitos de integración que han permitido a la Unión ganar en eficacia y en estabilidad y defender sus intereses estratégicos" (BORRELL FONTELLES, 2022).

Pero esta expansión europeista hacia el Este no parece que vaya a ser un viaje cómodo por dos razones. La primera de ella, sin duda, la resistencia rusa a perder capacidad de influencia en territorios que, no hace tanto, fueron de su entorno próximo. Un ejemplo de ello se vislumbra tras las masivas protestas y disturbios acaecidos en noviembre y diciembre de 2024 en Georgia por la decisión del partido populista y prorruso *Sueño Georgiano*, recién ganadas las elecciones en medio de denuncias de fraude, de suspender hasta 2028 el proceso de adhesión a la Unión Europea[292]. Esta situación

[290] Resolución del Parlamento Europeo, de 9 de junio de 2022, sobre la convocatoria de una convención para la revisión de los Tratados (2022/2705(RSP)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0244_ES.html (22/10/2023).

[291] Esta hipotética ampliación de la UE tendría como objetivo la adhesión de países como Turquía, Montenegro, Serbia, Macedonia del Norte, Albania, Bosnia y Herzegovina, Ucrania, Moldavia, Georgia y Kosovo. En este marco, el 2 de octubre de 2023 el AR/VP Josep Borrell convoca a los Ministros de Exteriores de la Unión Europea en Kiev "a la primera reunión de los 27 Estados miembros celebrada nunca fuera de la UE", cuestión recogida ampliamente por la prensa mundial. Disponible en: https://www.eeas.europa.eu/delegations/ukraine/ukraine-press-remarks-high-representative-josep-borrell-ahead-eu-foreign-ministers-meeting-kyiv_en?s=232 (29/10/2023).
Posteriormente, el 8 de noviembre de 2023, avanzando en esta filosofía que entiende la ampliación como política vital para la UE, la Comisión adopta el paquete para 2023, con una evaluación de la situación y progresos realizados por estos países y, por primera vez, también Ucrania, a la que se le concede el estatuto de candidato. Disponible en: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/COM_2023_690%20Communication%20on%20EU%20Enlargement%20Policy_and_Annex.pdf (09/11/2023).
El 14 de diciembre de 2023 la UE da un paso más con su aprobación a abrir las negociaciones de adhesión de Ucrania y Moldavia, y otorgando el estatus de candidato a Georgia. Disponible en: https://es.euronews.com/my-europe/2023/12/14/la-ue-acuerda-abrir-las-negociaciones-de-adhesion-con-ucrania-y-moldavia (19/12/2023).

[292] Puede verse el tratamiento en prensa de estas protestas. Disponible en:
https://elpais.com/internacional/2024-11-29/el-gobierno-de-georgia-frena-la-adhesion-a-la-ue-y-la-oposicion-se-echa-a-la-calle-para-protestar.html
https://elpais.com/internacional/2024-12-02/cientos-de-detenidos-en-georgia-tras-cuatro-noches-de-protestas-multitudinarias-contra-el-gobierno-prorruso.html
https://www.europapress.es/internacional/noticia-cinco-detenidos-veintena-agentes-heridos-ultima-noche-protestas-georgia-20241202080010.html

Ediciones Universidad de Salamanca | CC BY-NC-ND

atestigua la profunda división interna entre un amplio porcentaje de la sociedad georgiana proeuropea y el ejecutivo de Irakli Kobakhidze, alineado con las políticas del Kremlin. Las imágenes de las manifestaciones en la capital, Tiflis, rememoran los hechos acaecidos en 2013 en la Plaza de la Independencia de Kiev, con el estallido del Euromaidán, que precipitaron la huida del presidente ucraniano, Viktor Yanukóvich, y fueron la semilla temprana de la guerra ruso ucraniana que, desde febrero de 2022, inquieta a Europa.

En segundo lugar, para afrontar esta expansión estratégica de la UE hacia el Este, deben abordarse reformas de profundo calado como la del proceso de adopción de decisiones en el Consejo por *mayorías cualificadas*, en vez de por unanimidad, en busca de la agilidad en la toma de posición común, la reforma en el reparto de escaños en el Parlamento Europeo, la supresión de los vetos interesados y la capacidad de respuesta en tiempo real. Este proceso va a significar, como suele ser habitual en la lenta metamorfosis evolutiva de la Unión, el surgimiento de fricciones entre las posturas defendidas por aquellos EEMM que, como Polonia y Hungría, tienen una *visión utilitarista* de su condición europea, y aquellos otros partidarios de un continuo movimiento hacia delante que suponga avances en el compromiso fundacional de la UE, como los del arco mediterráneo.

En este debate interno, a nuestro modo de ver, habrán de pesar las lecciones aprendidas en cuanto a la aceptación e inmediata puesta en marcha por los recién llegados de las condiciones exigidas por la Unión, puesto que bajar la *nota de acceso* para dar cabida a nuevos socios tendría un coste en valores democráticos y principios fundamentales difícil de aceptar en un momento en que "Europa se enfrenta a opciones trágicas; la seguridad y la prosperidad ya no pueden darse por sentadas" (VAN MIDDELAAR, 2021).

3.2. La Política Exterior y de Seguridad Común: el camino hacia la deseada autonomía estratégica de la Unión

Conviene comenzar señalando varias cuestiones que derivan de la extraordinaria yuxtaposición de grandes acuerdos consecutivos entre 1945 y 1951, que contribuyen a formar el líquido amniótico en el que se gesta la postura europea que acabará condicionando, hasta el momento presente, su política exterior, de seguridad y de defensa. La primera de ellas, la íntima conexión con los valores y principios que refleja la Carta de las Naciones Unidas[293], que marca la estrecha colaboración entre ambas

https://www.elmundo.es/internacional/2024/12/02/674d747be4d4d890628b4787.html (14/12/2024).

[293] En este sentido, el artículo 21.1 TUE indica que "La acción de la Unión en la escena internacional se basará en los principios que han inspirado su creación, desarrollo y ampliación y que pretende fomentar en el resto del mundo: la democracia, el Estado de Derecho, la universalidad e indivisibilidad de los derechos humanos y de las libertades fundamentales, el respeto de la dignidad humana, los principios de igualdad y solidaridad y el respeto de los principios de la Carta de las Naciones Unidas y del Derecho Internacional. La Unión procurará desarrollar relaciones y crear asociaciones con los terceros países y con las organizaciones internacionales, regionales o mundiales que compartan los principios mencionados en el párrafo primero. Propiciará soluciones multilaterales a los problemas comunes, en particular en el marco de las Naciones Unidas".

Ediciones Universidad de Salamanca | CC BY-NC-ND

organizaciones a lo largo de su historia para alcanzar un mundo pacífico, justo y sostenible[294] dentro del marco del Derecho Internacional.

La segunda, no menos importante, es que las iniciativas estrictamente europeas para configurar una estructura de defensa propia e independiente no van a tener un apoyo decidido y quedarán relegadas sistemáticamente a la acción de la Alianza Atlántica, tanto por el interés de EE.UU., que no ve con buenos ojos esa posible autonomía continental, como por las contradicciones internas de los propios países europeos con visiones distintas en cuanto a la amenaza o al desarrollo de capacidades conjuntas para su defensa, entre otras. Paradójicamente, este planteamiento es radicalmente opuesto a la demanda actual de mayor potenciación de la seguridad de la Unión y sus Estados, como reacción a la amenaza real y próxima que supone la invasión rusa de Ucrania[295], que a su vez encaja con un reciente argumento que ayuda a entender la importancia de ese cambio que pivota en torno al concepto de *autonomía estratégica*, tan anhelada por Europa. En palabras del AR/VP Josep Borrell:

> "Porque el mundo ha cambiado. Sin ser «autónomos» es difícil declarar que somos una «unión política» capaz de actuar como «actor global» y como «Comisión geopolítica»" (BORRELL FONTELLES, 2020).

Conviene recordar, como ya se ha analizado anteriormente, que a mediados del siglo pasado en Europa se inician paralelamente una serie iniciativas para, por un lado, avanzar en la integración política y económica -las Comunidades Europeas- y, por otro, conseguir un compromiso de defensa mutua al margen de los EE.UU. -la Unión Europea Occidental-, con la idea de preservar los progresos de una vía de los posibles contratiempos en la otra. No obstante, autores como el profesor Coello de Portugal, consideran que el factor defensivo y militar de la Unión es intrínseco a su misma génesis política "porque el plan de unificación de Europa nació tras una II Guerra Mundial y con el ánimo decidido de evitar una tercera contienda armada" (COELLO DE PORTUGAL, 2024, pág. 91).

---

[294] Un ejemplo de este estrecho marco colaborativo entre la UE y las NNUU es el Comunicado de Prensa emitido por el Consejo Europeo el 23 de marzo de 2023, con ocasión de la sesión de trabajo del Consejo Europeo con el secretario general de las Naciones Unidas, António Guterres, destacando la importancia de la cooperación entre ellas para hacer frente a los desafíos actuales, subrayando el respaldo a la Carta de las NNUU y a sus principios, así como el respaldo al multilateralismo como eje central de actuación para avanzar en la colaboración que permita alcanzar un mundo pacífico, justo y sostenible. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/03/23/readout-of-the-working-session-of-the-european-council-with-the-un-secretary-general/ (19/10/2023).

[295] Cumplidos ya dos años de la guerra de agresión de Rusia contra Ucrania, la Unión es consciente de la posibilidad real de guerra y, fruto de ello, adopta una postura resuelta a seguir prestando apoyo a Ucrania de carácter político, financiero, económico, humanitario, militar y diplomático durante el tiempo que sea necesario. En concreto, en el apartado dos de las conclusiones del Consejo Europeo de 21 de marzo de 2024, se señala que "Ucrania, en el ejercicio de su derecho inmanente de legítima defensa, necesita urgentemente sistemas de defensa antiaérea, munición y misiles. En este momento crítico, la Unión Europea y los Estados miembros acelerarán e intensificarán la entrega de toda la asistencia militar necesaria. El Consejo Europeo se felicita de todas las iniciativas recientes en este sentido —en particular de la iniciativa puesta en marcha por Chequia para suministrar munición a Ucrania con carácter urgente- que posibilitarán el rápido cumplimiento del compromiso de la UE de proporcionar al país un millón de disparos de artillería". Disponible en: https://www.consilium.europa.eu/media/70843/20240321-euco-conclusions-es.pdf (21/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Los años noventa del siglo XX, marcados por la caída del muro de Berlín y la disolución de la URSS con sus consabidas consecuencias en el orden geopolítico mundial, motivan el anhelo de la Unión por consolidarse como verdadero actor internacional, para lo que necesita de una política exterior propia dirigida desde la consiguiente *autonomía estratégica* que le permita llevar a cabo acciones más asertivas en la defensa de sus intereses, coincidan estos o no con los de otros actores internacionales, y reivindicar su papel en el mundo. La firma del Tratado de Maastricht en 1992 simboliza un gran avance en este sentido por cuanto ordena las competencias de la Unión en torno a tres pilares, correspondiendo el segundo de estos pilares a la política exterior y de seguridad común (PESC)[296].

Los objetivos de la PESC son defender sus valores e intereses, consolidar la democracia, el Estado de Derecho y los derechos humanos, mantener la paz y prevenir los conflictos contribuyendo así a fortalecer la seguridad internacional, apoyar el desarrollo sostenible, fomentar la integración en el orden económico mundial, proteger el medio ambiente y contribuir a la gestión sostenible de los recursos naturales, prestar ayuda frente a las catástrofes a quienes lo necesiten y promover un sistema internacional basado en una cooperación multilateral sólida y en una buena gobernanza mundial. Esta PESC deberá ser *apoyada activamente y sin reservas* por los EEMM, que se comprometen a la solidaridad política mutua y al progreso en la convergencia de su actuación[297]. Asimismo, se abre la puerta al eventual establecimiento de una *política de defensa común* sobre la que construir una *fuerza de disuasión propia*, necesaria para demostrar una verdadera *autonomía estratégica* con la que alcanzar la pretendida relevancia internacional de la Unión y, con ello, amparar a sus ciudadanos bajo una égida de seguridad gestionada desde sus propios intereses.

Pero la realidad es que, pese a que en su origen fuera acertado afirmar que "la Unión Europea occidental es el producto de una cultura europea común" (HUNTINGTON, 1997, pág. 154), transcurridos más de setenta y cinco años del Tratado de Bruselas se puede constatar que:

> "[…] desde una perspectiva geopolítica, no solo Europa no es una unidad de análisis, sino que, además, son varias las partes de Europa que podrían ser mejor comprendidas si las tomáramos en cuenta como eslabones o prolongaciones de otros espacios, geopolíticamente más relevantes.
> Todo esto no puede ser omitido, pues contribuye sobremanera a entender las discrepancias tantas veces notadas (y anotadas, a modo de distintas

[296] El Título V del TUE se titula "Disposiciones generales relativas a la acción exterior de la Unión y disposiciones específicas relativas a la política exterior y de seguridad común", iniciando en el artículo 21 y finalizando en el 46, siendo así la PESC la parte del TUE con mayor número de artículos dedicados a desarrollar su materia. También configuran la base jurídica de la PESC los artículos 205 a 222 de la Quinta Parte del TFUE -Acción Exterior de la Unión-, y los artículos 346 y 347 de la Séptima Parte -Disposiciones Generales y Finales-.

[297] El artículo 24.2 TUE determina que "En el marco de los principios y de los objetivos de su acción exterior, la Unión dirigirá, definirá y ejecutará una política exterior y de seguridad común basada en el desarrollo de la solidaridad política mutua de los Estados miembros, en la identificación de los asuntos que presenten un interés general y en la consecución de una convergencia cada vez mayor de la actuación de los Estados miembros".

Ediciones Universidad de Salamanca | CC BY-NC-ND

> sensibilidades) entre las diferentes políticas exteriores y de seguridad de otros tantos Estados de la UE. Por el contrario, la ignorancia de estos factores contribuye a entender erróneamente que el hecho de que los diferentes Gobiernos europeos lleguen o no a acuerdos depende de la voluntad política de sus dirigentes, o poco más" (BAQUÉS QUESADA, 2023, págs. 30-31).

La disonancia en este pilar entre los EEMM y la Unión nos lleva a observar cómo los europeos tienen una *percepción diferente de los riesgos* conforme al Estado o región en el que se encuentren y, con ello, *de la amenaza a la que se exponen* de manera más directa. En otras palabras, "no todos los Estados europeos ven los problemas a través de las mismas lentes, ya que no comparten la misma historia ni la misma geografía. Y, en consecuencia, no tienen las mismas percepciones estratégicas" (BORRELL FONTELLES, 2020). Lo cual debe servir de ayuda para valorar en su justa medida todo el camino recorrido, hasta poder afirmar que:

> "[…] la competencia de la Unión en materia de política exterior y de seguridad común abarcará todos los ámbitos de la política exterior y todas las cuestiones relativas a la seguridad de la Unión, incluida la definición progresiva de una política común de defensa que podrá conducir a una defensa común"[298].

Lógicamente, para llegar hasta aquí consensuando la posición de atlantistas, europeístas y neutralistas, la UE ha tenido que hacer concesiones como esa prudente falta de concreción de plazos del Tratado de Maastricht para definir la política común de defensa, o el encaje de la *cláusula de abstención constructiva o solidaria* prevista para permitir alcanzar acuerdos en materia de política exterior sin necesidad de contar con unanimidad en la decisión y dejando una salida para los miembros que se acojan a ella[299].

Como ya hemos apuntado, el Tratado de Lisboa trata de avanzar en el proceso de integración apostando por dotar de un mayor protagonismo al Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, por cuanto amplia sus funciones al ejercer de vicepresidente de la Comisión (AR/VP) y al ostentar la presidencia permanente del Consejo Europeo. En este contexto, el Alto Representante tiene atribuida como función principal el velar por la unidad, la coherencia y la eficacia de la acción exterior de la Unión. Asimismo, ostenta el máximo nivel de representación y de dirección respecto al diálogo político con terceros y al establecimiento de la posición de la UE en las organizaciones y conferencias internacionales, para lo que cuenta con el

[298] Artículo 24.1 TUE

[299] El artículo 31.1 TUE dispone que "El Consejo Europeo y el Consejo adoptarán por unanimidad las decisiones de que trata el presente capítulo, salvo en los casos en que el presente capítulo disponga otra cosa. Se excluye la adopción de actos legislativos. En caso de que un miembro del Consejo se abstuviera en una votación, podrá acompañar su abstención de una declaración formal efectuada de conformidad con el presente párrafo. En ese caso, no estará obligado a aplicar la decisión, pero admitirá que ésta sea vinculante para la Unión. En aras de la solidaridad mutua, el Estado miembro de que se trate se abstendrá de cualquier acción que pudiera obstaculizar o impedir la acción de la Unión basada en dicha decisión y los demás Estados miembros respetarán su posición. En caso de que el número de miembros del Consejo que acompañara su abstención de tal declaración representara al menos un tercio de los Estados miembros que reúnen como mínimo un tercio de la población de la Unión, no se adoptará la decisión".

Ediciones Universidad de Salamanca | CC BY-NC-ND

apoyo del Servicio Europeo de Acción Exterior (SEAE), del Comité Político y de Seguridad (COPS) y de la Agencia Europea de Defensa (EDA).

El SEAE[300], auténtico servicio diplomático de la Unión, asiste al AR/VP en su función directiva de la PESC mediante sus propuestas con arreglo a la estrategia de la acción exterior y garantiza la coherencia de la misma apoyando a los servicios diplomáticos de los EEMM. Para esta labor cuenta con el bagaje que le proporcionan los análisis estratégicos que elabora el *EU Intelligence and Situation Centre* (EU INTCEN)[301], sobre la evaluación de la amenaza y los condicionantes geopolíticos que la definen conforme a la información facilitada por los servicios de inteligencia, las fuerzas armadas y los cuerpos policiales, integrada con la perspectiva de los diplomáticos. También se ocupa de velar por la coherencia de la acción exterior con respecto a las demás políticas de la Unión, y de facilitar apoyo y colaboración a las demás instituciones y órganos de la UE, en particular al Parlamento Europeo, al Presidente del Consejo Europeo, al Presidente del Consejo y a los miembros de la Comisión en el ejercicio de sus funciones respectivas en el ámbito de las relaciones exteriores.

Por su parte, el COPS[302] es responsable del seguimiento permanente de la situación internacional en lo concerniente a los intereses de la acción exterior y la política de defensa europeas, ejerce el control político y la dirección estratégica de las operaciones de gestión de crisis y contribuye a la definición de dichas políticas mediante la emisión de informes dirigidos al Consejo a demanda de éste, del AR/VP o por propia iniciativa. Está integrado por miembros del SEAE y por los embajadores de los EEMM en Bruselas.

La EDA[303] es el principal organismo para la planificación y priorización de capacidades de defensa de la Unión y se encarga de facilitar la cooperación entre los EEMM para el desarrollo de capacidades de defensa, promover la investigación y la innovación tecnológica en materia de armamento, impulsar la formación, la adquisición conjunta y

[300] El artículo 27.3 TUE establece que "En el ejercicio de su mandato, el Alto Representante se apoyará en un servicio europeo de acción exterior. Este servicio trabajará en colaboración con los servicios diplomáticos de los Estados miembros y estará compuesto por funcionarios de los servicios competentes de la Secretaría General del Consejo y de la Comisión y por personal en comisión de servicios de los servicios diplomáticos nacionales. La organización y funcionamiento del servicio europeo de acción exterior se establecerán mediante decisión del Consejo, que se pronunciará a propuesta del Alto Representante, previa consulta al Parlamento Europeo y previa aprobación de la Comisión". Su desarrollo normativo es a través de la Decisión del Consejo de 26 de julio de 2010 por la que se establece la organización y funcionamiento del Servicio Europeo de Acción Exterior. Diario Oficial de la Unión Europea L201/30 (2010/427 UE). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A32010D0427 (20/10/2023).

[301] Centro de Inteligencia y de Situación de la UE.

[302] El artículo 38 TUE recoge las funciones del Comité Político y de Seguridad.

[303] El artículo 42.3 TUE señala que "…La Agencia en el ámbito del desarrollo de las capacidades de defensa, la investigación, la adquisición y el armamento (en lo sucesivo denominada «Agencia Europea de Defensa») determinará las necesidades operativas, fomentará medidas para satisfacerlas, contribuirá a definir y, en su caso, a aplicar cualquier medida oportuna para reforzar la base industrial y tecnológica del sector de la defensa, participará en la definición de una política europea de capacidades y de armamento y asistirá al Consejo en la evaluación de la mejora de las capacidades militares". La EDA fue creada en 2004 por una Acción Conjunta del Consejo de Ministros (2004/551/PESC) y tiene su sede en Bruselas. Actualmente se rige por la Decisión (PESC) 2015/1835 del Consejo, de 12 de octubre de 2015, sobre el estatuto, la sede y las normas operativas de la EDA.

Ediciones Universidad de Salamanca | CC BY-NC-ND

la interoperabilidad de sistemas y componentes de defensa de los EEMM, así como fortalecer la base industrial de defensa europea. Esta Agencia es presidida por el AR/VP y la integran los Ministros de Defensa de los EEMM.

En cuanto al desempeño de las funciones del AR/VP, éste debe consultar periódicamente al Parlamento Europeo sobre los principales asuntos estratégicos y las opciones que para su tratamiento plantea, e informarle de la evolución de esta política para la elaboración de la *Resolución Anual sobre la aplicación de la PESC*[304], procedimiento a través del cual se efectúa el correspondiente *control parlamentario*, legitimador de la acción exterior ejercida.

La relación entre ambas instituciones se organiza mediante informes elaborados *ad hoc* por comisiones especializadas entre las que, por su relevancia y actualidad, y por ser objeto de estudio de esta tesis doctoral, cabe destacar la *Comisión especial sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación, y sobre el fortalecimiento de la integridad, la transparencia y la rendición de cuentas en el Parlamento Europeo*[305], de cuyos resultados debe rendir cuentas en el periodo de sesiones anual que se establezca[306]. Esta comisión especial, con mandato temporal, es la respuesta del Parlamento ante el descubrimiento de casos de corrupción entre sus miembros con terceros países involucrados[307], y la evidencia de la grave violación de valores y principios que supone la interferencia de actores extranjeros, estatales y no estatales, maliciosos y autoritarios, que están utilizando la manipulación de la información y otras tácticas para interferir en los procesos democráticos en la UE[308], como se ha comprobado que viene haciendo Rusia desde

[304] La Resolución del Parlamento Europeo, de 18 de enero de 2023, sobre la aplicación de la política exterior y de seguridad común: informe anual 2022: Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0009_ES.html (20/10/2023).

[305] El 18 de junio de 2020, el Parlamento Europeo decidió crear esta Comisión Especial sobre injerencias extranjeras en los procesos democráticos de la Unión Europea, con el mandato de formular un enfoque a largo plazo para detectar, analizar y hacer frente a las pruebas de injerencias extranjeras en las instituciones y, principalmente, en los procesos democráticos de la Unión y sus Estados miembros. Ésta se crea el 23 de septiembre de 2020.

[306] El primer Comité Especial sobre Injerencia Extranjera en todos los Procesos Democráticos de la Unión Europea, incluida la Desinformación (INGE), finalizó su mandato tras 18 meses de trabajo con un informe final -INGE1- que fue adoptado en el pleno del Parlamento el 9 de marzo de 2022 y que supuso la creación al día siguiente de un nuevo Comité Especial (ING2) para dar seguimiento y continuidad a la labor iniciada con el primer informe. Disponible en: https://www.europarl.europa.eu/committees/es/ing2/home/highlights (20/10/2023).

[307] El caso de las sospechas de corrupción entre los europarlamentarios ha tenido amplia cobertura en los medios de comunicación. Disponible en: https://www.europarl.europa.eu/news/es/press-room/20221212IPR64541/escandalo-de-corrupcion-eurodiputados-plantean-cambios-para-mas-transparencia
https://www.bbc.com/mundo/noticias-internacional-63951652
https://elpais.com/internacional/2022-12-13/las-claves-de-qatargate-el-escandalo-de-sobornos-que-ha-sacudido-el-parlamento-europeo.html (20/10/2023).

[308] Esta línea de acción de la PESC parte de la constatación de que actualmente, aunque se está trabajando en ello, la UE y sus Estados miembros aún no cuentan con un régimen específico legal y de sanciones para responder ante la interferencia extranjera y las campañas de desinformación, por lo que se hace necesario definir una estrategia común para hacer frente a esta amenaza. En este sentido puede consultarse el informe de Injerencias extranjeras en los procesos democráticos de la UE, de mayo de 2023, del

Ediciones Universidad de Salamanca | CC BY-NC-ND

antes de la invasión de Ucrania, tratando de aprovecharse del pluralismo de las democracias atacando sus procesos electorales, tanto locales, como regionales y nacionales y, también, fijando como objetivo las elecciones al Parlamento Europeo en 2024.

Todo ello viene a poner de relieve la importancia de la *autonomía estratégica europea* y su delimitación conceptual, por cuanto no se circunscribe únicamente al campo de la acción exterior o de la defensa, sino que tiene vinculación con diferentes ámbitos, como el económico, el energético, el tecnológico, el medio ambiental, el del comercio de materias primas o el de la extracción de metales y tierras raras (DACOBA CERVIÑO, 2021, pág. 3). Podemos por ello concluir que existe un *sesgo de defensa* en la práctica totalidad de las políticas sectoriales y ámbitos de actividad de la Unión por cuanto, implícitamente, hacen suyo el factor geoestratégico como pilar sustancial de las capacidades defensivas conjuntas (COELLO DE PORTUGAL, 2024, pág. 96).

La cuestión que subyace no es otra que la *propia existencia de la Unión* en un contexto geoestratégico altamente inestable y cambiante, tratando de mantener una complicada posición equidistante entre poderosos competidores sistémicos que se miran a los ojos desafiantes y a los que, de ninguna manera, se quiere ofender mientras se busca no continuar perdiendo relevancia en el escenario de capacidad de influencia a nivel mundial. La visión clásica del mundo occidental ha cambiado y Europa cada vez tiene menos presencia en un nuevo mapa global cuyo eje de coordenadas se ha desplazado hacia el Indo-Pacífico atraído por argumentos de índole demográfica[309], de carácter económico[310] o de competencia tecnológica e industrial[311]. Al mismo tiempo se han complicado las relaciones internacionales por cuanto los juegos de intereses generan extrañas parejas de baile como el caso de India, aliada de EE.UU. frente a China, mientras que también es socia económica de Rusia frente a Occidente. En medio de todo ello aparecen nuevos actores públicos y privados -organizaciones no gubernamentales, asociaciones, grupos de presión de distinta naturaleza- con intereses heterogéneos e, incluso, enfrentados y con una visión diferente de lo que sucede en el mundo, de lo que son problemas y de lo que pueden ser soluciones. Por ello, como dice el AR/VP Josep Borrell:

> "La conclusión es sencilla. Si no actuamos juntos ahora, seremos irrelevantes, como muchos señalan de forma convincente. La autonomía estratégica es, desde esta perspectiva, un proceso de supervivencia política" (BORRELL FONTELLES, 2020).

En lo que se refiere al ámbito de la seguridad y la defensa, que es el que nos ocupa, la *autonomía estratégica europea* ha sido factor de enfrentamiento interno entre los

Parlamento Europeo. Disponible en: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)747908 (20/10/2023).

[309] China e India suman entre ambas aproximadamente el sesenta por ciento de la población mundial.

[310] China es en 2022 la segunda economía del mundo por volumen de PIB e India podría convertirse en la tercera en cuestión de pocos años.

[311] China aglutina en su territorio al ochenta por ciento de los fabricantes de fármacos, es el mayor productor del mundo de coches eléctricos y de teléfonos móviles, mientras que entre Taiwán y Corea del Sur suman más del ochenta por ciento de la producción mundial de chips.

Ediciones Universidad de Salamanca | CC BY-NC-ND

miembros que la han entendido como "medio para recuperar el espacio político frente a los Estados Unidos" y aquellos otros "para los que tenía que evitarse, precisamente por miedo a acelerar el desentendimiento de Europa por parte de los Estados Unidos" (BORRELL FONTELLES, 2020). La cuestión que subyace no es otra que la elección del paraguas bajo el que los diferentes miembros de la Unión se sienten más protegidos frente a la amenaza que, eso sí, compartimos: Rusia.

Pero, aun así, debemos traer nuevamente a colación la disparidad de visiones existentes dentro de la Unión, pues no todos los socios europeos interpretan la defensa, la disuasión ni la potencialidad de la amenaza de igual manera.

Gran parte de ellos, principalmente del arco nororiental[312], es decir, los más próximos a las fronteras rusas, consideran que solo bajo el escudo de la OTAN y, por ende, de la preeminencia militar de EE.UU., se dispone de una auténtica disuasión. Sin embargo otros, más alejados geográficamente de Rusia, entienden que tanto la OTAN en el Concepto Estratégico de Madrid de junio de 2022, como EE.UU., en su Estrategia de Seguridad Nacional adoptada por la Administración Biden en octubre del mismo año, dejan claro que la nueva prioridad estratégica es China y la región del Indo-Pacífico, en tanto que la UE, firme defensora de la multilateralidad, tiene amplias relaciones comerciales con China y, por evidentes razones geográficas, también debe mirar hacia Rusia como incómodo vecino frente al que tiene que mantenerse alerta pero con el que no debe romper puentes de manera definitiva.

Este último planteamiento obliga a la Unión a progresar de manera conjunta hacia una legítima *alianza defensiva autónoma e independiente* como única opción realmente viable para garantizar su defensa territorial, reservándose "el derecho a intervenir, incluso militarmente, en cualquier lugar del mundo, ya sea fuera, o dentro, de la zona OTAN" (BAQUÉS QUESADA, 2023, pág. 125) siempre que ello represente un interés para ella. Un claro ejemplo lo representa la situación de conflictos y tensiones constantes en la zona del Sahel y el Mediterráneo oriental, donde "Europa debe actuar aún más, y por sí sola, porque estos problemas no afectan principalmente a los Estados Unidos" (BORRELL FONTELLES, 2020).

Por ello, el papel que ansía desempeñar la UE en el actual contexto de *great power competition* pasa por confiar en sí misma para gobernar su propio destino, porque sin la autonomía estratégica que respalde nuestro proyecto político no tendremos capacidad para posicionarnos como actor global determinante en la actual esfera geopolítica. Y esto requiere un plan de acción consensuado y la voluntad y los recursos para llevarlo a cabo. De otra manera, Europa será irrelevante.

3.2.1. La Estrategia Europea de Seguridad: una Europa segura en un mundo mejor (2003 – 2008)

[312] Es el caso de Polonia, Hungría, República Checa, Eslovaquia, Eslovenia, Estonia, Lituania, Letonia, Suecia o Finlandia.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En la reunión informal de Ministros de Asuntos Exteriores de la Unión que tiene lugar en mayo de 2003 en la isla griega de Kastelorizo, se encomienda al AR/VP Javier Solana la elaboración de un conjunto de indicaciones a partir de las que definir una estrategia global en el ámbito de la política exterior y de seguridad, documento que se presenta al Consejo Europeo de Salónica un mes después bajo el título de *Una Europa segura en un mundo mejor*. Esta propuesta es aceptada en diciembre de ese mismo año en Bruselas por el Consejo Europeo con la denominación oficial de *Estrategia Europea de Seguridad* (EES), siendo la primera vez que "la UE se ponía de acuerdo para realizar una evaluación conjunta de las amenazas y establecer objetivos comunes para promover sus intereses de seguridad partiendo de nuestros valores básicos"[313].

Esta primera estrategia, que presenta una Unión Europea como *actor global en materia de seguridad*, contempla los riesgos y amenazas a los que se enfrenta en un contexto internacional marcado por los terribles atentados del 11 de septiembre de 2001 en suelo norteamericano y la invasión de Irak de 2003, que conlleva un elevado desgaste interno para la Unión a cuenta de la falta de consenso entre los Estados que apoyan la invasión -Reino Unido, España e Italia- y los que se oponen a ella -liderados por el eje franco alemán-, dejando patente por un lado las divergencias en la interpretación del contexto geopolítico entre EE.UU. y la UE, y por otro la "inexistencia flagrante de una política exterior y de seguridad común" (ALAMINOS HERVÁS, 2018, pág. 15). Además, la UE se encuentra en el proceso de redacción de una *Constitución Europea* y atando los últimos cabos para la ampliación de quince a veinticinco Estados miembros que supondrá a corto plazo el Tratado de Atenas, asuntos de amplia relevancia que alientan a proclamar en su inicio que "Europa tiene que estar dispuesta a asumir su responsabilidad en el mantenimiento de la seguridad mundial y la construcción de un mundo mejor".

Para desarrollar este mensaje la EES se organiza en tres grandes apartados: las amenazas, los objetivos estratégicos y las implicaciones derivadas. Comienza así desgranando los *desafíos mundiales y las principales amenazas* para la seguridad de la Unión, siendo los primeros los riesgos asociados a la globalización y la consiguiente desaparición de las fronteras como clásico delimitador de la seguridad interior y la seguridad exterior, toda vez que "las amenazas lejanas pueden ser tan inquietantes como las cercanas", caracterizadas por una naturaleza más diversa y menos previsible que las tratadas en la segunda mitad del siglo pasado. Estas nuevas amenazas son el terrorismo en todas sus facetas, la proliferación de armas de destrucción masiva, los conflictos y crisis regionales con repercusión directa o indirecta en los intereses europeos, la descomposición de los Estados como consecuencia del mal gobierno y el colapso institucional, y la delincuencia organizada asociada a estructuras criminales que, incluso, pueden llegar a debilitar al Estado.

En segundo lugar, respecto a los *objetivos estratégicos*, se refleja a través de ellos la filosofía de "pensar a escala mundial y actuar a escala local" como forma de articular la gestión preventiva que permita a la UE proyectar estabilidad en su entorno y actuar, con todos los instrumentos a su alcance y en colaboración con sus socios, antes de que se

[313] Preámbulo de D. Javier Solana al "Informe sobre la aplicación de la Estrategia Europea de Seguridad: ofrecer seguridad en un mundo en evolución", de diciembre de 2008. Disponible en: https://www.consilium.europa.eu/media/30808/qc7809568esc.pdf (20/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

genere el conflicto o situación de crisis y, con ello, tratar de evitar sus consecuencias indeseadas. Estos objetivos estratégicos se agrupan en tres grandes bloques que abarcan, en primer lugar, el modo de afrontar las amenazas previamente identificadas mediante la combinación de todos los mecanismos de actuación disponibles, sean estos de carácter político, económico, civil, diplomático, comercial o, incluso, militar. En segundo lugar, la Unión define como estratégico el objetivo de crear seguridad en los países vecinos, yendo más allá de la necesaria estabilidad política al juzgar como premisa excluyente de la cooperación y elemento esencial de las relaciones de vecindad la buena gobernanza, en el convencimiento de que "la mejor protección para nuestra seguridad es un mundo de Estados democráticos bien gobernados". El tercer objetivo estratégico es la consolidación de un orden internacional basado en un multilateralismo eficaz, con una sociedad de actores estatales y no estatales que adecúan sus relaciones al imperio del Derecho Internacional con la Carta de las NNUU en la cúspide.

El tercer y último gran apartado está dedicado a las *implicaciones estratégicas para Europa*, a fin de señalar el camino a seguir para continuar avanzando en su política exterior y de seguridad de manera coherente y conjunta. Para ello incide:

1. En la necesidad de ser *más activos* en la prosecución de sus propios objetivos estratégicos, a través de la gama completa de instrumentos para coordinar la intervención preventiva de conflictos y la gestión de crisis de que dispone la UE.
2. En la necesidad de ser *más capaces* fomentando el desarrollo de todo el potencial militar, civil, diplomático y colaborativo con nuestros aliados, mediante decisiones estratégicas como la creación de la Agencia Europea de Defensa, o a nivel táctico ampliando las misiones desplegadas en el marco de los acuerdos Berlín Plus[314].
3. Y finalmente, en la necesidad de ser *más coherentes* armonizando la política exterior de la Unión y del resto de Estados miembros, incluso yendo más allá con el ámbito colaborativo de Justicia e Interior, puesto que "juntos somos más fuertes".

Cinco años después, en diciembre de 2008, el AR/VP Javier Solana presenta al Consejo Europeo el *Informe sobre la Aplicación de la Estrategia Europea de Seguridad: ofrecer seguridad en un mundo en evolución* (IApEES), en el que se analizan puntos de mejora de la EES partiendo de dos mensajes a nuestro entender esenciales -aunque contrapuestos- para interpretar el conjunto del documento. El primero de ellos es que si la Unión quiere proteger a sus ciudadanos debe estar en condiciones de determinar los acontecimientos, lo que "supone un pensamiento cada vez más estratégico, a la vez que una mayor eficacia y perceptibilidad de nuestra actuación en todo el mundo". Y el

[314] En marzo de 2003 se firma el Acuerdo Berlín Plus por la OTAN -representada por su secretario general George Robertson- y la UE –por el AR/VP Javier Solana- que recoge la intervención en misiones y operaciones de interés para la Unión conforme a cuatro grandes consideraciones:

1. El acceso de la UE a las capacidades de planeamiento de la OTAN.
2. La puesta a disposición de las capacidades militares de la OTAN para la ejecución de esas misiones de interés de la UE.
3. Estas operaciones de la Unión siempre serán dirigidas por un mando militar europeo –el SACEUR-.
4. El compromiso de adaptación de las estructuras de mando de la OTAN para que puedan interoperar con la UE en estas misiones.

Ediciones Universidad de Salamanca | CC BY-NC-ND

segundo, referido a que la UE y la OTAN "deben intensificar su asociación estratégica" sobre la base de la historia y la responsabilidad compartida en el ámbito de la seguridad. Este es un dilema planteado en la Estrategia de 2003 que, lejos de resolverse en la revisión de 2008, se aviva por cuanto la Unión busca influir en el orden internacional a través de su propia política exterior, mientras que autolimita el desarrollo de su política de seguridad al marco de intereses compartidos con la OTAN -y por tanto con EE.UU.-, lo cual genera consecuencias.

En cuanto al desarrollo formal y de contenido, el IApEES en su primer punto presenta los *retos mundiales y principales amenazas* que afectan a los intereses de la Unión en el ámbito de la seguridad. Ya no se refiere a *desafíos,* sino que habla de *retos*, semejantes aunque más complejos y prevalentes ahora. Así, aumenta el riesgo derivado de la proliferación de armas de destrucción masiva por el contexto nuclear a nivel global –Libia, Irán, Corea del Norte-. El terrorismo continúa golpeando en todo el mundo y consuma dos atentados en suelo europeo –en Madrid y Londres, en 2004 y 2005 respectivamente- que obligan a elevar los niveles de alerta y a avanzar en la Estrategia de la UE de lucha contra el terrorismo[315], implicando a las estructuras judiciales, policiales y de inteligencia. Aparece la primera referencia explícita a la ciberseguridad como amenaza vinculada a la protección de las infraestructuras críticas y como "nueva arma económica, política y militar". También la seguridad energética es objeto de atención, considerándose necesaria la "mayor diversificación de los combustibles, de las fuentes de suministro y de las rutas de tránsito" por cuanto la energía es un factor destacado de las relaciones entre la UE y otros países, entre los que destaca Rusia[316]. Finalmente, el cambio climático como factor multiplicador de amenazas y exacerbador de conflictos, especialmente en situaciones de pobreza y crecimiento demográfico.

El segundo punto del IApEES se centra en el *afianzamiento de la estabilidad en Europa y en otros sitios*, que comienza confiando en la política de ampliación de la Unión como "motor poderoso de estabilidad, paz y reforma", para después presentar la *política europea de vecindad* (PEV), iniciada en el 2004, como caso de éxito para coordinar las

[315] La Estrategia de la UE de lucha contra el terrorismo, de noviembre de 2005, se compone de cuatro aspectos que se ajustan a su compromiso estratégico de luchar contra el terrorismo de forma global, al tiempo que se respetan los derechos humanos y se crea una Europa más segura, que permita a sus ciudadanos vivir en un espacio de libertad, seguridad y justicia. Los cuatros pilares son la prevención de la radicalización y la captación, la protección de los objetivos personales y críticos potenciales, la persecución e investigación de los autores, y la respuesta para gestionar y enfrentar las consecuencias de un atentado.

[316] Sin duda la visión estratégica del AR/VP Javier Solana en 2008 era plenamente acertada en cuanto a la amenaza que supone la dependencia energética de la UE respecto a Rusia. A pesar de ello a principios de 2022, cuando Moscú decide invadir Ucrania, la Unión aún recibe aproximadamente el 40% de su gas de Rusia, mayormente a través del gasoducto que atraviesa el mar Báltico conocido como Nord Stream 1, inaugurado en 2012. El proyecto de ampliación a través del Nord Stream 2 no llega a entrar en servicio a raíz de la guerra. En respuesta, la Comisión Europea pone en marcha el 8 de marzo de 2022 la "Repower EU: Acción conjunta para una energía más asequible, segura y sostenible" en la que, entre otros aspectos, reconoce el papel potencial de las ayudas de Estado para apoyar a las empresas y sectores gravemente afectados por la evolución geopolítica del momento. A nivel nacional, el Gobierno de España publica el Real Decreto-ley 6/2022, de 29 de marzo, por el que se adoptan medidas urgentes en el marco del Plan Nacional de respuesta a las consecuencias económicas y sociales de la guerra en Ucrania. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-4972 (25/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

relaciones de la Unión con los países de su entorno próximo y con necesaria proyección más allá del vecindario inmediato por las consecuencias para los intereses de seguridad europeos. En este bloque se refiere a la estrecha vinculación entre seguridad, paz y desarrollo, a la piratería en las rutas marinas comerciales como nueva dimensión del crimen organizado, y al tráfico de armas ligeras, minas y municiones.

El IApEES cierra con un tercer apartado titulado *Europa en un mundo cambiante*, que vuelve a insistir en la necesidad de una Unión más eficaz y más capaz a través del incremento de sus capacidades militares, el régimen de colaboración recíproca y el reparto de cargas que nos permitan mejorar la coordinación estructural, adoptar decisiones estratégicas de forma autónoma y llevar a cabo una prevención temprana de la amenaza. Continúa refiriéndose al compromiso con nuestros vecinos para alcanzar mayor nivel de integración regional y al multilateralismo europeo, donde enfatiza el carácter de socio fundamental de los EE.UU. y el avance con la Unión Africana en la mejora de sus capacidades de gestión de crisis.

En cuanto a la repercusión práctica de la IApEES, haciéndonos eco de la opinión de algunos autores, podría decirse que fue de "acuse de recibo y olvido inmediato", en medio de un contexto de debilidad política -marcada por el referéndum irlandés al Tratado de Lisboa-, de inestabilidad estratégica -por el apoyo militar de Rusia a la autoproclamación de independencia de Abjasia y Osetia del Sur respecto de Georgia- y de profunda crisis financiera y económica mundial (ARTEAGA MARTÍN, 2016).

Dicho lo anterior, una vez analizada la EES de 2003 y su actualización de 2008, debemos dejar claro el valor de su repercusión como primera estrategia que define el marco conceptual de la seguridad europea, consensuada y aceptada por todos los socios, con la que "se ha conseguido mucho en poco tiempo" y que busca dar una imagen de la Unión más allá de la que proyecta como potencia civil abrazada al *soft power*[317], en cuanto poder de atracción a través de su cultura, sus valores y la autoridad moral transmitida a través de su política exterior (NYE, 2004, págs. 6-11). No obstante, debemos hacer un análisis crítico del documento para señalar las carencias y errores de planteamiento con las que hubo de lidiar desde su nacimiento.

En primer lugar, hay que advertir que es de rigor que los objetivos estratégicos sean definidos "en función de los intereses y de los retos, riesgos y amenazas, determinando el modo en que cada uno afecta a la seguridad de la Unión" (RUBIO DAMIÁN, 2012, pág. 10). Por ello, llama la atención la falta de definición de los intereses concretos que la UE quiere proteger con su EES, lo que nos obliga a deducir que estos habrán de ser, lógicamente, los recogidos en el artículo 21 TUE[318] para la PESC. De hecho, habría sido

[317] Joseph S. Nye conceptualiza el término *soft power* señalando que no es lo mismo que el poder de influir, que puede basarse en el *hard power* de las amenazas o la presión económica. El *soft power* es más que la simple persuasión o la capacidad de mover a la gente mediante argumentos, es la capacidad de atraer y de conseguir el consentimiento. En resumen, el *soft power* es el *attractive power*.

[318] El artículo 21 TUE establece que: "1) La acción de la Unión en la escena internacional se basará en los principios que han inspirado su creación, desarrollo y ampliación y que pretende fomentar en el resto del mundo: la democracia, el Estado de Derecho, la universalidad e indivisibilidad de los derechos humanos y de las libertades fundamentales, el respeto de la dignidad humana, los principios de igualdad y solidaridad y el respeto de los principios de la Carta de las Naciones Unidas y del Derecho Internacional.

Ediciones Universidad de Salamanca | CC BY-NC-ND

incluso conveniente concretarlos "en forma de objetivos de seguridad más operativos", cuestión que "resalta en mayor medida al compararlos con los objetivos e intereses a proteger contenidos en las estrategias nacionales, o incluso con los establecidos por la OTAN y la UEO" (ENSEÑAT Y BEREA, 2004, pág. 87).

En segundo lugar, debemos referirnos al carácter descriptivo y meramente doctrinal de las implicaciones estratégicas, donde se habla del desarrollo de las capacidades militares de la Unión y del gasto en defensa conjunto de sus miembros, pero que no concreta los supuestos, ni la forma ni los plazos para conseguir ese valor añadido que permita una "intervención temprana, rápida y, en caso necesario, contundente", así como tampoco hace mención a la *cláusula de defensa colectiva* del artículo 42.7 TUE, clave de la acción de respuesta coordinada y solidaria ante una agresión violenta a alguno de los Estados de la UE. Algunos autores contemplan la posibilidad de que "el necesario consenso probablemente haya obligado a mantener a la defensa ausente del documento, lo que permite albergar dudas de la propia consistencia de la estrategia elaborada" (ENSEÑAT Y BEREA, 2004, pág. 112).

En tercer lugar, no queda claro el encaje de este instrumento militar europeo que, por un lado, debe amoldarse al acuerdo transatlántico Berlín Plus y limitarse a las misiones allí definidas[319] y, por otro, debe mejorar sus capacidades alineado con lo que ya se declaró en el Consejo Europeo de Colonia de 1999 en cuanto a que "la Unión debe tener una capacidad de acción autónoma, respaldada por unos recursos militares creíbles, los medios para decidir emplearlos y la disposición de hacerlo, con objeto de responder a las crisis internacionales, sin perjuicio de la actuación de la OTAN". Porque, para tener *autonomía estratégica* y poder defender tus intereses como actor relevante en la escena internacional no solo hay que disponer de las capacidades militares y de su poder de disuasión, sino que también hay que tener el convencimiento y la firme decisión de *utilizarlas*, de manera *contundente* llegado el caso. La autonomía estratégica es

La Unión procurará desarrollar relaciones y crear asociaciones con los terceros países y con las organizaciones internacionales, regionales o mundiales que compartan los principios mencionados en el párrafo primero. Propiciará soluciones multilaterales a los problemas comunes, en particular en el marco de las Naciones Unidas.

2) La Unión definirá y ejecutará políticas comunes y acciones y se esforzará por lograr un alto grado de cooperación en todos los ámbitos de las relaciones internacionales con el fin de: a) defender sus valores, intereses fundamentales, seguridad, independencia e integridad; b) consolidar y respaldar la democracia, el Estado de Derecho, los derechos humanos y los principios del Derecho Internacional; c) mantener la paz, prevenir los conflictos y fortalecer la seguridad internacional, conforme a los propósitos y principios de la Carta de las Naciones Unidas, así como a los principios del Acta Final de Helsinki y a los objetivos de la Carta de París, incluidos los relacionados con las fronteras exteriores; d) apoyar el desarrollo sostenible en los planos económico, social y medioambiental de los países en desarrollo, con el objetivo fundamental de erradicar la pobreza; e) fomentar la integración de todos los países en la economía mundial, entre otras cosas mediante la supresión progresiva de los obstáculos al comercio internacional; f) contribuir a elaborar medidas internacionales de protección y mejora de la calidad del medio ambiente y de la gestión sostenible de los recursos naturales mundiales, para lograr el desarrollo sostenible; g) ayudar a las poblaciones, países y regiones que se enfrenten a catástrofes naturales o de origen humano; y h) promover un sistema internacional basado en una cooperación multilateral sólida y en una buena gobernanza mundial.

[319] Misiones humanitarias y de rescate, de mantenimiento o imposición de la paz, de gestión de crisis, de apoyo en la lucha contra el terrorismo o de control de desarme en conflictos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

"capacity to act autonomously when and where necessary and with partners wherever possible"[320].

Tampoco especifica la EES, al manifestar la necesidad de ser *más activos y capaces* para avanzar en la PESC a través del desarrollo de todo nuestro potencial militar y civil, de qué manera ni a través de que capacidades se deberían afrontar las amenazas, ni el procedimiento para implementar esa estrategia de acción colaborativa con nuestros aliados. En este mismo sentido, no se concreta la forma en la que se debe avanzar para armonizar la política del segundo y tercer pilar de la Unión y del resto de Estados miembros para ser *más coherentes* en el desempeño y más creíbles en la defensa de nuestros intereses (ALAMINOS HERVÁS, 2018, pág. 17).

Finalmente, en cuanto a la pretendida *asociación eficaz y equilibrada con EE.UU.* como socio privilegiado, compartiendo liderazgo y cargas, se analizará en el capítulo dedicado a la PCSD que EE.UU. siempre ha mirado con recelo el pilar europeo de la defensa y ha cuestionado el compromiso presupuestario de sus miembros con la OTAN, argumento que ha alimentado la percepción estadounidense de que Europa pretende tener una seguridad *low cost* a expensas de ellos lo cual, para un actor internacional principal que está decidido a mantener el liderazgo global con los costes políticos, económicos y militares que ello comporta, supone un planteamiento estratégico que no parece cuadrar con la pretensión europea de asociación eficaz y equilibrada entre iguales que propugna la EES. Para que esto suceda es necesario que se consolide la PESC como pieza clave de una Europa más capaz y determinada a defenderse, desde el papel de socio *inter pares* con EE.UU., lo cual está lejos de suceder en la primera década del siglo XXI. Para llegar a este nivel de desarrollo será aún necesario recorrer un largo camino de búsqueda de consenso e identificación de intereses, y de inversión presupuestaria a largo plazo en el ámbito de la defensa.

3.2.2. La Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea. Una visión común, una actuación conjunta: una Europa más fuerte (2016)

Si el complicado marco internacional en el que se fragua la EES de 2003 se define por la sinrazón del terrorismo, por la división frente a la invasión de Irak, por una Constitución Europea *non nata* y el vértigo de la mayor ampliación en la historia de la Unión, no es más optimista el ambiente que calienta el fogón donde se forja la estrategia que la sustituye, con una crisis financiera y económica mundial que se arrastra desde el 2008 al 2014, los atentados de DAESH en París en noviembre de 2015 y la salida de Reino Unido de la UE con el referéndum del *Brexit* en 2016[321] que, en principio, "dejaba una

[320] Esta definición de la autonomía estratégica como la "capacidad para actuar de manera autónoma cuando y donde sea necesario y, en la medida de lo posible, con los países asociados" se contempla en el apartado 2 de la Introducción de las Conclusiones del Consejo sobre la aplicación de la Estrategia Global de la UE en materia de Seguridad y Defensa. Disponible en: https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf (26/10/2023).

[321] El Acuerdo de Retirada del Reino Unido se ratificó el 30 de enero de 2020, conforme al artículo 50 TUE, cuyo apartado 1 estipula que "Todo Estado miembro podrá decidir, de conformidad con sus normas constitucionales, retirarse de la Unión", mediante negociación entre las partes con arreglo al apartado 3 del artículo 218 TFUE.

Ediciones Universidad de Salamanca | CC BY-NC-ND

UE con menor credibilidad estratégica, sin apenas capacidad disuasoria, con un músculo militar atrofiado y cada vez más dependiente de Washington para la seguridad euroatlántica" (COLOM PIELLA & CÓZAR MURILLO, 2022, pág. 90)

A pesar de lo demandante que resulta este clima geopolítico multipolar y complejo, o precisamente por esto mismo, la Unión tiene claro que necesita reconsiderar su política exterior y de seguridad para replantear su estrategia. Nadie duda de la importancia que la coordinación eficaz y la coherencia en la acción exterior tienen para el posicionamiento de la UE en ese contexto cambiante, por lo que se define el *enfoque integral*[322] como "guía de su actividad en el ámbito de la seguridad, de forma particular en lo referente a la gestión de crisis y la resolución de conflictos" (ALAMINOS HERVÁS, 2018, pág. 20). Se inicia por ello un proceso de consulta abierto y transparente para la redacción de esta nueva estrategia de seguridad en el que participan expertos en la materia, académicos, representantes de los Estados y las propias instituciones de la UE, liderados por el Instituto de Estudios de Seguridad de la UE (EUISS).

En esta dinámica, en septiembre de 2015, el EUISS publica un documento clave para entender la perentoria necesidad de redactar una nueva estrategia de seguridad. Se trata del libro *Hacia una estrategia global de la UE: antecedentes, proceso, referencias*[323], en cuyo prefacio la otrora recientemente nombrada AR/VP, Federica Mogherini, reflexiona sobre las tres principales razones que la sustentan. La primera de ellas es que la Unión necesita definir un marco de trabajo de su acción exterior que le permita combinar la respuesta rápida con la negociación paciente, la prevención de conflictos y la intervención postcrisis. Y debe ser ella, la UE, quien marque su propia agenda para no limitarse a ser meramente reactiva, por lo que debe definir y priorizar dónde puede, dónde debe y dónde quiere estar. Y ello requiere una estrategia de enfoque global. La segunda razón que identifica la AR/VP es en relación al amplio abanico de instrumentos de acción exterior que el Tratado de Lisboa confiere a la Unión para ser empleados, desde el *comprehensive approach*, en orden a dar un tratamiento holístico a los conflictos, a las crisis y al conjunto de la política exterior, que debe ser coherente en su conjunto como parte del enfoque global de la estrategia. En tercer lugar, Mogherini se muestra convencida de que las actuales amenazas asimétricas y multidimensionales conllevan la estrecha relación entre la seguridad interior y exterior, por lo que la UE debe estar particularmente atenta a lo que ocurre fuera de sus fronteras porque, de una u otra manera, puede acabar afectando a la seguridad y a los intereses de sus ciudadanos. Por eso deben generarse sinergias entre todos los Estados miembros para trabajar unidos y mantener una estrategia común y adaptada a la realidad de la amenaza.

[322] Informe sobre el enfoque integral de la UE y sus implicaciones para la coherencia de la acción exterior de la UE, de 21 de febrero de 2014, de la Comisión de Asuntos Exteriores del Parlamento Europeo. Disponible en: https://www.europarl.europa.eu/doceo/document/A-7-2014-0138_ES.html (26/10/2023).

[323] Este documento puede consultarse en la página del European Union Institute for Security Studies. Disponible en: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Towards_an_EU_Global_Strategy_0_0.pdf (27/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Sobre esta base se presenta en junio de 2016 la Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea (EUGS por sus siglas en inglés)[324] titulada *Una visión común, una actuación conjunta: una Europa más fuerte*. Desde su inicio el documento apuesta por el papel de la Unión como *proveedor mundial de seguridad* haciendo especial referencia a dos ideas que ayudan a entender, de manera realista, las auténticas posibilidades de la PESC: primeramente, el *carácter global* de esta EUGS, que va más allá del sentido geográfico del término integrando el amplio conjunto de instrumentos y capacidades que articulan el ejercicio del *soft power* y el *hard power* de la Unión y, en segundo lugar, la necesidad de la *autonomía estratégica* como única forma de defender sus principios, valores y prioridades en el actual escenario internacional, altamente cambiante, interdependiente e hiperconectado (DE CARLOS IZQUIERDO, 2016, pág. 15).

La EUGS se estructura en cuatro grandes apartados. El primero, con un alto contenido formal, titulado *Estrategia global para promover los intereses de los ciudadanos*, se centra en el multilateralismo y los valores que representa la Unión -paz y seguridad, prosperidad, democracia, orden mundial basado en normas- y cómo su defensa está íntimamente vinculada a nuestro propio beneficio, por cuanto:

> "Our interests and values go hand in hand. We have an interest in promoting our values in the world. At the same time, our fundamental values are embedded in our interests. Peace and security, prosperity, democracy and a rules-based global order are the vital interests underpinning our external action"[325].

Este enunciado lato de valores es adecuado, e incluso necesario, para interpretar el desarrollo posterior de medidas y líneas de actuación, toda vez que otorga contexto a la manera en que se concibe la PESC y condiciona su aplicabilidad.

En segundo lugar, desde el enfoque pragmático como común denominador, se enuncian los cuatro *principios rectores de nuestra acción exterior*: la unidad de intereses entre la Unión y los Estados miembros, la interacción de esferas de actuación característica de la globalización, la responsabilidad internacional que asume la Unión como proveedor de seguridad y la corresponsabilidad que comparte con sus socios.

El tercer y más extenso epígrafe define las *prioridades de la acción exterior* y constituye la columna vertebral para la consecución de los fines señalados que, lógicamente, se complementan entre sí. La primera es la *seguridad de la Unión* frente a las amenazas identificadas y para las que propone cinco líneas de actuación por sectores: seguridad y defensa, lucha contra el terrorismo, ciberseguridad, seguridad energética y comunicación estratégica. Este marco de seguridad común se construye sobre la *cláusula de asistencia mutua* en caso de agresión a cualquiera de los socios, la necesidad

[324] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union´s Foreign And Security Policy. Junio 2016. Disponible en: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (29/10/2023.)

[325] IBIDEM, página 13.

"Nuestros intereses y valores van de la mano. Tenemos interés en promover nuestros valores en el mundo. Al mismo tiempo, nuestros valores fundamentales están integrados en nuestros intereses. La paz y la seguridad, la prosperidad, la democracia y un orden global basado en reglas son los intereses vitales que sustentan nuestra acción exterior" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de que la Unión asuma un verdadero compromiso con su propia defensa[326], la cooperación de la comunidad de inteligencia en la lucha contraterrorista, el refuerzo de las capacidades tecnológicas y de explotación de la información en el ámbito de la ciberseguridad y, de manera novedosa, el *posicionamiento común frente a la desinformación y la injerencia extranjera*. El siguiente foco de atención se fija allende las fronteras de la Unión por cuanto cualquier acontecimiento fuera de ellas puede afectar a la seguridad interior, siendo para ello prioritaria la resiliencia de nuestros vecinos y de las regiones circundantes así como la reinterpretación de los flujos migratorios desde una perspectiva más amplia, humanitaria e integradora que coadyuve a un enfoque multilateral e integrado para abordar los actuales conflictos de naturaleza multidimensional, manejando conceptos como *seguridad humana*, prevención a favor de la paz, compromiso a medio y largo plazo en las crisis, gobernanza inclusiva e inversión económica en desarrollo, puesto que sin desarrollo no hay paz y sin paz no hay desarrollo. Para articular esta respuesta la Unión debe priorizar los espacios de cooperación a los que debe atender con la idea, no tanto de exportar su modelo, sino de potenciar sus propias dinámicas para encontrar aliados de distinto carácter -estratégicos, económicos, políticos, de desarrollo- con los que construir espacios de gobernanza y de seguridad, que permitan hacer realidad el compromiso de la UE con un orden mundial basado en el Derecho Internacional y unas NNUU fuertes sobre las que construir el orden internacional que vele por la paz, los derechos humanos, el desarrollo sostenible y el patrimonio natural de la humanidad.

La EUGS concluye alentando el movimiento *desde la visión a la acción* mediante tres propuestas. La primera, un posicionamiento de realidad en el que se aboga por una Unión creíble sustentada[327]:

> "[…] on our unity, on our many achievements, our enduring power of attraction, the effectiveness and consistency of our policies, and adherence to our values. A stronger Union requires investing in all dimensions of foreign policy, from research and climate to infrastructure and mobility, from trade and sanctions to diplomacy and development.
> In In this fragile world, soft power is not enough: we must enhance our credibility in security and defence"[328].

[326] Este compromiso de la Unión con su propia defensa se traduce en presupuesto dedicado a la adquisición de tecnología y el desarrollo de capacidades industriales y de innovación, mejorar la formación y la interoperabilidad de los equipos y las fuerzas, y avanzar en la organización, eficacia y eficiencia de las estructuras de combate para, por un lado, contribuir a la defensa conjunta en el marco de cooperación transatlántico y, por otro, para poder actuar de manera autónoma en caso de que sea necesario para preservar los intereses de la UE, única forma de consolidarse como "comunidad de seguridad", aprovechando para ello el potencial de la EDA.

[327] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union´s Foreign And Security Policy. Junio 2016. Página 44. Disponible en: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (02/11/2023).

[328] "En nuestra unidad, nuestros numerosos logros, nuestro atractivo perdurable, la eficacia y la coherencia de nuestras políticas y la adhesión a nuestros valores. Una Unión más fuerte requiere invertir en todas las dimensiones de la política exterior, desde la investigación y el clima hasta las infraestructuras y la movilidad, desde el comercio y las sanciones hasta la diplomacia y el desarrollo. En este mundo frágil, el soft power no es suficiente: debemos mejorar nuestra credibilidad en seguridad y defensa" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

La segunda propuesta es la de una Unión con capacidad de respuesta rápida y flexible frente a las amenazas y, la tercera, una UE integrada en la que se vinculen los ámbitos de Defensa -con la industria y el sector espacial como prioridades- y de Seguridad -a través de la cooperación policial, judicial y de la comunidad de inteligencia-.

Uno de los mensajes finales de la EUGS recoge el espíritu que sustancia la perspectiva que trata de dar a la PESC y resume perfectamente la idea principal: no basta con pretender ser un actor internacional, hay que *actuar* para dar credibilidad a nuestra voluntad. Por esta razón[329]:

> "This Strategy is underpinned by the vision of, and ambition for, a stronger Union, willing and able to make a positive difference to its citizens and in the world. We must now swiftly translate this into action"[330].

Llegados a este punto debe señalarse que son mayoría los analistas especializados que entienden que el momento en que se presenta la EUGS es el menos idóneo por el contexto de terrorismo, de crisis económica y debilidad política interna que sufre Europa y que, al igual que su antecesora, no va más allá en sus medidas "de las propuestas bien intencionadas de siempre: colaborar más, coordinarse mejor, mejorar las capacidades… (mejor Europa) pero ninguna instrucción para superar los problemas estructurales de fondo (más Europa)", lo que puede condenarla a la irrelevancia, máxime cuando se esperaba que la EUGS diera un impulso definitivo a la PCSD (ARTEAGA MARTÍN, 2016). No obstante, a nuestro entender, debe valorarse la referencia a la *acción común* que se reclama frente a la amenaza desinformativa y la injerencia extranjera que, ya entonces, comienzan a manifestarse sobre la Unión y sus EEMM.

En cualquier caso, en 2019 se edita un documento titulado *Estrategia Global de la Unión Europea: tres años después, mirando al futuro*[331] en el que se hace autocrítica sobre el estado de avance y aplicación de sus objetivos, y que puede sintetizarse en uno de los párrafos que conforman el prólogo de la AR/VP Federica Mogherini[332]:

> "The Global Strategy laid out a vision for Europe's place in the world, but it also and essentially promoted greater coherence in our Union's external action. We advocated the need to be more 'joined-up', not just as a way to move towards an ever closer Union, but primarily to make our action more effective and incisive"[333].

---

[329] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union´s Foreign And Security Policy. Op. Cit., página 51.

[330] "Esta estrategia se basa en la visión y ambición de una Unión más fuerte, deseosa y capaz de marcar una diferencia positiva respecto a sus ciudadanos y el mundo. Tenemos que traducir esto rápidamente en acción".

[331] The European Union´s Global Strategy. Three years on, looking forward. Disponible en: https://www.eeas.europa.eu/sites/default/files/eu_global_strategy_2019.pdf (26/10/2023).

[332] IBIDEM, página 5.

[333] "La Estrategia Global estableció una visión del lugar a ocupar por Europa en el mundo, pero también promovió una mayor coherencia en la acción exterior de la Unión. Defendimos la necesidad de estar más "unidos", no sólo como una forma de avanzar hacia una Unión cada vez más estrecha, sino principalmente para hacer que nuestra acción sea más eficaz e incisiva" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

De nuevo la referencia explícita a la *unidad* como clave para encontrar el sitio deseado en el escenario internacional, lo que hace presuponer que ésta sigue siendo la gran tarea pendiente de la gestión europea.

3.2.3. Reflexiones sobre la Política Exterior y de Seguridad Común: ¿cómo construir la imagen de una Unión creíble y cómo afecta a su seguridad?

De lo expuesto hasta el momento cabe subrayar que el diseño, la actualización e implementación coherente de la PESC no dejará nunca de ser una de las tareas más complicadas para la Unión. Este pilar no sólo es primordial para un buen gobierno de la UE desde el punto de vista *ad intra*, sino que también responde, en un enfoque claramente *ad extra*, a su anhelado posicionamiento como actor relevante en el orden y la seguridad internacional.

La dificultad advertida referente al rígido modelo de toma de decisiones no ayuda a la simplificación de dicha tarea, antes al contrario, supone un obstáculo que se empieza ya a cuestionar seriamente por sus consecuencias en la adopción de políticas estratégicas para la acción común, como por ejemplo el nuevo pacto sobre Migración y Asilo, que acomete una reforma integral de la política migratoria de la Unión en base a la denominada regla de la *solidaridad obligatoria*, que debe garantizar un sistema de corresponsabilidad de los veintisiete para la gestión y acogida de los migrantes y solicitantes de asilo, cuya puesta de largo, que se suponía iba a ser en la Cumbre Informal de la UE celebrada en octubre de 2023 en Granada[334] como respuesta a las cercanas crisis humanitarias de las islas de Lampedusa[335] y Canarias[336], no puede celebrarse con una declaración conjunta que establezca dicho acuerdo por el bloqueo de Hungría y Polonia que, una vez más, ralentizan la práctica decisora de la PESC. El Consejo y el Parlamento Europeo alcanzan un acuerdo finalmente el 20 de diciembre de 2023, tras intensas negociaciones que flexibilizan las normas de reparto de cuotas entre los EEMM[337].

Tampoco ayudan los movimientos unilaterales de política exterior de los EEMM que, aun siendo legítimos, confrontan abiertamente con la postura oficial de la Unión,

[334] Puede verse la repercusión en medios de prensa. Disponible en: https://es.euronews.com/my-europe/2023/10/06/hungria-y-polonia-bloquean-de-nuevo-una-declaracion-conjunta-de-la-ue-sobre-migracion (26/10/2023).

[335] Disponible en: https://es.euronews.com/2023/09/17/crisis-migratoria-ursula-von-der-leyen-y-giorgia-meloni-aterrizan-en-lampedusa (27/10/2023).

[336] Sobre la crisis canaria puede verse reperecusiñon en prensa. Disponible en: https://www.ondacero.es/emisoras/canarias/noticias/8-dias-octubre-llegan-4300-migrantes-canarias-media-520-dia_20231009652399dbe0d76200011f5ac5.html (27/10/2023).

[337] Finalmente se acuerdan cinco Reglamentos vinculados entre sí que, de cara a los EEMM flexibilizan el reparto obligatorio de cuotas estableciendo una penalización de 20.000 € por persona rechazada, pero que en definitiva endurecen el acceso a quienes traten de acceder de manera irregular a territorio de la UE. Puede verse la trascendencia en prensa. Disponible en: https://www.consilium.europa.eu/es/policies/eu-migration-policy/eu-migration-asylum-reform-pact/ https://spanish-presidency.consilium.europa.eu/es/programa/pacto-migratorio-presidencia-espanola-consejo-ue/ https://elpais.com/internacional/2023-12-20/la-ue-cierra-el-pacto-migratorio-tras-anos-de-negociacion-y-con-un-endurecimiento-de-los-requisitos-de-acogida.html (21/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

resquebrajando su pretendida acción común ante el resto de actores internacionales, situación que se vuelve a producir en octubre de 2023, de nuevo protagonizada por el verso suelto de la UE que representa Hungría, esta vez con ocasión de la celebración en Pekín del 10º aniversario de la Nueva Ruta de la Seda, donde su presidente Viktor Orban se reúne con Vladimir Putin para manifestarle que su país no busca el enfrentamiento con el Kremlin sino todo lo contrario, ampliar los contactos mutuos que se han visto perjudicados por las sanciones impuestas por Bruselas a Rusia[338].

Otro factor limitativo es la búsqueda de equilibrio y cohesión entre los intereses de la Unión y los intereses de política exterior e interior de cada uno de los EEMM. Fenómenos como la polarización social y el resentimiento ante lo *diferente*, la consiguiente radicalización en la política alimentada por la exacerbación de los nacionalismos, la concatenación de crisis económicas y financieras que castigan a amplios sectores de población en todo el mundo y que obligan a apostar por partidas presupuestarias que adelgazan la inversión en otras carteras más enfocadas al unionismo -defensa, industria o innovación-, y el taimado recurso a postulados autárquicos con interés manipulador y desinformativo que cuestiona la política dictada desde Bruselas para alcanzar metas partidistas a corto plazo, entre otros, conllevan la desafección al orden y a los valores de Europa y, al mismo tiempo, complican la gestión común que presupone la PESC.

Otro factor a tener en cuenta es la inestabilidad política en nuestras áreas de cooperación e influencia, como África y Oriente Próximo. De la inestabilidad en el Sahel es claro ejemplo la convulsa situación que en julio de 2023 vive Níger[339], considerado el socio más fiable de la UE en la zona, que avanza hacia la consolidación de un gobierno controlado por una junta militar, al igual que Mali o Burkina Faso, apoyados directa o indirectamente por Rusia, que muestra sus intereses geoestratégicos en África a través del despliegue de los mercenarios de Wagner con el objetivo de reforzar sus vínculos en la zona y "mostrar que está menos aislada de lo que parece" (FUENTE COBO, 2023, pág. 7). La desestabilización del Sahel es un factor de riesgo para el aumento de la amenaza terrorista yihadista y del crimen organizado especializado en la trata de seres humanos y la canalización de flujos migratorios hacia las fronteras del sur de Europa.

En cuanto a Oriente Próximo, el delicado equilibrio mantenido en los últimos años salta por los aires el 7 de octubre de 2023 con el ataque del movimiento islamista palestino Hamás a Israel desde la Franja de Gaza[340], un día después del 50 aniversario del ataque sorpresa de Egipto y Siria contra Israel en 1973, inicio de la Guerra de Yom Kipur. La sangrienta embestida de Hamás con cohetes, toma de rehenes e incursiones armadas en territorio israelí abre un abanico de graves consecuencias humanas, políticas, económicas y militares que se alimenta de narrativas como las del primer ministro israelí Benjamin Netanyahu cuando declara que "lo que hagamos a nuestros enemigos en los

[338] Disponible en: https://elpais.com/internacional/2023-10-17/viktor-orban-desafia-la-postura-europea-al-convertirse-en-el-primer-lider-europeo-que-se-reune-con-putin-en-los-ultimos-meses.html#?rel=lom (27/10/2023).
[339] Sobre este golpe de Estado elabora nota de prensa el DSN el 8 de agosto de 2023. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/situaci%C3%B3n-n%C3%ADger-tras-golpe-estado (27/10/2023).
[340] Disponible en: https://www.bbc.com/mundo/articles/cqlwz3yjyeeo (29/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

próximos días resonará en ellos durante generaciones"[341], anticipando los bombardeos intensivos en la Franja de Gaza que se producen los días siguientes en respuesta a la ofensiva de Hamás y que deviene en atentados en otras partes del mundo[342], cuestión que eleva aún más la escalada de tensión[343] e incrementa las posibilidades de que el conflicto palestino-israelí se contagie a otros países del entorno con predominancia de población musulmana[344]. El posicionamiento de los principales actores internacionales es instantáneo -EE.UU. con Israel, China con Palestina- y en la región es Egipto quien se postula como mediador en el conflicto abalado por sus fuertes vínculos e influencia, tanto con Israel como con Palestina, tal y como ocurrió en las últimas crisis en la Franja

[341] Cobertura mediática del ataque. Disponible en: https://cnnespanol.cnn.com/2023/10/10/analisis-guerra-israel-Hamás-conmociones-politicas-planeta-trax/ (29/10/2023).

[342] El viernes 13 de octubre de 2023, en la localidad de Arras (Francia), es asesinado un profesor y tres personas más resultan heridas graves en un ataque terrorista a un instituto de enseñanza media, perpetrado por un hombre de 20 años de edad nacido en Ingusetia, república de la Federación Rusa, próxima a Chechenia y de mayoría musulmana. Ese mismo día, en Pekín (China), un diplomático israelí es apuñalado en la calle, en un céntrico barrio de la capital china. Disponible en: https://elpais.com/internacional/2023-10-13/un-profesor-muere-apunalado-en-un-instituto-del-norte-de-francia-y-dos-personas-resultan-heridas-graves.html?outputType=amp https://www.abc.es/internacional/apunalado-empleado-embajada-israeli-pekin-20231013130138-nt_amp.html (29/10/2023).

[343] El Gobierno francés, a raíz del atentado de Arras, eleva al máximo el nivel de alerta antiterrorista de su plan Vigipirate, denominado "emergencia por atentado". A partir de este nivel de alerta, el 14 de octubre se llevan a cabo evacuaciones preventivas por amenaza de bomba en edificios singulares en París y otras zonas del país, como el Museo del Louvre, la Estación parisiense de Lyon y el Palacio de Versalles, entre otros.

[344] Nos referimos a países como Afganistán, Tayikistán, Kirguistán, Azerbaiyán, Uzbekistán o Irán, tradicional aliado de Hamás. Finalmente, respondiendo a las amenazas y declaraciones del líder supremo de Irán, Alí Jamenei, en su discurso televisado con motivo del Aíd al Titr que marca el fin del Ramadán, ocurre lo esperado y, en la noche del 13 al 14 de abril de 2024, Irán lanza más de 300 drones, misiles balísticos y de crucero contra Israel, en una acción reivindicada como respuesta al ataque contra su consulado en Damasco el 1 de abril, atribuido a Tel Aviv, y que acabó con la vida de siete altos mandos militares de la Guardia Revolucionaria iraní, entre ellos el general Mohammad Reza Zahedi, pieza esencial en las relaciones con Hezbolá, aliada de Hamás. El escudo antimisiles israelí -Domo de Hierro- consigue hacer fracasar el ataque iraní pero, a la vez, da pie a Israel para responder de manera directa o a través de proxies, cómo y cuándo decida, haciendo que la escalada del conflicto sea ya una realidad patente y poniendo encima del tablero de juego oriental el estallido, o no, de una nueva guerra que involucraría de manera directa a Irán, es decir, a otro miembro del bloque que aspira a destronar a EE.UU. y a sus socios occidentales como potencia hegemónica global. Esta respuesta se materializa en la madrugada del 19 de abril, cuando Israel bombardea una base aérea iraní en la provincia de Isfahán, centro de investigación y entrenamiento de su programa nuclear. Disponible en: https://elpais.com/internacional/2024-04-14/cronica-de-un-ataque-anunciado.html https://www.bbc.com/mundo/articles/cyj3nk8zv0lo https://www.europapress.es/internacional/noticia-guerra-iran-israel-directo-ultimas-noticias-conflicto-iran-israel-20240414083449.html https://www.rtve.es/noticias/20240417/netanyahu-ante-llamadas-moderacion-occidente-respuesta-iran-israel-reserva-derecho-protegerse/16065174.shtml https://www.elcorreo.com/internacional/netanyahu-desoye-todas-llamadas-6254831380001-20210518191512-vi.html?ref=https%3A%2F%2Fwww.elcorreo.com%2Finternacional%2Fnetanyahu-desoye-todas-llamadas-6254831380001-20210518191512-vi.html https://www.bbc.com/mundo/articles/c1ejq8lyj2lo https://elpais.com/internacional/2024-04-19/conflicto-israel-iran-y-guerra-en-gaza-en-directo.html (19/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de Gaza en agosto de 2022 y en mayo de 2023, donde el papel del gobierno egipcio resultó crucial.

Mientras tanto, las diferencias en el seno de la Unión salen de nuevo a la superficie a raíz de la condena que la Comisión hace un día después de los ataques terroristas de Hamás avisando que suspendería todos los pagos a las autoridades palestinas, lo que le obliga a una rectificación precisando que llevaría a cabo una revisión urgente de los fondos de ayuda europeos a Palestina[345]. Días después el desencuentro se reproduce por unas declaraciones de Úrsula von der Leyen que, como Presidenta de la Comisión, no le corresponde hacer y que no recogen la postura oficial de Bruselas[346], trasluciendo nuevamente una postura errática de la Unión. A ello se suma que, en el mismo mes de octubre, el día 26, la Asamblea General de las Naciones Unidas adopta una resolución no vinculante[347] para pedir una pausa humanitaria en la Franja de Gaza que conduzca a un cese en la escalada de las hostilidades, que tampoco obtiene una postura única de la Unión por cuanto 8 de sus miembros votan a favor frente a 4 votos en contra y 15 abstenciones[348], mientras en Bruselas el Presidente del Consejo de la UE insiste en la necesidad de un alto el fuego y de que se respete el Derecho Internacional ante el número de bajas civiles causadas por ambos bandos. Es esta una evidencia más de la libertad de los EEMM para llevar a cabo su propia política exterior, a pesar de los esfuerzos de la PESC para conseguir una postura única común que proyecte una imagen de identidad de la Unión, pero ésta solo se puede crear desde "dentro, es decir, desarrollando una verdadera y efectiva política exterior europea. Hasta que ello no se consiga, no creemos que la UE proyecte, haga lo que haga, una imagen monolítica en el mundo. Y quizás, este objetivo no se consiga nunca" (REAL, 2011, pág. 571).

En este mismo sentido, la guerra provocada por la invasión rusa de Ucrania ha puesto en juego muchas fichas de alto valor que obligan a posicionarse a todos y cada uno de los socios de la Unión, tanto en su estrategia de grupo como en la individual, frente a la apuesta retadora de la dependencia energética europea, el alineamiento estratégico

[345] De conformidad con la Posición Común del Consejo de 27 de diciembre de 2001 sobre la aplicación de medidas específicas para luchar contra el terrorismo, que es actualizada en julio de 2023, Hamás y su brazo militar Hamás-Izz al-Din al-Qassem están considerados como grupo terrorista, lo que conlleva la prohibición de facilitarle cualquier tipo de fondos y recursos económicos. Sin embargo, la decisión de proceder a la detención de sus integrantes o impedir las muestras de apoyo a Hamás en territorio de los EEMM sigue siendo competencia de la legislación nacional respectiva de cada uno de ellos. Disponible en: https://es.euronews.com/my-europe/2023/10/09/la-ue-suspende-inmediatamente-todos-los-pagos-a-las-autoridades-palestinas (29/10/2023).

[346] La posición oficial de la UE en política exterior se determina en el Consejo de la UE y en el Consejo de Asuntos Exteriores, no en la Comisión. Disponible en: https://elpais.com/internacional/2023-10-14/von-der-leyen-matiza-su-discurso-tras-las-criticas-e-insta-a-israel-a-que-respete-el-derecho-internacional.html (29/10/2023).

[347] El proyecto de Resolución 23-20614 (S) A/ES-10/L.25 para la protección de los civiles y cumplimiento de las obligaciones jurídicas y humanitarias ante las medidas ilegales israelíes en la Jerusalén Oriental Ocupada y el resto del territorio Palestino Ocupado, fue adoptada con 120 votos a favor, 14 en contra y 45 abstenciones. Puede consultarse la nota de prensa de ONU. Disponible en: https://news.un.org/en/story/2023/10/1142932 (29/10/2023).

[348] A favor votan Bélgica, España, Francia, Irlanda, Luxemburgo, Malta, Eslovenia y Portugal, en contra votan República Checa, Croacia, Austria y Hungría, y se abstienen el resto de EEMM. Puede consultarse el panel de votación. Disponible en: https://twitter.com/UN_News_Centre/status/1717992371906839005/photo/2 (29/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

con la OTAN, el apoyo militar a Ucrania como país vecino prioritario para la seguridad de la UE, el bloqueo económico y comercial a Rusia o las restricciones comerciales y a la exportación, entre otras. El compromiso para el mantenimiento a medio y largo plazo de estas medidas supone un desgaste interno para la UE y una auténtica prueba de esfuerzo para la PESC, por cuanto exige de unidad y coherencia, vinculación entre políticas y gestión de la respuesta estratégica común. Debemos avanzar juntos para ser creíbles en nuestra disuasión y mantener nuestro esfuerzo de apoyo a Ucrania, donde se juega la seguridad de todos los europeos, máxime si EE.UU. llega a plantearse su posición en el conflicto y decide desvincularse de la carga financiera que conlleva el suministro de material y armas, que harían balancear el delicado equilibrio entre los contendientes.

Por ello, si el objetivo verdadero es una Unión creíble e integrada, con capacidad de respuesta, solo hay un camino a recorrer y pasa necesariamente por la consabida *autonomía estratégica* como forma de aunar intereses, instrumentos y políticas, especialmente cuando se vive una situación tan compleja como la que actualmente constriñe a Europa. "No hacerlo resultará invariablemente en un grave debilitamiento de la influencia internacional y, en última instancia, de la seguridad de los Estados miembros de la UE" (ALCARO, 2021). Este y no otro parece ser el camino. Cuestión diferente será la facilidad para recorrerlo, sobre todo mientras las capacidades y la decisión final del recurso a la fuerza siga recayendo en los EEMM en vez de en la Unión como entidad jurídica propia.

En esta línea de pensamiento, el Presidente francés Emmanuel Macron reclama, en su discurso de La Sorbona del 25 de abril de 2024[349], una mayor soberanía tecnológica e industrial sobre la que construir la unidad estratégica europea que ponga fin a nuestra dependencia en sectores clave para, de esta manera, "no ser superados por la Historia" y quedar relegados al papel de meros observadores de la lucha hegemónica sino-estadounidense, a la que se tratan de sumar otras potencias regionales y revisionistas como Rusia o Irán.

3.3. La Política Común de Seguridad y Defensa: la determinación de Europa por alcanzar su propia alianza militar

La recuperación de Europa tras la Segunda Guerra Mundial pasa necesariamente por conjurar el fantasma de una nueva confrontación en suelo continental, para lo que Francia y Reino Unido se alían mediante el Tratado de Dunquerque[350] con el objetivo de contrarrestar al enemigo común que, en ese momento, representa para ambos Alemania. Justo un año después, en marzo de 1948, estos dos países junto con Bélgica, Países Bajos y Luxemburgo acuerdan en el Tratado de Bruselas[351] un marco de

[349] Disponible en: https://legrandcontinent.eu/es/2024/04/25/construir-un-nuevo-paradigma-el-discurso-completo-de-emmanuel-macron-en-la-sorbona/ (26/04/2024).

[350] Tratado de Alianza y Asistencia Mutua, entre Gran Bretaña y Francia, firmado el 4 de marzo de 1947 en Dunquerque.

[351] Tratado de colaboración en materia económica, social y cultural y de legítima defensa colectiva, firmado en Bruselas el 17 de marzo de 1948, enmendado por el Protocolo por el que se modifica y completa el Tratado de Bruselas, firmado en París el 23 de octubre de 1954. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

cooperación económica, social, cultural y, principalmente, de defensa conjunta ante, esta vez sí, la identificación de la URSS como nueva amenaza compartida y con más probabilidad de materializarse, por delante incluso de un posible resurgimiento alemán. Se crea de esta manera la Unión Occidental (UO) con la voluntad de hacer realidad una alianza militar defensiva de los países de Europa occidental al margen de los EE.UU.

En abril de 1949 se firma el Tratado de Washington siendo que, de los doce miembros que conforman inicialmente la Alianza del Atlántico Norte, cinco de ellos son los integrantes de la UO, los cuales ya están comprometidos con su defensa mutua por el artículo VIII del Tratado de Bruselas[352], que expresamente recoge la apertura de consultas a petición de cualquiera de sus miembros sobre aquellas situaciones que pudieran constituir una amenaza para la paz o la estabilidad económica de éstos, en cualquier ámbito en que surja esta amenaza. Esta cuestión viene a confirmar el hecho de que "a mediados del siglo XX, con la segunda guerra mundial recién terminada y aun no cicatrizada, antes de que la Europa económica y política haya echado a andar, el flanco defensivo avanza a buena velocidad, no solo en su dimensión transatlántica sino en la estrictamente continental" (FUENTES MONZONÍS-VILLALONGA, 2011, pág. 3). No obstante, hay que decir que el espíritu que da aliento a los cinco firmantes del Tratado de Bruselas flaquea ante la evidencia de la supremacía armamentística y el poderío militar americano, lo que les lleva a reconsiderar la situación dando lugar a una resolución del Consejo de la Unión Occidental de 20 de diciembre de 1950 en la que deja claro que delega "todas sus competencias en materia de seguridad y defensa en la OTAN" (BAQUÉS QUESADA, 2023, pág. 93). Esta decisión de *ir a lo fácil* y resguardarse bajo el escudo noratlántico será determinante a largo plazo, hasta el extremo de seguir condicionando a día de hoy la política de defensa de la Unión.

Posteriormente, los países firmantes de la CECA[353], entre los que se encuentran Italia y la República Federal de Alemania, hacen un nuevo intento por construir una alianza militar sustentada por un ejército europeo al margen de los EE.UU., e inician en mayo de 1952 el proyecto de la Comunidad Europea de Defensa (CED) que se frustra sin llegar a entrar en vigor por la falta de consenso en la Asamblea Nacional francesa. Los

https://www.dipublico.org/121077/tratado-de-colaboracion-en-materia-economica-social-y-cultural-y-de-legitima-defensa-colectiva-firmado-en-bruselas-el-17-de-marzo-de-1948-y-enmendado-por-el-protocolo-que-modifica-y-completa-el-trat-2/ (29/10(2023).

[352] El artículo VIII punto 3 del Tratado de Bruselas firmado el 17 de marzo de 1948 señala que: "At the request of any of the High Contracting Parties the Council shall be immediately convened in order to permit Them to consult with regard to any situation which may constitute a threat to peace, in whatever area this threat should arise, or a danger to economic stability" (A petición de cualquiera de las Altas Partes Contratantes, se convocará inmediatamente el Consejo para permitirles consultarse sobre cualquier situación que pueda constituir una amenaza a la paz, en cualquier zona en que se presente esa amenaza, o un peligro a la estabilidad económica). Traducción propia.

Es importante señalar que esta amenaza para la paz o la estabilidad económica de las partes contratantes no está sujeta a ningún condicionante territorial, por lo que cabría entender que pudiera producirse tanto dentro como fuera de su propio territorio, con las derivadas estratégicas que ello conlleva. El Tratado de Bruselas va en este sentido más allá incluso que el artículo 5 del Tratado de Washington que, expresamente, establece que el ataque armado contra los aliados debe producirse en la zona del Atlántico Norte, es decir, en Europa o América del Norte.

[353] Los integrantes de la Comunidad Europea del Carbón y del Acero (CECA) eran Francia, la República Federal de Alemania, Italia, Bélgica, Países Bajos y Luxemburgo.

Ediciones Universidad de Salamanca | CC BY-NC-ND

británicos desde el primer momento se desvinculan de esta iniciativa, dejando clara su elección a favor de la OTAN.

3.3.1. La relación OTAN - UE: el Caballo de Troya

Son muchos los autores que han reflexionado sobre las posturas y las discrepancias que, desde el comienzo, se han sostenido a ambos lados del Atlántico en relación con el proyecto de construcción de una defensa europea autónoma, pareciendo todos ellos coincidir en que:

> "[…] aunque la defensa europea nunca se planteó como una alternativa a la OTAN –y por lo tanto a la presencia norteamericana en el continente- lo cierto es que Washington y sus más fieles aliados en Europa, nunca quisieron apoyar una iniciativa militar europea que pudiera poner en entredicho la acción en Europa de la Alianza Atlántica" (FUENTES MONZONÍS-VILLALONGA, 2011, pág. 4).

Insistiendo en la idea de conseguir una defensa europea autónoma, en octubre de 1954 se firman en París los Protocolos al Tratado de Bruselas permitiendo que se sumen a los cinco miembros iniciales la República Federal de Alemania[354] e Italia, dando lugar a la Unión Europea Occidental (UEO) que, a pesar de contar con la cláusula de defensa mutua similar a la del Tratado de Washington, nace lastrada por la delegación de competencias a la OTAN que hizo ya la Unión Occidental y que, abundando en la cuestión, ratifica el propio Consejo de la UEO en otra resolución de 27 de febrero de 1957 (BAQUÉS QUESADA, 2023, págs. 92-93).

Con la reunificación de Alemania y la consiguiente desaparición de la URSS deviene un nuevo orden internacional en el que busca su acomodo el proyecto de seguridad europeo. Este proyecto se define en el Tratado de Maastricht de 1992 que, por un lado, sienta las bases para una futura defensa común que permita una capacidad autónoma de gestión de crisis y, por otro, encarga a la UEO la ejecución de las decisiones de la Unión con repercusiones en el ámbito de la defensa.

Hemos de tener en cuenta que este modelo se diseña con el conflicto de los Balcanes occidentales ardiendo en el patio trasero de la Unión que, evidenciando su incapacidad para intervenir, da paso a una operación militar coordinada de la OTAN y las fuerzas de Naciones Unidas UNPROFOR[355] para poner fin al conflicto y negociar los Acuerdos de Dayton (MORA BENAVENTE, 2017, pág. 125).

Al mismo tiempo, el liderazgo en solitario que ejerce EE.UU. en el mundo a finales del siglo XX le obliga a reconsiderar sus objetivos estratégicos, concluyendo que el mantenimiento en las siguientes décadas de su hegemonía como única superpotencia pasa por disminuir su compromiso con Europa y, además, que ésta asuma parte de la responsabilidad y de las cargas derivadas de su defensa a través de la UEO. Con esta

[354] La República Federal de Alemania aceptó a cambio de ingresar en la OTAN y en la UEO una serie de condiciones, entre las que se encontraban la prohibición de fabricar armas nucleares y la autorización al establecimiento de fuerzas aliadas en su territorio, entre otras.
[355] La Operación Fuerza Deliberada se llevó a cabo entre el 30 de agosto y el 20 de septiembre de 1995.

Ediciones Universidad de Salamanca | CC BY-NC-ND

idea, en junio de 1996 se firma el Acuerdo de Berlín para tratar de armar un *pilar europeo de la OTAN* que permita a la UEO lanzar, con sus propios medios y el apoyo de las capacidades de planeamiento y militares de la Alianza, operaciones de paz y estabilización de conflictos[356] en los que EE.UU. no quiera intervenir y donde la OTAN como tal no esté comprometida. Es este un modelo de *complementariedad absoluta* que presupone, ingenuamente, que los intereses de Europa y de EE.UU. son -y seguirán siendo- los mismos (MORA BENAVENTE, 2017, pág. 126).

Con todo, el proyecto de defensa común europea no supera el mundo de las ideas y prueba de ello es que en el Tratado de Ámsterdam[357] de 1997 "a lo más que se llegó fue a decir que la UE avanzaría *progresivamente* hacia esa defensa común. De nuevo, prudentemente, sin calendario ni ulteriores aclaraciones. Síntoma inequívoco de que la brecha seguía abierta" (BAQUÉS QUESADA, 2023, pág. 128). Herida que se abre aún más con las guerras de los Balcanes, que "revelaron la incapacidad europea para gestionar crisis de forma autónoma, la brecha militar existente entre los aliados y la dependencia estratégica de Washington" (COLOM PIELLA, MEDINA IBORRA, & PEÑA RAMOS, 2017, pág. 115).

Para saltar definitivamente al mundo de la realidad, en 1998 Francia y el Reino Unido, los dos miembros de la UE con mayor poder de disuasión y defensa, acuerdan en la declaración de Saint Malo[358] cinco puntos estratégicos que ponen sobre la mesa la voluntad de cambiar el enfoque de la defensa europea:

> "The European Union needs to be in a position to play its full role on the international stage. This means making a reality of the Treaty of Amsterdam, which will provide the essential basis for action by the Union […].
> To this end, the Union must have the capacity for autonomous action, backed up by credible military forces, the means to decide to use them, and a readiness to do so, in order to respond to international crises […].
> In order for the European Union to take decisions and approve military action where the Alliance as a whole is not engaged, the Union must be given appropriate structures and a capacity for analysis of situations, sources of intelligence, and a capability for relevant strategic planning, without unnecessary duplication […].
> Europe needs strengthened armed forces that can react rapidly to the new risks, and which are supported by a strong and competitive European defence industry and technology.

[356] El Acuerdo de Berlín de 1996 se firma siendo Secretario General de la OTAN Javier Solana, y configura en el ámbito de actuación de la defensa europea las conocidas como "Misiones Petersberg", de carácter humanitario o de rescate, de mantenimiento de la paz y misiones de gestión de crisis, incluyendo la imposición de la paz con fuerzas de combate.

[357] El Tratado de Ámsterdam señala que la UEO es parte del desarrollo de la Unión y que le proporciona capacidad operativa, por lo que se fomentarán relaciones institucionales más estrechas entre ellas con vistas a la posibilidad de integración de la UEO en la Unión. No obstante, puede decirse que la UEO fue una organización vacía de contenido por la delegación de competencias a la OTAN que hizo desde su origen, cuestión que acaba definiendo su precario balance de resultados tras 57 años de existencia, hasta su completo cese de actividades en junio de 2011.

[358] Declaración de Saint Malo, de 4 de diciembre de 1998. Disponible en: https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf (27/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> We are determined to unite in our efforts to enable the European Union to give concrete expression to these objectives"[359].

Esta declaración es un paso firme y decidido, de hecho el primero, que vindica la voluntad europea de consolidarse como actor internacional de relevancia y marca el inicio de la Política Europea de Seguridad y Defensa (PESD) que, tímidamente, se enunciaba dentro del segundo pilar del Tratado de Maastricht como una hipótesis futurible. Esta declaración es interpretada al otro lado del Atlántico como un claro desafío a los intereses aliados y supone la gota que colma el vaso. La reacción estadounidense es inmediata y toma cuerpo en la *doctrina Albright* -la teoría de las tres "*des": de-linking*, *duplicating* y *discriminating*[360]- que establece los límites operativos de las capacidades de defensa europea: no *desvincular* la seguridad de EE.UU. y de la UE, no *duplicar* las capacidades y los recursos dentro de la estructura de la OTAN, y no *discriminar* a los aliados en el proceso de toma de decisiones de la defensa europea (MORA BENAVENTE, 2017, pág. 129). Este es el caballo de Troya que EE.UU. regala a Europa, el modelo *everything with NATO* que se apoya íntegramente en la superioridad militar y nuclear norteamericana bajo cuya égida se siente cómoda y protegida la Unión, lo que alimenta la displicencia de sus miembros que, sintiéndose suficientemente arropados, son renuentes a *gastar* en un proyecto de defensa europeo de cuya bondad y éxito desconfían toda vez que, de la mano estadounidense, ya tienen cobertura de seguridad.

A pesar de ello, el Consejo Europeo de Helsinki de junio de 1999 avanza en la línea de cooperación atlántica y define unos objetivos operativos, los *Helsinki Headlines Goals*[361], para cuya ejecución práctica crea una estructura de Comités[362], aunque la realidad es

[359] 1. "La Unión Europea debe estar en condiciones de desempeñar su papel en el escenario internacional. Esto implica hacer realidad el Tratado de Ámsterdam, que constituirá la base esencial para la acción de la Unión".
2. "Para ello, la Unión debe tener capacidad de acción autónoma, respaldada por fuerzas militares creíbles, medios para poder decidir utilizarlas y estar dispuestos a hacerlo, para responder a las crisis internacionales".
3. "Para que la Unión Europea pueda tomar decisiones y aprobar acciones militares cuando la Alianza en su conjunto no esté comprometida, es necesario dotar a la Unión de estructuras apropiadas y de la capacidad de análisis de situaciones, fuentes de inteligencia y la capacidad para la planificación estratégica pertinente, sin duplicaciones innecesarias".
4. "Europa necesita Fuerzas Armadas fortalecidas que puedan reaccionar rápidamente a los nuevos riesgos y que estén respaldadas por una industria y una tecnología de defensa europeas fuertes y competitivas".
5. "Estamos decididos a unir nuestros esfuerzos para permitir que la Unión Europea dé expresión concreta a estos objetivos" (Traducción propia).

[360] Las tres *des* hacen referencia a los términos en inglés desvinculación (*de-linking*), duplicar (*duplicating*) y discriminación (*discriminating*).

[361] Se aprueba el catálogo de fuerzas por el que la UE debe ser capaz de desplegar 60.000 efectivos, en un plazo máximo de 30 días y mantenerlos desplegados 1 año, manteniendo el ámbito de actuación marcado por las Misiones Petersberg.

[362] Estos son el *Comité Político y de Seguridad*, integrado por embajadores de los EEMM, encargados de la dirección estratégica y la supervisión de la política de seguridad y defensa aplicada a las operaciones; el *Comité Militar*, integrado por los jefes de Estado Mayor de las fuerzas armadas de los EEMM, encargados del asesoramiento militar al anterior y de fijar las directrices militares que debe aplicar el Estado Mayor al conducir las operaciones; y el *Comité de Gestión Civil de Crisis*, compuesto por representantes de los EEMM para el acercamiento global a los conflictos y las crisis.

Ediciones Universidad de Salamanca | CC BY-NC-ND

que la UE sigue dependiendo de las capacidades de la OTAN al no tener capacidad operativa para asumir de manera independiente una operación militar de gestión de crisis (MORA BENAVENTE, 2017, pág. 134).

Este vínculo transatlántico se renueva en la Declaración Conjunta UE-OTAN sobre la Política Europea de Seguridad y Defensa, acordada el 16 de diciembre de 2002, que "significó el apoyo explícito de la Alianza a la PESD y supuso una declaración conjunta sobre su nueva asociación estratégica" (LABORIE IGLESIAS M. , 2010, pág. 3) basada en la indivisibilidad de la seguridad euro atlántica y para cuya materialización se firman los Acuerdos Berlín Plus[363] el 17 de marzo de 2003. Sin embargo, unos días después EE.UU. invade Irak dejando en evidencia, por un lado, su política exterior unilateral y, por otro, la falta de acuerdo interno en la Unión para posicionarse ante este movimiento, entre los que ven la dependencia atlántica como un freno al desarrollo de la defensa europea autónoma y los que, por el contrario, entienden que solo en el marco de la OTAN se cubren sus expectativas de seguridad. En todo caso, queda patente que la relación entre la UE y la OTAN ha sido históricamente complicada, "eso suponiendo que se pueda utilizar el adverbio para una narrativa de apenas 20 años. La dificultad radica, en pocas palabras, en la percepción, en las dos organizaciones, de que la otra trata de hacer cosas que no le corresponden" (MORA BENAVENTE, 2017, pág. 155), cuestión agravada desde que la UE empezó a construir su propia política de seguridad y defensa en aras de una anhelada autonomía estratégica.

En este complejo y tenso marco de relaciones aprueba el Consejo Europeo, en diciembre de 2003, la Estrategia Europea de Seguridad en la que se aboga por asumir más responsabilidad en su propia seguridad, eso sí, dentro de la esfera de complementariedad atlántica y bajo el prisma *NATO-first*, para consolidarse como *comunidad de defensa* y poder actuar de manera autónoma disuadiendo ante posibles amenazas, respondiendo a los conflictos y protegiendo sus intereses, tanto dentro como fuera de sus fronteras. Este concepto de seguridad parte de su interpretación como *un continuo donde es imposible separar el ámbito interior del exterior*, por lo que es necesario que la UE proyecte su acción estabilizadora y pacificadora en su vecindario y en las regiones circundantes a través de un enfoque multilateral, global y efectivo bajo la jurisdicción del Derecho Internacional y la Carta de las NNUU. Sin embargo, como ya se ha analizado anteriormente, la falta de definición de los intereses concretos a proteger, la falta de encaje entre la voluntad de avanzar en la capacidad de defensa autónoma y la limitación operativa que recoge el acuerdo transatlántico Berlín Plus, el carácter descriptivo y meramente doctrinal de las implicaciones estratégicas y, sobre todo, la indefinición respecto a la manera de armonizar la PESC de la UE y la del resto de Estados miembros para ser *más coherentes* y más creíbles en la defensa de nuestros intereses, actúan como fuerte viento en contra que frena el avance de la tan desigualmente anhelada PESD.

[363] Los Acuerdos Berlín Plus recogen cuatro reglas principales: 1) el acceso de la UE a los sistemas de planeamiento aliado; 2) las operaciones UE serán comandadas por un mando militar europeo -DSACEUR-; 3) el uso de recursos y capacidades aliados por la UE; 4) el desarrollo coherente y de refuerzo mutuo de las capacidades OTAN y UE para que puedan actuar de manera conjunta.

Ediciones Universidad de Salamanca | CC BY-NC-ND

3.3.2. El nacimiento en Lisboa de la Política Común de Seguridad y Defensa de la UE

Partiendo del hecho de que "el factor *atlántico* ha sido y sigue siendo una de las cuestiones más divisivas en la formulación de la política exterior comunitaria" que "ha limitado especialmente el desarrollo de una política de defensa europea" (DÍAZ RODRÍGUEZ, 2018, pág. 5), habrá de ser el Tratado de Lisboa -aprobado en 2007 y en vigor desde 2009- el que insufle nueva vida al homúnculo que representa por entonces la *identidad europea de defensa*, comenzando con el cambio de denominación que, a partir de entonces, será de *Política Común de Seguridad y Defensa* (PCSD).

Desde ahora la UE tiene una personalidad jurídica[364] sobre la que poder construir la *identidad de seguridad y defensa* que pretende alcanzar, para cuyo análisis debemos recurrir a las cuatro claves interpretativas que se encuentran en las *Disposiciones sobre la Política Común de Seguridad y Defensa* del mencionado Tratado de la Unión Europea[365].

En primer lugar la *naturaleza* de la PCSD, que entra a formar parte de la PESC ofreciendo una capacidad operativa basada tanto en medios civiles como militares para el desarrollo de misiones fuera de la Unión, asumiendo los EEMM el compromiso de mejorar sus capacidades militares y de ponerlas a disposición para contribuir a la consecución de los objetivos fijados por el Consejo UE[366], en el que tiene que conseguirse la unanimidad para la adopción de las decisiones relativas a la PCSD. No obstante, existen algunas excepciones, como por ejemplo cuando el Consejo adopta medidas que implementan una decisión de la UE o decisiones relacionadas con la Agencia Europea de Defensa (EDA) y la cooperación estructurada permanente (PESCO), cuando las decisiones se toman por mayoría cualificada.

La segunda clave interpretativa del Tratado de Lisboa es el carácter de *alianza defensiva* que adquiere la PCSD mediante la *cláusula de asistencia mutua*, elemento de sustentación de este nuevo enfoque de la defensa europea, donde se integra el factor *territorio* hasta entonces inexistente en el artículo 42.7 TUE[367], por cuanto "si un Estado

[364] El artículo 47 del Tratado de Lisboa establece que "La Unión tiene personalidad jurídica".
[365] Título V, Capítulo 2, Sección 2, artículos 42 a 46 TUE.
[366] El apartado 3 del artículo 42 TUE recoge que "Los Estados miembros pondrán a disposición de la Unión, a efectos de la aplicación de la política común de seguridad y defensa, capacidades civiles y militares para contribuir a los objetivos definidos por el Consejo. Los Estados miembros que constituyan entre ellos fuerzas multinacionales podrán asimismo ponerlas a disposición de la política común de seguridad y defensa. Los Estados miembros se comprometen a mejorar progresivamente sus capacidades militares…". Por su parte, el apartado 4 del artículo 42 estipula que "El Consejo adoptará por unanimidad, a propuesta del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad o a iniciativa de un Estado miembro, las decisiones relativas a la política común de seguridad y defensa, incluidas las relativas al inicio de una misión contemplada en el presente artículo. El Alto Representante podrá proponer que se recurra a medios nacionales y a los instrumentos de la Unión, en su caso conjuntamente con la Comisión".
[367] Conviene en este sentido recordar que el artículo VIII punto 3 del Tratado de Bruselas firmado el 17 de marzo de 1948 determina que "A petición de cualquiera de las Altas Partes Contratantes, se convocará inmediatamente al Consejo para que pueda celebrar consultas respecto a cualquier situación que pueda constituir una amenaza para la paz, cualquiera que sea la zona en que se produzca, o un peligro para la estabilidad económica". De ahí la importancia de incluir la referencia expresa al territorio de los EEMM

Ediciones Universidad de Salamanca | CC BY-NC-ND

miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas", siendo éste el anclaje jurídico sobre el que articular, a partir de ahora, la respuesta de la Unión ante una agresión armada en el territorio de sus EEMM.

La tercera clave se encuentra en el artículo 42.3 TUE, donde se dispone el compromiso de los EEMM "a mejorar progresivamente sus capacidades militares" y la potenciación del papel de la Agencia Europea de Defensa para, desde dentro del Consejo de la UE, *fomentar las sinergias en el ámbito de la armonización* de requerimientos procedimentales y la mejora de las capacidades militares a través de la investigación, la tecnología y la innovación, el diseño de plataformas de prueba tecnológica, la concertación de ejercicios y maniobras multinacionales para mejorar la interoperabilidad de tropas y equipos, o el compromiso con la industria de defensa europea para contribuir a su competitividad y solidez. La EDA actualmente desempeña un papel fundamental para la coordinación de las diferentes herramientas de cooperación en materia de defensa[368] que, sobre todo a partir de la salida del Reino Unido de la UE, se han puesto en marcha para avanzar en el desarrollo de las capacidades europeas.

La cuarta clave interpretativa del Tratado de Lisboa hace referencia a la naturaleza de los *tres tipos de misiones colaborativas* que puede desempeñar la Unión a través de sus EEMM. En primer lugar, conforme al artículo 42.1 TUE, "las misiones fuera de la Unión que tengan por objetivo garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional" en el marco de complementariedad acordado con la OTAN[369], pero con la novedad de que se supera el ámbito de actuación de las Misiones Petersberg al incluirse nuevos objetivos, entre ellos, las misiones de asesoramiento y asistencia en cuestiones militares y la contribución de esas misiones a la lucha contra el terrorismo mediante el apoyo a terceros países en su territorio[370]. Seguidamente el artículo 42.5 TUE, en relación con el artículo 44, fija el segundo tipo de misiones que, en ese mismo marco de actuación y en defensa de los

delimitar geográficamente el ámbito de la agresión armada que pueda suscitar la invocación de la cláusula de asistencia mutua, al igual que hace el artículo 5 del Tratado de la OTAN.

[368] En concreto el Plan de Desarrollo de Capacidades (PDC), la Revisión Anual Coordinada de la Defensa (CARD), la Cooperación Estructurada Permanente (PESCO) y el Fondo Europeo de Defensa (FED).

[369] El artículo 42.2 del Tratado de Lisboa establece que "La política de la Unión con arreglo a la presente sección no afectará al carácter específico de la política de seguridad y de defensa de determinados Estados miembros, respetará las obligaciones derivadas del Tratado del Atlántico Norte para determinados Estados miembros que consideran que su defensa común se realiza dentro de la Organización del Tratado del Atlántico Norte (OTAN) y será compatible con la política común de seguridad y de defensa establecida en dicho marco".

[370] Este tipo de misiones se definen en el artículo 43, que determina que "1) Las misiones contempladas en el apartado 1 del artículo 42, en las que la Unión podrá recurrir a medios civiles y militares, abarcarán las actuaciones conjuntas en materia de desarme, las misiones humanitarias y de rescate, las misiones de asesoramiento y asistencia en cuestiones militares, las misiones de prevención de conflictos y de mantenimiento de la paz, las misiones en las que intervengan fuerzas de combate para la gestión de crisis, incluidas las misiones de restablecimiento de la paz y las operaciones de estabilización al término de los conflictos. Todas estas misiones podrán contribuir a la lucha contra el terrorismo, entre otras cosas mediante el apoyo prestado a terceros países para combatirlo en su territorio".

Ediciones Universidad de Salamanca | CC BY-NC-ND

valores e intereses de la Unión, el Consejo puede encomendar a un grupo de EEMM que lo deseen y dispongan de las capacidades para llevarlas a cabo[371]. Finalmente, el tercer tipo de misión se encuadra en el modelo colaborativo denominado *cooperación estructurada permanente* (PESCO), prevista en el artículo 42.6 TUE en relación con el artículo 46, que señala que "los Estados miembros que cumplan criterios más elevados de capacidades militares y que hayan suscrito compromisos más vinculantes en la materia para realizar las misiones más exigentes establecerán una cooperación estructurada permanente en el marco de la Unión. Esta cooperación se regirá por el artículo 46 y no afectará a lo dispuesto en el artículo 43"[372].

Merece la pena, por su actual trascendencia y dimensión, ahondar en el entonces novedoso *mecanismo de la PESCO* que introduce el Tratado de Lisboa, con referencia al Protocolo 10 anexo[373], pero que nunca antes había sido utilizado hasta que se decide convertirlo en el eje sobre el que articular la revitalización de la PCSD como respuesta de oportunidad ante el Brexit. A este respecto, la salida del Reino Unido representa las dos caras de la moneda, con un anverso que refleja el abandono de la UE por parte de uno de los miembros con más presupuesto dedicado a defensa y con mayores capacidades militares pero que, en el reverso, muestra la salida del principal defensor de los intereses norteamericanos que prioriza el modelo OTAN y relega a simple comparsa al proyecto de defensa común europea.

Esta estrategia de *huida hacia delante* que inicialmente lideran Francia, Alemania, Italia y España obtiene carta de naturaleza con la Decisión del Consejo de la UE de 11 de diciembre de 2017, por la que se establece una *cooperación estructurada permanente* y se fija la lista de los Estados miembros participantes –actualmente son veintiséis-[374], para impulsar la colaboración intergubernamental bajo unos exigentes criterios aplicados al desarrollo de capacidades militares, al progreso tecnológico e industrial de

[371] El artículo 42 apartado 5) señala que "El Consejo podrá encomendar la realización de una misión, en el marco de la Unión, a un grupo de Estados miembros a fin de defender los valores y favorecer los intereses de la Unión. La realización de esta misión se regirá por el artículo 44", el cual determina que "1). En el marco de las decisiones adoptadas de conformidad con el artículo 43, el Consejo podrá encomendar la realización de una misión a un grupo de Estados miembros que lo deseen y que dispongan de las capacidades necesarias para tal misión. La gestión de la misión se acordará entre dichos Estados miembros, en asociación con el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad".

[372] Estas *misiones más exigentes* encuadradas en la PESCO se definen en el artículo 42.6 TUE y se regulan conforme al artículo 46, en el que se establece que "1) Los Estados miembros que deseen participar en la cooperación estructurada permanente mencionada en el apartado 6 del artículo 42 y que reúnan los criterios y asuman los compromisos en materia de capacidades militares que figuran en el Protocolo sobre la cooperación estructurada permanente notificarán su intención al Consejo y al Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad".

[373] Protocolo (nº 10) sobre la cooperación estructurada permanente establecida por el artículo 42 del Tratado de la Unión Europea. DO C 326 de 26.10.2012, p. 275–277. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A12012M%2FPRO%2F10 (27/10/2023).

[374] Todos los países de la UE excepto Malta. La última incorporación es la de Dinamarca, acordada por una Decisión del Consejo de fecha 23 de mayo de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/05/23/eu-defence-cooperation-council-welcomes-denmark-into-pesco-and-launches-the-5th-wave-of-new-pesco-projects/ (29/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la defensa y al despliegue de operaciones conjuntas de la Unión. El esquema de la PESCO ofrece un marco jurídico de obligado cumplimiento para los Estados firmantes que les exige planificar, desarrollar e invertir en proyectos de capacidades compartidas, mejorar los despliegues conjuntos y la disponibilidad operativa de sus fuerzas armadas, todo ello con el consiguiente beneficio asociado a la economía de escala[375].

La coordinación de estos proyectos PESCO se lleva a cabo desde una Secretaría en la que se integra la EDA, el SEAE y el Estado Mayor de la UE (EMUE), resultando que en la primera fase –que se extiende del 2018 al 2025- se han puesto en marcha sesenta y ocho proyectos[376], de los que son buenos ejemplos el Mando Médico Europeo[377] o los Equipos de Respuesta Rápida Cibernética[378].

Pero a pesar del apreciable progreso que la PESCO ha supuesto para el estímulo de la defensa europea, como laboratorio en el que "los diversos Estados que integran la UE se vayan acostumbrando a compartir, en lo posible, el I+D+i de los proyectos más ambiciosos, así como la política de adquisiciones" (BAQUÉS QUESADA, 2023, pág. 140) hay que decir que la evolución de la PCSD no ha sido todo lo efectiva que se pudiese esperar por distintas razones, que mayormente se imbrican con la redacción que el propio TUE firmado en Lisboa le dedica a esta política y que, en definitiva, conforma el *spiritus legis*. En ningún caso debe pasarse por alto que esta redacción está influenciada por la necesidad de acercar posturas entre las distintas concepciones que los EEMM mantienen sobre su seguridad y, sin lugar a dudas, por el peso de la OTAN en la estructura de defensa europea.

Con ello, las tres principales razones que, a nuestro juicio, obstruyen el desarrollo de la PCSD se refieren a la vaguedad en su concreción, al alcance y efectividad de la cláusula de asistencia mutua del artículo 42.7 TUE, y a los dilemas de interpretación que ésta plantea.

Partiendo del hecho de que la Unión no cuenta con capacidades ni instrumentos propios para llevar a cabo esta PCSD, sino que depende de los medios civiles y militares que los EEMM pongan a su disposición, la primera de estas causas limitativas a las que nos referimos es la *vaguedad en la concreción de la PCSD*, por cuanto el artículo 42.2 únicamente señala que "la política común de seguridad y defensa incluirá la definición progresiva de una política común de defensa de la Unión". Nuevamente, la ambigüedad es el factor que rebaja el nivel de ambición a la hora de definir la estructura de mando y de la fuerza que, en el marco de la autonomía estratégica, debe dar soporte a las decisiones que un actor con voluntad de "mantener la paz, prevenir los conflictos y

[375] Disponible en: https://eda.europa.eu/what-we-do/EU-efence-initiatives/permanent-structured-cooperation-(PESCO) (29/10/2023).

[376] Estos proyectos se encuadran en grupos por tipología: instalaciones y entrenamiento; formación y sistemas de tierra; ámbito marítimo; sistemas aéreos; ciberespacio; habilitación conjunta; y ámbito espacial. Disponible en: https://www.pesco.europa.eu (29/10/2023).

[377] Proyecto European Medical Command. Disponible en: https://www.bundeswehr.de/en/organization/bundeswehr-medical-service-mmcc-emc- (29/10/2023).

[378] Cyber Rapid Response Teams. Disponible en: https://crrts.eu/management.html (29/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

fortalecer la seguridad internacional"[379] va a tener que adoptar para llevar a cabo la disuasión y, en su caso, poder intervenir en acciones de combate conforme a sus intereses geopolíticos. Y este es el sustrato esencial para que brote la raíz que permita sostener la voluntad de los EEMM con el fin de unificar criterios y confiar en la viabilidad de una defensa común europea y autónoma que, tal y como está redactado este artículo, no parece ser tal sino todo lo contrario, es decir, que "los Estados miembros no quisieron que la PCSD compita con sus políticas de defensa nacionales ni con la OTAN" (DÍAZ RODRÍGUEZ, 2018, pág. 8)

La segunda razón que, a nuestro juicio, lastra el despegue de la PCSD es la referida al *alcance y efectividad de la cláusula de asistencia mutua* del artículo 42.7. TUE que dispone:

> **"**Si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas. Ello se entiende sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros.
> Los compromisos y la cooperación en este ámbito seguirán ajustándose a los compromisos adquiridos en el marco de la Organización del Tratado del Atlántico Norte, que seguirá siendo, para los Estados miembros que forman parte de la misma, el fundamento de su defensa colectiva y el organismo de ejecución de ésta".

La afectación a la esencia de esta cláusula se deriva de la doble autolimitación a su alcance que, a toda vista, se paga como tributo para conseguir su encaje en los diferentes planteamientos de los EEMM, derivada de la inclusión de los dos apartados finales del artículo que traslucen una asimetría en el compromiso con la PCSD. De un lado, el que indica que dicha cláusula debe entenderse sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros, concesión a los Estados neutrales de la Unión[380] al no imponerles "asumir obligaciones incompatibles con su propia identidad- si bien dichos Estados no renunciarían, en ningún caso, a la protección que dicho mecanismo les pudiera ofrecer" (URREA CORRES, 2016, pág. 21). Y de otro, la cesión a los Estados que ven en la OTAN su estructura defensiva de referencia[381], al señalar que "los compromisos y la cooperación en este ámbito seguirán ajustándose a los compromisos adquiridos en el marco de la Organización del Tratado del Atlántico Norte, que seguirá siendo, para los Estados miembros que forman parte de la misma, el fundamento de su defensa colectiva y el organismo de ejecución de ésta". En cuanto a este apartado final, su interpretación literal parece dar preferencia automática a la cláusula de defensa colectiva del artículo 5 del Tratado de Washington -filosofía *NATO first*- lo que supone dejar la cláusula de asistencia mutua del artículo 42.7

[379] Artículo 21.2.d del TUE: "La Unión definirá y ejecutará políticas comunes y acciones y se esforzará por lograr un alto grado de cooperación en todos los ámbitos de las relaciones internacionales con el fin de… mantener la paz, prevenir los conflictos y fortalecer la seguridad internacional, conforme a los propósitos y principios de la Carta de las Naciones Unidas, así como a los principios del Acta Final de Helsinki y a los objetivos de la Carta de París, incluidos los relacionados con las fronteras exteriores".

[380] Como por ejemplo Austria, Irlanda, Chipre o Malta.

[381] Principalmente los países más próximos a las fronteras rusas que se incorporaron a la UE en 2004, como Polonia, República Checa, Hungría, Eslovaquia, Eslovenia, Estonia, Lituania o Letonia.

Ediciones Universidad de Salamanca | CC BY-NC-ND

TUE para casos residuales[382]. Sin embargo, hay autores partidarios de una nueva interpretación más acorde con la evolución de ambas estructuras que "debiera poner al Tratado de la UE y a su artículo 42.7 como la cláusula de defensa colectiva prioritaria en caso de agresión en Europa, manteniendo a la Alianza Atlántica, y a su artículo 5, como la segunda respuesta, caso de un ataque contundente" (GARCÍA SERVET, 2015, pág. 100). De esta forma, en atención a la creciente complejidad de la amenaza actual, se podría recurrir a una u otra opción en función de las circunstancias concretas del ataque, el lugar y la forma en que se produzca y los sujetos afectados, desaconsejando en todo caso el recurso automático al mecanismo OTAN para invocar la defensa colectiva (URREA CORRES, 2016, pág. 23)[383].

La tercera razón que consideramos perjudica el desarrollo de la PCSD se deriva de los *dilemas de interpretación* que plantea en sí misma la cláusula de asistencia mutua cuando, en su primer párrafo, establece que "si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas". La primera dificultad exegética se deriva de la ausencia de un procedimiento definido para su invocación por parte del EEMM agredido, la valoración de los hechos por el Consejo y la articulación de la respuesta coordinada en el marco del Derecho Internacional, cuando ciertamente se trata de un mecanismo de extrema relevancia cuya falta de concreción resta, sin ningún género de duda, certeza a su aplicabilidad. El segundo inconveniente que se plantea es que la cláusula de asistencia mutua únicamente concreta obligaciones para los EEMM que, en un plano intergubernamental y de manera soberana y autónoma, decidirán sobre el tipo de ayuda y su alcance[384], sin mención alguna al compromiso ni al papel que la propia Unión, como estructura supranacional responsable de la adopción de decisiones que afecten a la defensa conjunta, debe desempeñar como tal. Y, finalmente, tampoco se define el alcance territorial de la respuesta a esa agresión armada que, esta sí, debe materializarse dentro de las fronteras de la UE.

A estas dificultades intrínsecas de la cláusula de asistencia mutua que acabamos de analizar hemos de añadir una nueva: la relación que ésta guarda con la cláusula de solidaridad. Nos referimos aquí a la disyuntiva de aplicación entre la cláusula de asistencia mutua del articulo 42.7 TUE y la cláusula de solidaridad recogida en el artículo 222 TFUE[385], que fue concebida "bajo la necesidad de dotar a la Unión de una

[382] Básicamente quedaría para los supuestos de ataque a un EEMM que no fuese de la OTAN -caso de Austria, Irlanda, Malta o Chipre-, o hacia un EEMM que fuese también de la OTAN pero cuyo territorio atacado quedase fuera del ámbito de actuación aliado -supuesto típico de Ceuta y Melilla-.

[383] De hecho Francia, tras los atentados terroristas en París de noviembre de 2015, no invoca el artículo 5 del Tratado de Washington sino el artículo 42.7 del Tratado de Lisboa.

[384] Conforme al artículo 42.7 TUE, cada EEMM es soberano para decidir qué tipo de asistencia puede prestar y con qué medios, que no necesariamente han de ser militares.

[385] El artículo 222 TFUE dispone que "1. La Unión y sus Estados miembros actuarán conjuntamente con espíritu de solidaridad si un Estado miembro es objeto de un ataque terrorista o víctima de una catástrofe natural o de origen humano. La Unión movilizará todos los instrumentos de que disponga, incluidos los medios militares puestos a su disposición por los Estados miembros, para:
a) prevenir la amenaza terrorista en el territorio de los Estados miembros; proteger a las instituciones democráticas y a la población civil de posibles ataques terroristas; prestar asistencia a un Estado miembro en el territorio de éste, a petición de sus autoridades políticas, en caso de ataque terrorista;

Ediciones Universidad de Salamanca | CC BY-NC-ND

herramienta útil para luchar contra el terrorismo tras el impacto que provocaron en toda la Unión Europea los atentados del 11 de septiembre en Nueva York y los del 11 de marzo de Madrid", es decir, un modo de afrontar la amenaza del terrorismo de carácter internacional (URREA CORRES, 2016, págs. 28-29). Por ello, esta cláusula de solidaridad se encuentra ubicada dentro del apartado que el TFUE dedica a la acción exterior de la Unión y, como tal, es un instrumento más de la PESC que tiene su desarrollo procedimental específico en la Decisión del Consejo 2014/415/UE[386], por la que ya no solo los EEMM sino la propia Unión se obliga a la movilización de todos los instrumentos de que disponga[387], incluidos los medios militares puestos a su disposición, para prestar asistencia a un socio en su territorio en caso de ataque terrorista, catástrofe natural o humana, que desborde "claramente las capacidades de respuesta de que dispone"[388].

Pero paradójicamente, cuando esas circunstancias descritas se han materializado dentro del territorio de la UE, no se ha utilizado. En este punto debemos recordar los terribles atentados cometidos por el DAESH en noviembre de 2015 en París que motivan que Francia no invoque la cláusula de solidaridad del artículo 222 TFUE, sino el artículo 42.7 del Tratado de Lisboa, porque "no necesita ayuda para combatir un fenómeno terrorista en su territorio, más allá de la cooperación policial y en materia de inteligencia", sino que lo que París busca es que sus socios le presten "apoyo en operaciones militares en el Sahel y en Oriente Medio" (MORA BENAVENTE, 2017, pág. 148). Y aquí es donde radica la cuestión porque, verdaderamente, parece que:

> "[…] las razones por las que Francia invoca la cláusula de asistencia mutua -en detrimento de la cláusula de solidaridad- residen en el atractivo que para los Estados sigue provocando la inspiración intergubernamental que desprende su regulación. Una vez más, la disyuntiva entre dos disposiciones del Tratado reproduce, en realidad, la misma tensión dialéctica sobre la que se asienta el

b) prestar asistencia a un Estado miembro en el territorio de éste, a petición de sus autoridades políticas, en caso de catástrofe natural o de origen humano.

2. Si un Estado miembro es objeto de un ataque terrorista o víctima de una catástrofe natural o de origen humano, a petición de sus autoridades políticas los demás Estados miembros le prestarán asistencia. Con este fin, los Estados miembros se coordinarán en el seno del Consejo.

3. Las modalidades de aplicación por la Unión de la presente cláusula de solidaridad serán definidas mediante decisión adoptada por el Consejo, a propuesta conjunta de la Comisión y del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Cuando dicha decisión tenga repercusiones en el ámbito de la defensa, el Consejo se pronunciará de conformidad con el apartado 1 del artículo 31 del Tratado de la Unión Europea. Se informará al Parlamento Europeo. A efectos del presente apartado, y sin perjuicio del artículo 240, el Consejo estará asistido por el Comité Político y de Seguridad, con el apoyo de las estructuras creadas en el marco de la política común de seguridad y defensa, y por el comité contemplado en el artículo 71, que le presentarán, en su caso, dictámenes conjuntos.

4. Para asegurar la eficacia de la actuación de la Unión y de sus Estados miembros, el Consejo Europeo evaluará de forma periódica las amenazas a que se enfrenta la Unión".

[386] Decisión del Consejo 2014/415/UE, de 24 de junio de 2014, relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad.

[387] La propia Decisión 2014/415/UE, en su punto 5, señala entre los instrumentos pertinentes la Estrategia de Seguridad Interior de la Unión Europea, el Mecanismo de Protección Civil de la Unión y las estructuras creadas en el marco de la PCSD.

[388] El artículo 4.1 de la Decisión 2014/415/UE dispone que: "En caso de catástrofe o ataque terrorista, el Estado miembro afectado podrá invocar la cláusula de solidaridad si, tras haber utilizado las posibilidades ofrecidas por los medios e instrumentos existentes a escala nacional y de la Unión, considera que la crisis desborda claramente las capacidades de respuesta de que dispone".

Ediciones Universidad de Salamanca | CC BY-NC-ND

> propio proyecto de construcción europea: la supranacionalidad como vocación, el intergubernamentalismo como devoción" (URREA CORRES, 2016, pág. 34).

Y todo ello no hace sino afectar gravemente a la proyección de credibilidad de la política de defensa europea.

3.3.3. La cristalización de un nuevo enfoque: la Brújula Estratégica para la Seguridad y la Defensa (2022)

El Brexit, la primera legislatura de Donald Trump como Presidente de los EE.UU., la inestabilidad en el Sahel o la invasión rusa de Ucrania suponen para la Unión factores revulsivos y propulsores del espíritu colaborativo aplicado a la PCSD.

Esta línea de colaboración se inicia en noviembre de 2016, cuando el Consejo de la UE aprueba el Plan de Implementación de Seguridad y Defensa[389] para trasladar la visión que marca la EUGS con el objetivo de consolidar a la Unión como comunidad de seguridad capaz de actuar de manera autónoma a través de una PCSD creíble, definiendo para ello un nuevo nivel de ambición centrado en tres prioridades estratégicas: responder con un enfoque integrado ante los conflictos y crisis exteriores, fomentar el desarrollo de las capacidades de defensa de los socios, y proteger la seguridad de la Unión y de sus ciudadanos.

Para alcanzar estas metas dicho Plan propone trece propuestas de acción entre las que, en atención al objeto de nuestro estudio, merecen ser destacadas las seis siguientes:

1. Profundizar en la cooperación en materia de defensa, utilizando a la EDA como clave del desarrollo de capacidades compartidas y creándose al efecto la Revisión Anual Coordinada de la Defensa (CARD) como forma de alinear esfuerzos, de identificar puntos de coincidencia de intereses y de ganar transparencia en los proyectos, permitiendo de esta manera optimizar recursos y generar economías de escala. A su vez, este modelo permite tener una visión global de los planes de colaboración e inversión que, a nivel de toda la UE, se están implementado en este momento, su nivel real de desarrollo y las posibilidades de acometer proyectos futuros en similares condiciones.
2. Desarrollar una Capacidad Militar de Planificación y Conducción de operaciones de la UE (MPCC), complementaria a la estructura que, dependiente del SEAE, representa la Capacidad Civil de Planificación y Ejecución (CPCC) que gestiona las misiones civiles de asesoramiento, desarrollo de capacidades o gestión de fronteras en que se implica la Unión.
3. Mejorar la gestión de la información como soporte para la anticipación y el conocimiento del contexto en el ámbito del análisis de inteligencia civil y militar, a través de la Capacidad Única de Análisis de Inteligencia (SIAC).
4. Fortalecer la relevancia, usabilidad y desarrollo de las herramientas de Respuesta Rápida de la Unión, incluyendo los *EU Battlegroups* (EUBG), en

[389] Plan de Implementación de Seguridad y Defensa, del Consejo de la Unión Europea. Bruselas 14 de noviembre de 2016. 14392/16. Disponible en https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf (01/11/2023)

Ediciones Universidad de Salamanca | CC BY-NC-ND

concreto su composición modular para mejorar la flexibilidad de uso, la movilidad, la preparación y la financiación efectiva de sus despliegues.

5. Potenciar la PESCO como vía para mejorar la cooperación en el ámbito de defensa entre los EEMM con mayores capacidades y voluntad de asumir un superior compromiso en su desarrollo.
6. Impulsar la cooperación con los socios estratégicos de la UE, tanto a nivel de países como de organizaciones, destacando las NNUU, la OTAN, la OSCE y la Unión Africana[390].

Este Plan de Implementación de Seguridad y Defensa, a su vez, forma parte de un paquete mayor de medidas entre las que se encuentra el Plan de Acción Europeo de Defensa (EDAP)[391], que presenta propuestas clave para el impulso del Fondo Europeo de Defensa (EDF) en apoyo de la investigación conjunta y el desarrollo de equipos y tecnologías de defensa[392], el fomento de la inversión en *pymes* y proveedores del sector, y el reforzamiento del mercado único de la seguridad y la defensa para rentabilizar los contratos públicos, evitar la duplicidad de las inversiones y mejorar la competitividad europea. En este sentido, el EDF ha sido concebido para beneficiar a la PCSD y, como señalan algunos estudiosos del tema, ha supuesto un "verdadero punto de inflexión para la industria puesto que por primera vez la Comisión lanza iniciativas concretas para financiar proyectos de defensa que repercutan en una mayor cooperación industrial" (CALVO GONZÁLEZ-REGUERAL, 2021).

No obstante, el principal escollo frente a todo este esfuerzo impulsor sigue siendo la necesaria reorientación de las estrategias de inversión y de adquisiciones militares por los EEMM, que deben priorizar, por un lado, el enfoque europeísta de la defensa frente a la particular gestión de compras de cada uno de ellos y, por otro, la voluntad cooperadora en el ámbito de la industria europea frente al proteccionismo de los mercados nacionales. A este objetivo está contribuyendo la EDA impulsando iniciativas como la denominada *Industry Engagement*[393] que, alineada con la Base Industrial y Tecnológica de Defensa Europea (EDTIB), busca ampliar las capacidades de defensa y garantizar la tan ansiada *autonomía estratégica* de la Unión a través del fomento de consorcios tecnológicos e innovadores transfronterizos, la mejora de la gestión de la información para el acceso a los proyectos de desarrollo y la facilitación del acceso a la financiación con cargo a los fondos de la UE.

[390] La Unión Africana es una organización intergubernamental clave para la UE en cuanto a su posicionamiento en el continente por cuanto reúne a 55 Estados miembros que respaldan su capacidad de intermediación mediante canales diplomáticos y misiones de apoyo a la paz.

[391] Comunicado de Prensa de 30 de noviembre de 2016, de la Comisión Europea, sobre el Plan de Acción Europeo de Defensa: hacia un Fondo Europeo de Defensa. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_16_4088 (011/11/2023).

[392] Un ejemplo es el proyecto KOIOS de inteligencia artificial para la defensa, del programa anual 2021 del EDF, cuyo objetivo es adaptar al entorno operacional y de toma de decisiones de las fuerzas armadas las innovaciones de la IA. Este proyecto es coordinado por la empresa española CT. Disponible en: https://www.defensa.com/otan-y-europa/ct-lidera-proyecto-inteligencia-artificial-koios-apoyado-fondo (07/11/2023).

[393] Disponible en: https://eda.europa.eu/what-we-do/industry-engagement (01/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Debemos también hacer mención al hecho de que, en noviembre de 2020, el Consejo adopta la Decisión (PESC) 2020/1639 por la que se abre la participación de terceros Estados en proyectos individuales PESCO[394], con la idea de dar entrada a socios estratégicos de la Unión que puedan aportar valor a sus intereses de seguridad y defensa, con un innegable enfoque *win to win*. Cierto es que aunque esta es una vía idónea para dar formato institucional a las relaciones existentes entre la industria de defensa europea y británica, enraizadas a lo largo de muchos años, hasta ahora no ha sido objeto de deseo para nuestros antiguos socios, que prefieren mantener acuerdos bilaterales y multilaterales como la Iniciativa Europea de Intervención (EI2) liderada por Francia que, en un contexto estratégico cada vez más complicado, marca como prioridad "mantener su relación de seguridad privilegiada con el Reino Unido y mantener a Gran Bretaña anclada en la seguridad colectiva europea después del Brexit" (MOYA CÁNOVAS, 2019, pág. 8) de acuerdo a los intereses galos. Sin embargo, este modelo colaborativo sí ha llamado la atención de Canadá, Noruega y Estados Unidos que, en mayo de 2021, entraron a participar en el proyecto *Movilidad Militar* como área de interés compartido entre socios OTAN[395].

En línea con esta planificación del EDAP, en febrero de 2021 la Comisión Europea presenta el Plan de Acción sobre las sinergias entre las industrias civil, de la defensa y espacial[396] con un doble objetivo: sensibilizar a la opinión pública acerca del efecto multiplicador de la inversión en investigación y desarrollo en estos sectores y, en segundo lugar, generar sinergias enriquecedoras entre estas vertientes de la industria reforzando la complementariedad de los proyectos de la UE para aumentar su eficiencia y eficacia, fomentando la transferencia de tecnología desde el sector de la defensa al civil -*spin offs*-, y facilitando la absorción por el sector de la defensa de las innovaciones y desarrollos investigativos de la industria civil -*spin ins*-.

Este Plan de Acción presenta once líneas estratégicas que, en teoría, deben coadyuvar a que la UE consiga el liderazgo tecnológico y digital necesario para protegerse ante los desafíos que plantea el complejo contexto internacional actual:

1. Un enfoque de los proyectos basado en las capacidades definidas por las necesidades de los usuarios y su compromiso de adquirir los productos desarrollados al efecto.
2. La promoción de sinergias entre los programas para facilitar los *spin-offs* y los *spin-ins* entre los tres sectores de la industria.

---

[394] Decisión (PESC) 2020/1639 del Consejo de 5 de noviembre de 2020 por la que se establecen las condiciones generales en las que se podrá invitar excepcionalmente a terceros Estados a participar en proyectos individuales de la Cooperación Estructurada Permanente. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020D1639 https://www.consilium.europa.eu/en/press/press-releases/2020/11/05/eu-defence-cooperation-council-sets-conditions-for-third-state-participation-in-pesco-projects/ (01/11/2023).

[395] Comunicado de prensa. Disponible en: https://www.consilium.europa.eu/en/press/press-releases/2021/05/06/pesco-canada-norway-and-the-united-states-will-be-invited-to-participate-in-the-project-military-mobility/ (01/11/2023).

[396] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción sobre las sinergias entre las industrias civil, de la defensa y espacial. Comisión Europea. Bruselas, 22 de febrero de 2021. COM (2021) 70 final. Disponible en: https://commission.europa.eu/document/2353ded9-0e39-4d35-a46c-67c62779afe1_es (01/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

3. El apoyo decidido a *pymes*, empresas emergentes y organismos de investigación y tecnología.
4. La consecución de la soberanía tecnológica europea en áreas críticas[397].
5. La aplicación de normativas unificadas para ahorrar costes y mejorar la eficiencia operativa.
6. La innovación aplicada a las tecnologías de doble uso.
7. El establecimiento del Centro de Competencia de Ciberseguridad para reducir las vulnerabilidades de las infraestructuras y sistemas críticos de la Unión.
8. El fomento de la participación en los proyectos de actores no convencionales y empresas emergentes para apoyar el desarrollo de las tecnologías disruptivas.
9. El fortalecimiento de la competitividad de la industria europea en el sector de los drones.
10. La definición de un sistema global de comunicaciones seguras de la UE para proporcionar acceso a la conectividad de alta velocidad a través de una infraestructura espacial multiorbital.
11. Y la gestión del tráfico espacial para preservar los activos de la Unión en el espacio frente a posibles colisiones con otros satélites o desechos espaciales.

Otro paso adelante se formaliza un mes después, en marzo de 2021, cuando el Consejo adopta la Decisión (PESC) 2021/509 por la que crea el Fondo Europeo de Apoyo a la Paz[398] para, en la filosofía de dar una respuesta ágil y efectiva a las crisis y amenazas de interés estratégico para la Unión, financiar las misiones y operaciones que, en el marco de la PESC, se lleven a cabo en solitario o conjuntamente con sus socios en el marco de la prevención de conflictos, el aseguramiento de la paz y la preservación del orden internacional. Esta forma de financiación aplica a conceptos como equipamiento militar, infraestructuras de apoyo y asistencia técnica.

En medio de esta corriente impulsora de sinergias entre sectores estratégicos e industriales y de líneas de financiación, el 21 de marzo de 2022, tras meses de trabajo colaborativo entre todos los EEMM de la UE para valorar las amenazas y acordar una visión estratégica común que defina su política de seguridad y defensa del próximo

[397] Estas áreas críticas son la electrónica y el sector digital (IA, seguridad y ciberdefensa, análisis forense digital, informática de alto rendimiento y computación en la nube, fotónica, microprocesadores y electrónica impresa o flexible ligera, tecnología cuántica, fotónica, comunicaciones y redes seguras, y sensores de distinta naturaleza y funcionalidad); la fabricación avanzada (nanotecnología, robótica, semiconductores y microelectrónica); el espacio y la aeronáutica (tecnologías espaciales, de posicionamiento, navegación y temporización de precisión, de observación de la Tierra de alta definición, comunicaciones y conectividad seguras por satélite); la sanidad (biotecnologías y tecnologías químicas, biológicas, radiológicas y nucleares); la energía (tecnologías energéticas); y la movilidad (sistemas autónomos).

[398] Decisión (PESC) 2021/509 del Consejo de 22 de marzo de 2021, por la que se crea un Fondo Europeo de Apoyo a la Paz y se deroga la Decisión (PESC) 2015/528. DOUE núm. 102, de 24 de marzo de 2021. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80367 (07/11/2023).
Esta Decisión al mismo tiempo deroga el anterior instrumento de financiación *mecanismo Athena*, aprobado por la Decisión (PESC) 2015/528. Originalmente el Fondo Europeo de Apoyo a la Paz tenía un límite de 5.692 millones de euros para el periodo 2021-2027, pero fue ampliado en diciembre de 2022 en otros 2.287 millones de euros a la vez que se convino que, en caso de necesidad, podría aumentarse este límite máximo otros 3.500 millones de euros hasta 2027, cuestión que se lleva a efecto en marzo de 2023 fijando el Consejo un límite financiero para el Fondo de 7.979 millones de euros hasta el 2027.

Ediciones Universidad de Salamanca | CC BY-NC-ND

decenio, el Consejo de la Unión Europea aprueba la Brújula Estratégica para la Seguridad y la Defensa (BESD), apostillada con el lema *Por una Unión Europea que proteja a sus ciudadanos, valores e intereses y contribuya a la paz y la seguridad internacionales*[399]. Su nacimiento prácticamente coincide en el tiempo con la invasión rusa de Ucrania, a la que el AR/VP Josep Borrell, en su prólogo, califica como acelerador de la *política de poder* que instrumentaliza cualquier situación como arma usable en la permanente batalla de narrativas que se disputa en este contexto internacional multipolar, altamente cambiante, incierto, complejo y ambiguo.

Debemos comenzar señalando que, como novedad respecto a sus dos antecesoras, la Brújula Estratégica está respaldada, primeramente, por el *compromiso de llevarla a la práctica* que cada uno de los EEMM asume con su aprobación y, en segundo lugar, por el sistema de seguimiento que se formaliza a través de los *Informes Anuales de progreso en su aplicación*[400]. No obstante, el elemento diferencial de la Brújula Estratégica es su *enfoque práctico orientado a guiar la agenda de seguridad y defensa europea* una vez demostrado tener "la mentalidad, los medios y los mecanismos para defender a la Unión, a sus ciudadanos y sus socios"[401], como se ha visto con el apoyo prestado a Ucrania para restablecer su libertad y la legalidad internacional. Para la adecuada gestión de su defensa, la UE necesita una aproximación global a este complejo entorno de amenazas que le permita utilizar todas las herramientas de que dispone para, en el lenguaje del poder, enfrentar de igual a igual al resto de competidores sistémicos recurriendo, según la ocasión, al *soft power* o al *hard power* y defender sus intereses. La BESD es la firme constatación de la legítima ambición europea por convertirse en un *proveedor de seguridad* capaz y confiable que, como muestra de compromiso con los resultados que pretende, establece la inmediata implementación práctica de las más de ochenta acciones concretas planteadas para alcanzar los objetivos fijados a través de los medios disponibles y en los plazos señalados. Todo ello se organiza en torno a cuatro áreas de trabajo definidas por cuatro verbos de acción: *actuar*, *dar seguridad*, *invertir* y *cooperar*.

La línea *actuar* pretende la mayor asertividad de la UE como *proveedor de seguridad* internacional, mediante la rapidez y contundencia en la respuesta ante cualquier tipo de crisis que, en el marco de la PCSD, afecte a los intereses de la Unión tanto dentro como fuera de su territorio. En este sentido, se propone la Capacidad de Despliegue Rápido (EURDC) para disponer de una fuerza militar europea modular y escalable de

[399] Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales. Bruselas, 21 de marzo de 2022. 7371/22. Disponible en: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf (08/11/2023).

[400] El primero de estos Informes Anuales de progreso de la implementación de la BESD es el de marzo de 2023, donde el AR/VP Josep Borrell señala que ha servido para lo que su propio nombre indica, es decir, para mostrar la dirección en que la UE debe avanzar para mantenerse en el camino adecuado, por cuanto se está acortando la distancia entre nuestras aspiraciones y nuestros actos. Disponible en: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf (06/11/2023).

[401] Prólogo del AR/VP Josep Borrell a la Brújula Estratégica para la Seguridad y la Defensa. Disponible en: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en (5/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

hasta cinco mil efectivos, con sus correspondientes habilitadores estratégicos[402], de la que son parte integrante los *EU Battlegroups*, así como el desarrollo de capacidades de las misiones civiles para poder desplegar en el plazo de treinta días a doscientos expertos civiles y su correspondiente equipamiento. También forman parte de esta estrategia el fortalecimiento de la Capacidad Militar de Planificación y Conducción (MPCC) mediante la flexibilidad y movilidad de las fuerzas y el desarrollo de ejercicios regulares *en vivo*[403], como forma de entrenar la respuesta para hacer frente a una agresión armada en el territorio de la Unión en el marco de la *asistencia mutua* del artículo 42.7 TUE.

La segunda línea de acción, *dar seguridad,* busca preparar a la Unión para afrontar con éxito los retos emergentes a través del aumento de las capacidades de inteligencia y securización de las comunicaciones, mediante el potenciamiento de la SIAC y del *EU Satellite Centre* para generar inteligencia geoespacial. Respecto a la amenaza híbrida, la respuesta se coordina desde el marco que define la *EU Hybrid Toolbox*[404] para combatir la injerencia extranjera y sus consiguientes campañas desinformadoras y de manipulación en las sociedades europeas, así como la creación de un equipo de respuesta rápida y la mejora de las herramientas de ciberdiplomacia. Los dominios estratégicos se garantizan mediante una política de ciberdefensa de la Unión, que implica la redacción de un Reglamento de Ciberesiliencia[405] y la creación de una Unidad Cibernética conjunta, así como la definición de estrategias específicas para la seguridad y defensa espacial, marítima y aérea. Otros riesgos que se valoran hacen referencia al terrorismo, a la proliferación de armas y al cambio climático, con los desastres y las emergencias que genera, para lo que se propone mejorar el soporte militar de ayuda a las autoridades civiles en dichos supuestos.

Por lo que respecta a la línea de *inversión*, su objetivo es aumentar el gasto en defensa del conjunto de la UE, alineándolo así con la ambición de operar como *proveedor de seguridad* global. Con esta finalidad se diseña una estrategia de desarrollo de capacidades civiles y militares de última generación en todos los dominios operacionales[406] mediante proyectos conjuntos que, involucrando a la industria

[402] Los *habilitadores estratégicos* hacen referencia a los equipamientos de soporte y proyección de tropas como el transporte aéreo estratégico, las capacidades de repostaje en vuelo, las bases de comunicaciones, los activos médicos, las capacidades de ciberdefensa, las capacidades de inteligencia, vigilancia y reconocimiento, etc.

[403] El primer ejercicio militar en vivo de la UE para la gestión de crisis se lleva a cabo en España en septiembre de 2023, bajo el nombre MILEX 23. Disponible en: https://emad.defensa.gob.es/prensa/noticias/2023/09/Listado/230918-ni-inicio-milex-23.html (06/11/2023).

[404] La *Caja de Herramientas Híbridas de la Unión* es un conjunto de medidas para la identificación y reacción ante posibles narrativas manipuladoras y desinformativas extranjeras, creadas por el StratCom (Strategic Communication) del SEAE en el marco analítico conocido como FIMI (Foreign Information Manipulation and Interference).

[405] Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023, por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión. DOUE 18.12.2023. Disponible en: https://www.boe.es/doue/2023/2841/L00001-00027.pdf (22/04/2024).

[406] La Brújula Estratégica centra el desarrollo de capacidades de siguiente generación en las áreas definidas en la CARD, como por ejemplo el sistema de carro de combate principal, la plataforma naval de alta gama

Ediciones Universidad de Salamanca | CC BY-NC-ND

europea, aprovechen la financiación de los EDF y de la PESCO con vistas a incrementar la interoperabilidad de los sistemas y equipos y que, en otro orden de cosas, se beneficien de las ventajas de la economía de escala cuyo impulso procura el Programa de Inversión en Defensa (EDIP)[407]. Otro de los objetivos es reducir las brechas críticas en habilitadores estratégicos, así como la dependencia tecnológica y de las cadenas de valor esenciales para la seguridad y la defensa, con proyectos como el Programa de Innovación en Defensa (EUDIS)[408].

Finalmente, la cuarta línea de acción, *cooperar*, trata de profundizar en la contribución de la Unión al reforzamiento de la paz y la seguridad mundial, así como a la defensa del orden internacional a través de la estabilidad que, junto con sus socios, puede proyectar desde una triple perspectiva: multilateral, regional y bilateral[409]. Para contribuir a esta idea nace el Foro Schuman de Seguridad y Defensa[410], modelo del compromiso de la UE con la creación de una red de socios y actores de diferente naturaleza e intereses para analizar retos, debatir iniciativas y proponer soluciones conjuntas frente a los desafíos que representa el nuevo orden mundial.

Visto lo anterior, podemos concluir que, efectivamente, la Brújula Estratégica representa la cristalización de un nuevo enfoque de la seguridad y la defensa europea más ambicioso pero alcanzable, más estratégico pero orientado a la acción, más europeo pero alineado con sus socios. Al mismo tiempo, conlleva la toma de conciencia de la necesidad de dar un salto cualitativo en la responsabilidad y el compromiso conjunto para que, definitivamente, Europa tome la iniciativa de su propia defensa y, con ello, proyecte una imagen creíble de proveedor de seguridad fuerte y coherente ante el mundo, sus socios y sus ciudadanos. En definitiva, como señala Coello de Portugal, la Brújula Estratégica es el instrumento utilizado para definir con claridad y orientar de forma adecuada la estrategia de la Unión frente a las cambiantes

digital y conectada, el sistema de combate aéreo del futuro y contra aviones no tripulados, los sensores y plataformas espaciales de observación de la Tierra, y la interconexión de todos los dominios, entre otras.

[407] El Programa Europeo de Inversión en Defensa (EDIP) permite la formación de consorcios entre los Estados miembros, con el objetivo de desarrollar colaborativamente y adquirir de manera conjunta capacidades de defensa a través de la industria europea, con beneficios fiscales y de financiación. Disponible en: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/european-defence-investment-programme y en https://cnv-consulting.eu/wp-content/uploads/2023/04/1-CV-Consulting-EDIP-Rebuilding-European-Defence-by-Strengthening-our-Industry.pdf (07/11/2023).

[408] El Plan de Innovación en Defensa de la UE (EUDIS) es un conjunto de instrumentos habilitados por el Fondo Europeo de Defensa (FED) para que las pequeñas y medianas empresas (pymes), incluidas las empresas emergentes y otros actores no tradicionales del ecosistema industrial de defensa, dispongan de más oportunidades de acceso a esta financiación y, con ello, reforzar la innovación en materia de defensa en la Unión Europea. Disponible en: https://eudis.europa.eu/index_en (07/11/2023).

[409] En el ámbito multilateral la referencia de la Brújula Estratégica es tanto a la OTAN como a NNUU, en el regional a la OSCE, la Unión Africana y la Asociación de Naciones del Asia Sudoriental, y en el marco bilateral a EE.UU., Noruega, Canadá, Reino Unido y países de América latina, entre otros.

[410] La primera reunión del Schuman Security and Defence Partnership Forum se celebró entre el 20 y 21 de marzo de 2023, con la presencia de los 27 EEMM de la Unión y más de 400 participantes de 50 países y organizaciones internacionales de Europa, América, África, Oriente Medio, y la región de Asia-Pacífico, con la idea de ofrecer soluciones. Disponible en: https://www.eeas.europa.eu/eeas/schuman-security-and-defence-forum_en (07/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

circunstancias y, a su vez, definir los riesgos, retos y desafíos que habrá de afrontar en el corto y medio plazo (COELLO DE PORTUGAL, 2024, pág. 102).

Como vemos, la UE busca ser jugador geoestratégico, no un mero pivote geopolítico, y la invasión rusa de Ucrania ha funcionado como elemento disruptor que ha contribuido a que adopte un papel más asertivo en la determinación de sus propias capacidades de defensa, que pasan por disponer de más armas, por tener la autonomía tecnológica para producirlas y mantenerlas, y por invertir en investigación y desarrollo industrial que pueda aplicarse al campo militar[411]. Esta proactividad es el camino que la UE debe recorrer para alcanzar la capacidad de influencia en el tablero mundial, multipolar y asimétrico, en el que, lógicamente, el simple hecho de jugar exige competir para no ser eliminado.

3.3.4. El Libro Blanco de la Defensa y el Plan ReArm Europe: la estrategia de defensa europea mirando al 2030

En marzo de 2025 la Comisión Europea, en cierta forma desconcertada ante la velocidad y la profundidad de los cambios que se suceden en el orden internacional a partir de la segunda llegada de Donald Trump a la Casa Blanca, da un golpe encima de la mesa y se muestra contundente en el mensaje inicial de su *Joint White Paper for European Defence - Readiness 2030*[412]:

> "Europe faces an acute and growing threat. The only way we can ensure peace is to have the readiness to deter those who would do us harm"[413].

Si con la Brújula Estratégica la UE exteriorizaba su íntima ambición de ser un proveedor de seguridad con su correspondiente rol geoestratégico, con el Libro Blanco de la Defensa parece ir un paso más allá mostrándose decidida a *tomar las armas* para asegurar su propio futuro en un entorno de competencia sistémica. La Unión, al fin, no tiene reparos en decir en voz alta que se prepara para disuadir, hasta con las armas, al que pretenda agredirla.

Para demostrar esta firme determinación lo primero que hace la Comisión Europea es un análisis DAFO en el que distingue:

---

[411] En esta idea, la Comisión impulsa la estrategia europea para reforzar la industria de defensa y propone como objetivo que, para 2030, los EEMM compren a empresas de la UE al menos la mitad del material militar. Disponible en: https://elpais.com/internacional/2024-03-05/bruselas-urge-a-impulsar-la-industria-europea-de-defensa-para-rearmarse-frente-a-la-amenaza-de-rusia.html https://www.elconfidencial.com/mundo/2024-03-05/bruselas-urge-a-que-en-2030-el-50-de-la-compra-de-armamento-en-la-ue-sea-de-material-europeo_3842815/ https://www.lavanguardia.com/internacional/20240306/9537750/cuando.html (08/03/2024).

[412] Joint White Paper for European Defence - Readiness 2030. Brussels, 19.3.2025. JOIN(2025) 120 final. Disponible en: https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf (23/03/2025).

[413] "Europa se enfrenta a una amenaza aguda y creciente. La única forma en que podemos garantizar la paz es estar listos para disuadir a aquellos que quieren hacernos daño" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

1. Sus propias *debilidades*, referidas a la insuficiente preparación para su autodefensa después de décadas de escasa inversión, y la consiguiente falta de credibilidad estratégica frente a sus oponentes.
2. Las *amenazas* propiciadas, por un lado, por actores que están configurando un nuevo orden internacional, donde se conjugan las ambiciones territoriales de Rusia, el aumento del gasto en defensa y la falta de transparencia de China, la inestabilidad de Oriente Medio, los conflictos extremistas de África, y por otro, por factores externos identificados con las amenazas híbridas[414], la carrera tecnológica global[415], el acceso a las materias primas críticas para la producción y el desarrollo de las capacidades de defensa y, finalmente, la posible agresión armada a Europa.
3. Sus *fortalezas*, que le proporcionan a la UE el elemento diferencial, y que se vertebran en torno a su vasto potencial de recursos, al poder tecnológico e industrial latente, a su capacidad productiva y, sobre todo, a su fe y compromiso con los principios y valores democráticos.
4. Las *oportunidades* que se sitúan en el exterior de la Unión y que pueden favorecer sus intereses, básicamente la vinculación de sus EEMM con la OTAN y la propia coyuntura temporal, que favorece la propuesta de la Comisión Europea para construir de manera autónoma un futuro seguro y de bienestar para los ciudadanos.

El objetivo no es otro que garantizar la paz desde la disuasión, sobre la base de tres pilares: el inquebrantable compromiso europeo con el Derecho Internacional, el nexo de unión de sus EEMM a través de la democracia, y la voluntad de llevar a efecto este proyecto de defensa a través del denominado *Plan ReArm Europe 2030*.

En este sentido, el Libro Blanco de la Defensa supone el marco para el desarrollo del Plan ReArm Europe 2030 que fija los siguientes objetivos para dicho periodo temporal:

1. En el corto plazo, la reposición urgente de munición, armas y equipamiento militar de los EEMM y el decidido apoyo a Ucrania frente a Rusia, claramente identificada como la mayor amenaza para la seguridad común europea.
2. En el medio y largo plazo, el desarrollo de capacidades de defensa de la UE en colaboración con la OTAN, y el diseño de una línea estratégica de desarrollo tecnológico e investigativo para potenciar la industria y revitalizar el mercado de defensa europeo.

El Libro Blanco muestra también una faceta mediadora de la Comisión Europea respecto a los EEMM a través del compromiso de integración, dentro de su visión de la *defensa conjunta,* de las respectivas *políticas de defensa nacionales*, señalando expresamente que:

[414] Amenazas híbridas que se refieren a los ciberataques, el sabotaje de infraestructuras críticas submarinas, la interferencia en sistemas satelitales, la desinformación, el espionaje político e industrial o la instrumentalización de las migraciones, entre otras.

[415] La innovación y el desarrollo de las tecnologías asociadas a la IA, la computación cuántica, la biotecnología, la robótica o la tecnología hipersónica resultan hoy por hoy claves para la proyección industrial, económica y militar a medio y largo plazo.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] the EU will always act in a way that is without prejudice to the specific character of the security and defence policy of certain Member States and taking into consideration the security and defence interests of all Member States"[416].

La estrategia de construcción de esta capacidad disuasoria de Europa frente a una posible agresión se organiza en torno a cinco grandes líneas de desarrollo:

1. Cerrar las *brechas críticas de capacidad*[417] a través de la actuación multidimensional y colaborativa entre los propios EEMM y la OTAN, la mejora de la *movilidad de tropas y equipamientos militares* en territorio UE, la protección de las *fronteras europeas* por tierra, mar y aire[418], el desarrollo de un paquete de *medidas de defensa ómnibus* con el objetivo de armonizar y simplificar normativa y procedimientos que afectan a la base tecnológica e industrial europea de defensa, y la generación de *reservas estratégicas* potenciando asociaciones transfronterizas para el acopio, almacenamiento y distribución de productos de defensa, componentes y materias primas asociadas.
2. El *aumento del apoyo militar a Ucrania* en el marco de la denominada *Porcupine Strategy* donde queda patente, por un lado, la íntima conexión entre la seguridad europea y la de Ucrania por cuanto que, independientemente de posibles acuerdos de paz, ésta permanecerá como la primera línea de defensa frente a Rusia, y por otro, que este es el escenario donde actualmente se está definiendo el nuevo orden mundial y el peso específico de sus principales actores.
3. El desarrollo de un sector industrial europeo de la defensa fuerte e innovador, a través de seis líneas estratégicas: la generación de demanda agregada con un flujo constante de pedidos; la resiliencia de la cadena de suministros; la creación de un mercado de equipos de defensa europeo; la simplificación y armonización normativa; el impulso de la innovación disruptiva aplicada a la defensa y, finalmente, la atracción y sustento del talento en el sector.
4. El aumento del gasto en defensa de los EEMM europeos cuyo gasto conjunto sigue siendo inferior al de, por ejemplo, EE.UU., Rusia o China. Para ello, el Plan ReArm Europe recoge una serie de recomendaciones para la activación coordinada de la inversión, como por ejemplo la redacción de un nuevo Reglamento para proporcionar préstamos a los EEMM respaldados por el presupuesto de la UE, la flexibilización de los actuales instrumentos financieros para permitir una mayor inversión en defensa, o la movilización del capital privado para llevar sus soluciones a escala industrial, entre otras.
5. La cooperación con socios y aliados para alcanzar mayores estándares de seguridad europeos frente a los desafíos de seguridad actuales, mediante la

[416] "La UE siempre actuará sin perjuicio del carácter específico de la política de seguridad y defensa de algunos Estados Miembros y teniendo en cuenta los intereses de seguridad y defensa de todos los Estados Miembros" (Traducción propia).

[417] El Libro Blanco marca siete áreas prioritarias de acción para solventar las *brechas críticas de capacidad*: la defensa aérea y antimisiles multicapa y de amplio espectro, los sistemas de artillería avanzada y de largo alcance, la creación de una reserva estratégica de municiones y misiles y conseguir una adecuada capacidad de producción, el desarrollo y adquisición de drones y sistemas antidrones, la mejora de la movilidad militar, la protección de las infraestructuras críticas, y la innovación en IA, guerra cuántica, cibernética y electrónica.

[418] En este ámbito se menciona expresamente la creación de un *Escudo de la Frontera Oriental* para reforzar la protección física y cibernética frente a Rusia y Bielorrusia.

Ediciones Universidad de Salamanca | CC BY-NC-ND

firma de acuerdos de *asociación de seguridad y defensa*[419] o la profundización en las relaciones ya existentes.

La Comisión Europea, consciente del reto que supone la puesta en marcha efectiva de este amplio marco de acciones normativas, ejecutivas y presupuestarias, avanza la llegada de hitos intermedios y complementarios como:

1. La *Preparación de la Estrategia de la Unión*, para dar un enfoque integral a los riesgos derivados de los conflictos y crisis.
2. La *Estrategia de Seguridad Interior de la Unión*, marco compartido desde el que prevenir, detectar y responder eficazmente a las amenazas de seguridad europeas.
3. La *Comunicación Conjunta sobre Movilidad Militar* -prevista para el año 2025-, para mejorar la capacidad de llevar a efecto movimientos rápidos de tropas y equipos militares por todo el territorio de la Unión, con las consiguientes acciones orientadas al fortalecimiento de la logística de las fuerzas armadas, la simplificación de regulaciones administrativas y procedimientos, o la creación de cuatro corredores multimodales prioritarios para uso militar[420].
4. El inicio -también en el 2025- del *Diálogo estratégico con la industria de la defensa*, para tratar cuestiones referidas a la simplificación y armonización de normativa y procedimientos *específicos* del sector de la defensa y, también, de aquellas políticas y reglamentos de la Unión *no específicos* del sector de defensa pero que pueden obstaculizar la necesaria y rápida evolución de la base tecnológica e industrial europea de la defensa.
5. La reafirmación del *Programa Europeo de Inversión en Defensa* (EDIP)[421] y la adopción prioritaria del correspondiente Reglamento EDIP.
6. La revisión de la *Directiva sobre Defensa y Contratación de Seguridad*[422] -prevista para 2026- como requisito previo indispensable para poder conseguir una industria europea de la defensa fuerte e innovadora, complementada por la redacción de una *Hoja de Ruta Europea de la Tecnología del Armamento*, para dar entrada a las empresas de innovación y desarrollo tanto de tecnología civil como militar, independientemente de su tamaño.

Conforme a esto, en nuestra opinión, el *camino a seguir para la defensa europea* que traza el Libro Blanco se basa en tres ideas principales:

---

[419] En concreto se refiere el Libro Blanco a los recientes acuerdos firmados con Noruega, Japón y la República de Corea, y abunda en la posibilidad de nuevos acuerdos con Reino Unido, Canadá, o la India.

[420] Ferrocarriles, carreteras, corredores marítimos y aéreos.

[421] Como vimos en el apartado anterior, el Programa Europeo de Inversión en Defensa figuraba en la línea de *inversión* de la Brújula Estratégica, para impulsar la formación de consorcios industriales entre los EEMM con el objetivo de desarrollar de manera conjunta capacidades de defensa.

[422] Directiva 2009/81/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE. Diario Oficial de la Unión Europea. L 216/76 de 20.8.2009. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32009L0081 (23/03/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

1. La primera de ellas se refiere a que la UE *es y sigue siendo un proyecto de paz*, lo cual no implica una visión *naif* del complejo equilibrio político en el que los actores sistémicos, que luchan desaforadamente por el liderazgo mundial, utilizan todos los medios a su alcance para tratar de imponerse. Y la guerra es uno de ellos.
2. Una vez más *Europa se ve obligada a avanzar* en su proyecto de unión política, económica y, esta vez sí, de defensa y seguridad, en un contexto de crisis auspiciado por el actual cambio de paradigma en las relaciones y en el juego de alianzas internacionales. Uno de los aceleradores ha sido, sin duda, la renovación de Donald Trump en el cargo de Presidente de los EE.UU., cuyos posicionamientos diplomáticos y estratégicos nos recuerdan a la Guerra Fría, cuando las dos potencias dominantes se repartían sus zonas de influencia en partes alícuotas que, inexorablemente, condicionaban el futuro de los países a través de la única decisión que podían tomar por sí mismos: el bando con el que se posicionaban. En este sentido, el Libro Blanco de la Defensa representa la decisión que ha tomado Europa de no elegir bando para garantizar la seguridad de los ciudadanos europeos, cuyos principios y valores representa.
3. El *futuro de seguridad y defensa de la Unión está ligado íntimamente al de Ucrania*, de forma que la ambición territorial rusa y su rol de potencia desestabilizadora representa la principal amenaza para la seguridad de toda Europa. Este compromiso debe ser ahora, debe ser decidido y debe mantenerse en el tiempo.

Por todo ello, no nos parece baladí la frase elegida por la Comisión Europea para cerrar el Libro Blanco de la Defensa Europea: *The EU and its Member States must rise to this historic challenge*[423].

3.3.5. Reflexiones sobre la Política Común de Seguridad y Defensa: ¿herbívoros en un entorno de carnívoros?

En el año 2015 el Centre For European Policy Studies (CEPS) iniciaba su informe *More Union in European Defence* señalando que:

> "The Common Security and Defence Policy (CSDP) is the weakest link in the European integration project. Longstanding obstacles block further integration, such as differences between member states in threat perceptions and strategic cultures, divergences in intentions and preferences and, in some cases, lack of mutual trust and solidarity. Yet the Lisbon Treaty demands and permits a great deal more in terms of our common security and defence activities" (BLOCKMANS & FALEG, 2015, pág. 1)[424].

[423] "La UE y sus Estados Miembros deben estar a la altura de este desafío histórico" (traducción propia).

[424] "La Política Común de Seguridad y Defensa es el eslabón más débil en el proyecto de integración europea. Obstáculos que vienen de atrás bloquean aún más la integración, como las diferencias entre los Estados miembros en la percepción de la amenaza y las culturas estratégicas, las divergencias en las intenciones y las preferencias y, en algunos casos, la falta de confianza mutua y solidaridad. Sin embargo, el Tratado de Lisboa exige y permite mucho más en cuanto a nuestras actividades comunes de seguridad y defensa" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Este informe concluía apuntando que era el momento de que los EEMM dieran un paso adelante para formalizar un marco de colaboración militar europeo más eficiente y efectivo aprovechando, como viene siendo habitual en la Unión, las oportunidades que brindan las crisis y los tiempos de cambios.

Podemos convenir que, objetivamente, el Tratado de Lisboa representa el primer impulso firme a la que se bautiza como PCSD por parte de una UE que comienza, en ese momento, a ser consciente de la dimensión de las nuevas amenazas que le conciernen únicamente a ella. Sin embargo, adolece de una falta de concreción y, a nuestro entender, de ambición que le resta efectividad a la hora de alcanzar su verdadero objetivo: la *autonomía estratégica*. Ésta representa la senda, más o menos tortuosa, que la Unión debe andar para llegar a la consideración de actor global en materia de seguridad, lejos de aquel *gigante económico, enano político y gusano militar* que describía, allá por 1991, el ministro de Asuntos Exteriores belga Mark Eyskens.

Pero para recorrer ese camino hasta la *autonomía estratégica*, auténtica clave de bóveda de la seguridad europea, es preciso que la Unión lo haga guiada por una sola voz autorizada en política exterior, respaldada a su vez en el consenso respecto a lo que todos los EEMM consideren *amenazas* y entiendan como *medios y recursos disponibles* para articular las respuestas, esencia misma de la *unidad de percepción* y de la *solidaridad de acción*. Y esto, a su vez, requiere una *voluntad decidida de actuar* aplicando cualquiera de los instrumentos de la amplia panoplia a su alcance, tanto civiles como militares, que pueden operar en el habitual y confortable margen del *soft power* o, llegado el caso, en el más frio e inhóspito del *hard power*.

La madurez en la formación de esta ansiada *identidad europea de defensa* va a seguir necesitando de la ayuda de instituciones como la Agencia Europea de Defensa, en el papel de impulsor -y supervisor- de los esfuerzos armonizadores de desarrollos tecnológicos, adquisición de equipamientos y definición de requerimientos procedimentales, y de instrumentos como la PESCO para optimizar la inversión en proyectos compartidos y avanzar en la disponibilidad del potencial militar y civil de la Unión con el que poder operar en las misiones y operaciones que lo requieran, como el reciente ejemplo del soporte prestado a Ucrania orientado a dar respuesta a las demandas de sistemas de combate y armamento de distinto tipo que "ha subrayado aún más la importancia de la interoperabilidad y la intercambiabilidad entre los Estados miembros. Los proyectos PESCO en curso están adaptando su alcance y sus plazos y están considerando sinergias para responder mejor al cambiante panorama de la seguridad mundial"[425]. En suma, siguiendo la tesis del profesor Coello de Portugal, la PCSD:

> "[…] constituye una importante parte del camino para que los valores de democracia, libertad, Estado de Derecho y protección de los derechos fundamentales propios de la Unión sean respetados en el mundo; y para que la Unión como sujeto político en tránsito hacia la soberanía, sea considerada como

[425] Informe de la EDA sobre desarrollo y ejecución de los proyectos PESCO, de julio de 2023. Disponible en: https://eda.europa.eu/news-and-events/news/2023/07/11/pesco-projects-adapt-and-accelerate-amid-shifting-european-security-landscape-eu-report-finds (30/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> un influyente actor global en la escena internacional del siglo XXI" (COELLO DE PORTUGAL, 2024, pág. 108)

Pero también resulta inevitable avanzar en el *modelo de relación* con la OTAN, cuya égida protectora tanta dependencia y tolerancia ha generado durante años en el metabolismo europeo. El *NATO-first* debe dejar paso a un nuevo formato de vínculo noratlántico basado en un mayor compromiso de la Unión con su propia seguridad, desempeñando un papel de auténtico aliado confiable, fuerte y decidido, pero autónomo respecto a las decisiones que afecten a sus intereses, no siempre coincidentes. Sirva como ejemplo la identificación que de China hacen las respectivas estrategias de EE.UU. y la OTAN como amenaza de seguridad. Así, mientras que EE.UU., de nuevo liderado por Donald Trump, observa con atención a Taiwán y mantiene un frente abierto de feroz competencia sistémica con China, la OTAN mira con recelo su cada vez mayor potencia militar y presencia en el Mar de China Meridional. Por su parte, la UE mantiene con la potencia asiática sustanciales lazos económicos y comerciales que reclaman otra posición geoestratégica, en la que se prioriza como foco de atención de seguridad a Rusia y, como probable en el medio plazo, a África.

África por su parte, respecto al conflicto en Ucrania, se siente marginada "en una guerra tratada como un juego de suma cero en la que no son protagonistas pero sí perdedores natos. Como consecuencia de la ola de desilusión que recorre África, sus gobiernos están tomando decisiones, en el contexto de un futuro incierto, basadas en el interés propio, lo que incluye eludir sanciones y asegurar alianzas con países no occidentales" (FUENTE COBO, 2023, pág. 21), cuestión que sí debe preocupar, y mucho, a la Unión, máxime cuando Rusia está aumentando su presencia en determinadas zonas del Sahel, aprovechando el vacío dejado por anteriores potencias europeas, como Francia.

Este nuevo enfoque de la seguridad y la defensa europea inevitablemente exige que la Unión cuente con capacidades e instrumentos propios que le otorguen un grado de *autonomía tecnológica* suficiente para poder acometer, con garantías, las líneas básicas de sostenimiento de la PCSD y, con ello, dar cuerpo a una defensa creíble europea porque, como señala el Presidente del Consejo, Charles Michel, refiriéndose a la invasión rusa:

> "[…] pensé que Europa estaba viviendo un momento decisivo. Tanto los veintisiete jefes de Estado o de Gobierno como yo mismo constatamos que se trataba de un ataque no solo contra Ucrania, sino también contra nuestro sistema de valores democráticos. Y decidimos apoyar a Ucrania por todos los medios necesarios: humanitarios, financieros e incluso, por primera vez en la historia de la Unión, militares"[426].

[426] Artículo de opinión del presidente Charles Michel, "El mundo mira a nuestro continente europeo", de 5 de octubre de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/10/05/the-world-is-watching-our-european-continent-op-ed-article-by-president-charles-michel/ (30/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Igual pensamiento manifiesta el Presidente francés Emmanuel Macron en su discurso de La Sorbona de abril de 2024[427], cuando señala que la condición *sine qua non* para la seguridad de Europa, actualmente, es que Rusia no gane la guerra de agresión que libra contra Ucrania, por cuanto asistimos a un *cambio de paradigma en materia de seguridad* donde se demuestra que, frente a estos actores desinhibidos y altamente activos en el manejo de amenazas híbridas, la UE debe construir un marco de seguridad y defensa común, creíble e integrado, basado en la colaboración operativa entre los ejércitos europeos, la formación conjunta de sus mandos militares, el impulso de una cultura común de los líderes civiles y la potenciación de las capacidades de ciberseguridad y ciberdefensa. Asumir directamente la responsabilidad de nuestra defensa nos permitirá tomar nuestras propias decisiones y dirigir de manera autónoma nuestra acción estratégica en este sentido.

A tenor de los estudios de opinión púbica que muestran un sentir favorable de los ciudadanos europeos hacia la PCSD y el gasto de sus países en defensa, con una contrastada "comprensión del papel del poder duro y blando en tales políticas" (SCHILDE, ANDERSON, & GARNER, 2019) parece que, de nuevo aprovechando una crisis, Europa definitivamente ha comenzado a creer en la *necesidad de defenderse por sí misma* para proteger sus valores y lo que la democracia representa, máxime cuando en palabras de Josep Borrell al prologar la Brújula Estratégica, "hemos demostrado que estamos dispuestos a pagar el precio por defender nuestra seguridad y la de nuestros socios, el precio de la libertad". Y el precio a pagar por no parecer un herbívoro en un mundo de carnívoros no es barato[428].

Es por todo lo anterior que, en marzo de 2025, se presenta el Libro Blanco como prueba del compromiso de los EEMM con la Unión de la defensa, la cual, como manifiesta la AR/VP Kaja Kallas, *valora su seguridad en base a lo que invierte en ella*[429]. Por ese firme convencimiento en la idea de que solamente la determinación colectiva por construir un proyecto de defensa europeo propio, independiente y autónomo puede garantizar la paz, los principios y la prosperidad de los ciudadanos, se acuerda por la Comisión Europea este paquete de medidas que marcan el camino a seguir con el horizonte temporal de 2030 que, desde luego, no se basa únicamente en la fuerza militar y de las armas, sino en alcanzar la ansiada autonomía estratégica que le asegure a la Unión un futuro como actor estratégico relevante, como proveedor creíble de seguridad y defensa. Papel que, por circunstancias históricas que ya hemos analizado, se había delegado en otros. Parece que, por fin, ha llegado el momento de recuperarlo.

---

[427] Disponible en: https://legrandcontinent.eu/es/2024/04/25/construir-un-nuevo-paradigma-el-discurso-completo-de-emmanuel-macron-en-la-sorbona/ (26/04/2024).

[428] Referencia que hizo el AR/VP Josep Borrell en su conferencia en Madrid, en la Fundación Carlos de Amberes, el martes 11 de octubre de 2022, en el marco de análisis de la guerra en Ucrania. Disponible en: https://elpais.com/internacional/2022-10-11/borrell-en-una-autocritica-a-la-ue-nuestra-prosperidad-estaba-basada-en-la-energia-barata-de-rusia-y-las-oportunidades-de-negocio-con-china.html (30/10/2023).

[429] Cita de la presentación del Libro Blanco de la Defensa Europea y el Plan ReArm Europe – Preparación 2030, el 19 de marzo de 2025, en Bruselas, con la intervención de Úrsula von der Leyen, Presidenta de la Comisión Europea, y Kaja Kallas, Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793 (25/03/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

3.4. La cooperación en el ámbito de la seguridad interior de la Unión Europea

Convienen algunos autores que la seguridad interior ha sido desde los orígenes de las Comunidades Europeas una prioridad en la agenda política comunitaria, "por lo que se ha convertido en un asunto trascendental que siempre ha estado presente en el proceso de integración europea" (ANGUITA OSUNA, 2021, pág. 15). Otros, por el contrario, entienden que durante la primera fase de creación de la Unión Europea "los asuntos relativos a la libertad, seguridad y justicia, siguiendo la terminología actual, no estuvieron incluidos en los ámbitos materiales de la cooperación europea" (ALBALADEJO CAMPOS, 2011, pág. 49).

Por nuestra parte, nos inclinamos a favor de esta segunda postura doctrinal para la cual, mientras que desde sus inicios Europa trataba de avanzar en paralelo en la integración política y económica al tiempo que buscaba conseguir un compromiso de defensa mutua sin la OTAN, la confluencia en el ámbito de la seguridad interior de sus miembros no se consideraba objetivo común estructural, probablemente por las derivadas que ello implicaría en cuanto a la cesión de competencias entroncadas con la esencia de la soberanía y el control de las políticas internas de los EEMM, aferrados aún al carácter formal de aquella que preconiza la negación de toda subordinación del Estado a otro poder superior, convirtiendo el asunto en cuestión espinosa que pudiera echar al traste cualquier negociación que la contemplara en su agenda.

Es por ello que, en nuestra opinión, ese criterio de preservación nacional de lo que se concibe como el *núcleo duro de la soberanía* se ha ido manteniendo como corolario que subyace incluso en el actual TUE, de modo que "la necesidad de emplear el término *política* para referirse a la cooperación policial y judicial está presente en el subconsciente colectivo del sector, pero hasta ahora ni los Tratados ni los Consejos ni el mismo Programa de Estocolmo avalan la existencia de una *política común*" (ARTEAGA MARTÍN, 2010, pág. 4), pudiendo de esta forma concluir que, a fecha de hoy, *no existe una política común de seguridad interior de la UE definida como tal en ninguno de sus Tratados*. Es esta, sin duda, una de las *debilidades* de la actual consideración de la seguridad europea que, a nuestro parecer, debe evolucionar en clave de *fortaleza* para que el proyecto de construcción soberana y autonomía estratégica que tanto ansía la Unión pueda consolidarse en el actual contexto global del siglo XXI.

No obstante, dicho lo anterior, hay que destacar que la cooperación en materia judicial y policial entre los miembros de la UE se inicia hace más de cuarenta años en el marco de las relaciones intergubernamentales como "Trevi, Schengen y Prüm, cuyos logros se han comunitarizado después de mostrar su eficacia. Por su parte, la Comisión ha ido asumiendo el ejercicio de esas nuevas competencias comunitarias relacionadas con el control en las fronteras, el asilo, la inmigración y la cooperación judicial" (ARTEAGA MARTÍN, 2010, pág. 1).

Ediciones Universidad de Salamanca | CC BY-NC-ND

3.4.1. Surgimiento y arraigo de la colaboración policial en la UE

Este carácter colaborativo a nivel bilateral o multilateral entre los EEMM en el ámbito de la Justicia y de los Asuntos de Interior (JAI) ya se atisba en el Consejo Europeo de Roma de diciembre de 1975 en el que, desde un prisma económico y centrado exclusivamente en los trabajadores, se plantea como objetivo la libre circulación de las personas (GARCÍA SAN PEDRO, 2006, pág. 201), y se acuerda proseguir con los trabajos "para la supresión de los controles fronterizos y la armonización de las condiciones de entrada y estancia en los Estados miembros", estipulando la adopción de "una propuesta del Primer Ministro del Reino Unido para que los Ministros de Interior de la Comunidad, o los ministros con similares responsabilidades, se reúnan para debatir asuntos relevantes de su competencia, en particular en materia de orden público"[430]. Meses después, esas relaciones intergubernamentales entre los Ministros de Interior y Justicia de los EEMM están funcionando en el marco del denominado Grupo de Trevi y tienen reflejo en las actas del Consejo que les anima "a continuar con sus actividades"[431], fijando expresamente la lucha contraterrorista como una de las prioridades de la cooperación.

El Grupo de Trevi era una "estructura informal de cooperación intergubernamental en el ámbito policial en la que se reunían periódicamente los ministros de Interior o Justicia de los Estados miembros de la Unión Europea hasta el Tratado de Maastricht. Acordada en el Consejo Europeo de Roma de diciembre de 1975, debe su nombre a la fontana de Trevi romana"[432], según precisa el Diccionario panhispánico del español jurídico. Otros autores, no obstante, consideran que su nombre se deriva del acrónimo en inglés de *Terrorism, Radicalism, Extremism and International Violence* (DÍAZ FERNÁNDEZ A. M., 2012, pág. 164). Sea como fuere, este foro servía a los representantes de los Estados participantes para intercambiar experiencias e información y ponerse de acuerdo para la aplicación de las medidas que adoptaban en los ámbitos de la lucha contra el terrorismo y el crimen organizado, siendo así que el Grupo de Trevi "a través de sus reuniones regulares proporcionó a las fuerzas policiales europeas el marco necesario para poder comunicarse e intercambiar información sobre crímenes transfronterizos así como compartir mejores prácticas para afrontarlas" (DÍAZ FERNÁNDEZ A. M., 2012, pág. 164).

En 1986 el Acta Única Europea[433] modifica los Tratados constitutivos de las Comunidades Europeas marcando una estrategia de cohesión económica y social a través de la consecución de un mercado único interior, entendido como un espacio libre de fronteras interiores y con libertad de circulación para personas, mercancías, servicios y capitales. Al mismo tiempo, la seguridad común sigue circunscrita a la perspectiva de

[430] Acta del Consejo Europeo de Roma de 1975. Disponible en: https://www.consilium.europa.eu/media/20809/1975_december_rome__eng_.pdf (12/11/2023).
[431] Acta del Consejo de Bruselas de 1976. Disponible en: https://www.consilium.europa.eu/media/20797/bruxelles_july_1976__eng_.pdf (12/11/2023).
[432] Disponible en: https://dpej.rae.es/lema/grupo-de-trevi (12/11/2023).
[433] El Acta Única Europea fue firmada el 28 de febrero de 1986 y entró en vigor el 1 de julio de 1987. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:11986U/TXT (14/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la política exterior, donde se busca una mayor coordinación de las posiciones de los EEMM a través de la Comisión de Ministros de Asuntos Exteriores en el marco de la Cooperación Política Europea, mientras que los ámbitos de justicia y asuntos de interior, que no reciben referencia expresa alguna, permanecen en la esfera de la cooperación intergubernamental. "A raíz del Acta Única, los Estados miembros crearon, siempre al margen del marco comunitario, nuevos grupos de trabajo en función de sus necesidades, tales como el grupo *ad hoc* «inmigración» en 1986, el Comité Europeo de Lucha contra la Droga (CELA) en 1989, o el Grupo de Ayuda Mutua (GAM), encargado de cuestiones aduaneras" (GARCÍA SAN PEDRO, 2006, pág. 202).

Pero las dificultades para hacer realidad tanto la libre circulación de las personas como el espacio sin fronteras interiores en el territorio de la Unión, que al fin y al cabo son avances estrechamente vinculados entre otros a la coordinación para afrontar el terrorismo y la delincuencia transfronteriza, llevan a que en junio de 1985 Francia, Alemania, Países Bajos, Bélgica y Luxemburgo firmen el Acuerdo de Schengen[434] que, cinco años más tarde, se complementa con su Convenio de Aplicación[435] para consolidar el desarrollo de un espacio común a través de la unificación de la política de visados, inmigración y asilo, y la cooperación policial y judicial en materia penal.

Respecto a la cooperación policial merece ser destacado el cariz operativo de Schengen por cuanto, por un lado, reúne instrumentos como los oficiales de enlace, las vigilancias y seguimientos transfronterizos, las entregas controladas y los equipos conjuntos de investigación y, por otro, dispone el intercambio de información para compensar la ausencia de controles fronterizos a través de una base de datos compartida por todos los firmantes, el Sistema de Información Schengen (SIS)[436] y su estructura de

[434] Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985. Diario Oficial de la Unión Europea L239/1, Consejo de 22/09/2000. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:42000A0922(02) (15/11/2023).

[435] Convenio de Aplicación del Acuerdo de Schengen, firmado el 19 de junio de 1990. Diario Oficial de la Unión Europea L239/1, Consejo de 22/09/2000. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:42000A0922(02) (15/11/2023).

[436] El Sistema de Información de Schengen (SIS), cuya base de datos central se ubica físicamente en Estrasburgo (National Schengen Information System – CSIS), es el sistema de intercambio de información para la protección de la seguridad de las fronteras europeas. Al no existir fronteras interiores, el SIS funciona como el necesario instrumento de cooperación entre las autoridades de vigilancia de fronteras y de inmigración, la policía y las autoridades aduaneras y judiciales de la UE y de los países asociados a Schengen. La responsable de la supervisión y de la evaluación del sistema, así como del funcionamiento del SIS y la red de oficinas nacionales SIRENE es la Comisión Europea. La gestión operativa del SIS corre a cargo de la Agencia de la UE para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud (eu-LISA), que también gestiona otros sistemas como EURODAC -gestión de solicitudes de asilo y refugio- y el VIS -Sistema de Información de Visados-. Por su parte, cada país es responsable de la creación de su propia estructura nacional (National Schengen Information System –NSIS), del funcionamiento y del mantenimiento del SIS en su ámbito, así como de disponer de una ley de Protección de Datos de carácter personal. En 2013, se implementó el SIS II con nuevas funcionalidades, como la posibilidad de añadir impresiones dactilares y fotografías a las descripciones, y en marzo de 2023 se implementaron capacidades más actualizadas conforme a la evolución tecnológica en campos como los datos biométricos para verificar la identidad de las personas registradas en el sistema, las descripciones de personas relacionadas con delitos de terrorismo, la emisión de descripciones relativas a personas vulnerables o desaparecidas, la gestión de las decisiones de retorno para personas que se encuentren ilegalmente en la

Ediciones Universidad de Salamanca | CC BY-NC-ND

funcionamiento auxiliar a través de las Oficinas Nacionales SIRENE[437], a la vez que se regula la protección de los datos de carácter personal en él recogidos junto con la garantía de su custodia (OUTRIVE, 2001, págs. 45-46). En noviembre de 1990 se adhiere al convenio Italia, en junio de 1991 lo hacen España[438] y Portugal, y en noviembre de 1992 hace lo propio Grecia, comenzando la aplicación real y efectiva del Espacio Schengen en marzo de 1995, momento en que siete de los países firmantes[439] suprimen definitivamente las fronteras interiores para dar lugar a ese espacio común[440], por el que cualquier persona que resida o haya cruzado regularmente las fronteras exteriores de cualquiera de los Estados asociados puede circular libremente sin controles fronterizos.

Parece razonable entender por todo ello que estos acuerdos "supusieron una verdadera *revolución* para el concepto tradicional de seguridad de los Estados, abriendo paso a nuevas formas avanzadas de cooperación policial, judicial penal, política de visados, etc." (ALBALADEJO CAMPOS, 2011, pág. 50), que fueron concebidas como medidas compensatorias necesarias para, por un lado, mantener la seguridad de este Espacio

UE, o la cooperación ampliada al registro de embarcaciones, aeronaves y armas de fuego. Su funcionamiento y condiciones de utilización se acogen a lo establecido en el Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.o 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56). Disponible en: https://www.boe.es/doue/2018/312/L00056-00106.pdf (16/11/2023).

[437] El acrónimo SIRENE corresponde a Supplementary Information Request at the National Entry (solicitud de información complementaria a la entrada nacional), y se corresponde con la red conformada por las oficinas nacionales de cada uno de los países miembros, llamadas Oficinas SIRENE, únicos puntos de contacto a efectos de consulta de datos, operativas 24x7x365 para responder al intercambio de información en el marco del SIS, y también actúan como punto nacional de contacto de Prüm. Hay una Oficina Nacional por cada uno de los países –en España está integrada en la División de Cooperación Internacional de la Dirección General de la Policía- y Europol también dispone de una. Respecto a sus competencias, entre otras, a las oficinas SIRENE les corresponde validar y suministrar información adicional sobre las descripciones relativas a personas buscadas para su detención, supervisar la calidad de los datos y la compatibilidad de las descripciones, coordinar las actividades transfronterizas relacionadas con las descripciones del SIS, tramitar las solicitudes de acceso a los datos personales, y contactar con el país que haya emitido la descripción cuando se produzca una coincidencia y se hayan emprendido las acciones requeridas o cuando no sea posible emprender las acciones requeridas.

[438] España firma el Convenio Schengen el 25 de junio de 1991 y fija consideraciones específicas sobre las ciudades autónomas de Ceuta y Melilla, para las que estipula un régimen de exención de visados en materia de pequeño tráfico fronterizo con las provincias marroquíes de Tetuán y Nador.

[439] Francia, Alemania, Bélgica, Luxemburgo, Países Bajos, Portugal y España.

[440] En la actualidad forman parte del espacio Schengen Alemania, Austria, Bélgica, Croacia, Dinamarca, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Islandia, Italia, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, República Checa, República Eslovaca, Suecia y Suiza. El 30 de diciembre de 2023 la UE acuerda por unanimidad la entrada gradual de Rumanía y Bulgaria en el espacio Schengen, siendo a partir del 31 de marzo de 2024 cuando se eliminan los controles de fronteras interiores aéreas y marítimas, manteniéndose los controles por tierra temporalmente a expensas de la negociación con Austria. Disponible en: https://es.euronews.com/2024/03/28/rumania-y-bulgaria-se-uniran-parcialmente-al-espacio-schengen-de-europa-el-domingo
https://elpais.com/internacional/2024-03-30/rumania-y-bulgaria-inician-una-entrada-parcial-en-el-espacio-schengen-por-las-reticencias-de-austria.html (1/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Schengen sin fronteras interiores y, por otro, reforzar el control de acceso por sus fronteras exteriores.

En 1992, tres años antes de que comenzase la aplicación de Schengen, el Tratado de Maastricht redefine la construcción de la UE asentándola en tres pilares: un Primer Pilar con las competencias comunitarias transferidas por los EEMM para hacer efectiva la integración política y económica, un Segundo Pilar de carácter intergubernamental para avanzar en la Política Exterior y de Seguridad Común, y un Tercer Pilar, también de naturaleza intergubernamental, para la cooperación en los ámbitos de la justicia y de los asuntos de interior[441]. Esta cooperación JAI se organiza en torno a nueve cuestiones que se consideran de interés compartido: la política de asilo, el cruce de las fronteras exteriores, la inmigración, las drogodependencias, el fraude internacional, la cooperación judicial en materia civil y penal, la cooperación aduanera y la cooperación policial en materia de terrorismo, drogas y crimen organizado transnacional "incluidos, si es necesario, determinados aspectos de la cooperación aduanera en conexión con la organización, a escala de la Unión, de un sistema de intercambios de información dentro de una Oficina Europea de Policía (Europol)"[442], dando así comienzo la andadura de esta agencia de la Unión, con sede en La Haya, responsable de coadyuvar a la cooperación policial entre los EEMM y de apoyar sus investigaciones contraterroristas y de criminalidad organizada.

Para irle dando forma y contenido a esta encomienda se crea inicialmente la Unidad de Drogas de Europol[443], con la tarea de analizar e intercambiar información sobre actividades delictivas concretas que afecten al menos a dos EEMM y, en relación con ellas, colaborar con los servicios policiales competentes. Posteriormente se van ampliando estas capacidades a la lucha contra el tráfico ilícito de drogas y materiales radiactivos y nucleares, la trata de seres humanos, la inmigración clandestina, el tráfico ilícito de vehículos y el blanqueo de capitales asociado al crimen organizado. En julio de 1995 el Consejo firma el Convenio Europol por el que se crea la Oficina Europea de Policía[444], instrumento de genuina cooperación horizontal entre EEMM y embrión de la sólida agencia en la que hoy se ha convertido Europol, que entra plenamente en funcionamiento con la definición del espacio de libertad, seguridad y justicia que

[441] Así se denomina el Título VI del TUE aprobado en Maastricht el 7 de febrero de 1992: Disposiciones relativas a la cooperación en los ámbitos de la justicia y de los asuntos de interior.

[442] Así se recoge literalmente en el artículo K.1.9) del TUE firmado en Maastricht. Diario Oficial de las Comunidades Europeas 92/C 191/01. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:1992:191:FULL&from=LV (15/11/2023).

[443] La Unidad de Drogas de Europol estuvo operativa desde marzo de 1995 hasta julio de 1999, fecha en que es sustituida por Europol. Se recoge en la Acción Común 95/73/JAI, de 10 de marzo de 1995, relativa a la Unidad de Drogas de Europol. Diario Oficial de las Comunidades Europeas L 62 de 20.3.1995. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:l14005a (15/11/2023).

[444] Acto del Consejo, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol). Diario Oficial de las Comunidades Europeas C 316, de 27 de noviembre de 1995. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:1995:316:FULL&from=EL (17/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

establece el Tratado de Ámsterdam y la decidida apuesta que por ella se hace como instrumento para operativizar dicha cooperación policial[445].

La entrada en vigor el 1 de mayo de 1999 del Tratado de Ámsterdam comporta importantes novedades en relación con la materia objeto de estudio. En cuanto a lo concerniente al Tratado de la Unión Europea (TUE), en su nuevo Título VI[446] se abandona la referencia a la cooperación en el ámbito JAI para pasar a definir un objetivo más ambicioso centrado en ofrecer a sus ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia (ELSJ) mediante una cooperación policial y judicial más estrecha entre los EEMM manteniendo, eso sí, esta acción común dentro del tercer pilar. Esta novedosa y más amplia visión de la cooperación supone un compromiso de los socios para que la Unión "ponga los medios necesarios para, primero, que se respeten en su territorio los derechos y libertades fundamentales, segundo, que los ciudadanos puedan circular y residir libremente y, tercero, que se mantengan y desarrollen una buenas condiciones en materia de seguridad para las personas luchando contra la delincuencia, incluidos fenómenos como el terrorismo o el tráfico de drogas" (LUENGO ALFONSO, 2000, pág. 125). A estos efectos se contempla incluso la cooperación reforzada, siempre que la misma impulse los objetivos de la Unión, proteja y sirva a sus intereses para avanzar hacia el pretendido ELSJ[447]. No obstante, este Tercer Pilar sufre relevantes modificaciones en su contenido, como la transferencia de las cuestiones de visados, asilo, inmigración y cooperación judicial en materia civil al pilar comunitario, quedando ahora recogidas en el Tratado Constitutivo de la Comunidad Europea (TCE)[448]. Otra significativa consecuencia lograda en Ámsterdam es la integración del acervo de Schengen en los Tratados[449], aunque sin lograr un régimen jurídico y de aplicación único por las particularidades de algunos EEMM[450].

El Consejo Europeo de Tampere, celebrado a propuesta española entre el 15 y el 16 de octubre de 1999, se aplica en exclusiva a la creación del ELSJ por cuanto "los Jefes de Estado y de Gobierno habían constatado que, mientras en otros ámbitos se había progresado de forma sustancial en el proceso de integración europea, la consecución de este objetivo requería un impulso político al más alto nivel" (GARCÍA SAN PEDRO, 2006, pág. 204), lo que lleva al Consejo Europeo a invitar al resto de Instituciones de la Unión

[445] Artículo K.2.2 del Tratado de Ámsterdam por el que se modifican el Tratado de la Unión Europea, los Tratados Constitutivos de las Comunidades Europeas y determinados actos conexos, firmado el 2 de octubre de 1997. Publicado en Diario Oficial de las Comunidades Europeas 97/C 340/01. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:1997:340:FULL (17/11/2023).

[446] El Título VI del TUE firmado en Ámsterdam es el de "Disposiciones relativas a la cooperación policial y judicial en materia penal", y engloba del artículo K.1 al K.14.

[447] Título VI bis del TUE "Disposiciones sobre una cooperación reforzada", del articulo K.15 al K.17.

[448] Título III bis del TCE "Visados, inmigración y otras políticas relacionadas con la libre circulación de personas".

[449] La incorporación del Acuerdo y el Convenio Schengen al TUE y TCE se lleva a cabo con un "Protocolo anejo por el que se integra el acervo de Schengen en el marco de la Unión Europea". El acervo de Schengen tal como figura en el apartado 2 del artículo 1 de la Decisión 1999/435/CE del Consejo, de 20 de mayo de 1999, es publicado en el Diario Oficial de la Unión Europea L 239 de 22 de septiembre de 2000. Disponible en: https://publications.europa.eu/resource/cellar/b3ff51f8-d0c0-4370-bfc3-39de639a93a2.0005.05/DOC_1 (18/11/2023).

[450] Irlanda, UK y Dinamarca.

Ediciones Universidad de Salamanca | CC BY-NC-ND

a promover la aplicación plena e inmediata del Tratado de Ámsterdam como una de sus prioridades políticas, con los objetivos de desarrollar una política común de asilo y migración con un enfoque global en el que se contemple la gestión de los flujos migratorios y la colaboración con los países de origen, alcanzar un auténtico Espacio Europeo de Justicia a través del reconocimiento mutuo de resoluciones judiciales y la mayor convergencia legislativa, la lucha contra la delincuencia organizada y transnacional grave -con especial atención al blanqueo de capitales-, y la integración de los temas de justicia y asuntos de interior en otras políticas de la Unión, en concreto de la acción exterior[451]. El desarrollo del programa de Tampere permitió el establecimiento de dos herramientas fundamentales de cooperación en materia de terrorismo y delincuencia grave: la orden europea de detención y entrega (OED)[452] y los equipos conjuntos de investigación (ALBALADEJO CAMPOS, 2011, pág. 55).

Este impulso decidido al ELSJ se proyecta seguidamente en el Tratado de Niza[453], firmado en febrero de 2001 y en vigor desde febrero de 2003, principalmente orientado a la preparación de las estructuras institucionales de cara a la ampliación de la UE que consolida el Tratado de Atenas[454], siendo su cuestión más relevante la carta de naturaleza que se otorga a la European Union Agency for Criminal Justice Cooperation (Eurojust)[455], para el fomento de la colaboración de las autoridades judiciales en materia penal a través de acciones como la facilitación de la extradición entre EEMM, la prevención de conflictos de jurisdicción o el acuerdo en los elementos básicos de los tipos delictivos y las penas asociadas para la delincuencia organizada, el terrorismo y el tráfico ilícito de drogas.

Ese espíritu animoso y expansionista de Europa se retroalimenta con la adhesión de los nuevos EEMM que firman el Tratado de Atenas[456], los cuales proporcionan a la Unión una diversidad cultural claramente enriquecedora y un mayor peso específico en el contexto internacional pero, también, un impacto en la seguridad interior de la UE

[451] Conclusiones de la Presidencia, Consejo Europeo de Tampere 15 y 16 de octubre de 1999. Disponible en: https://www.europarl.europa.eu/summits/tam_es.htm (18/11/2023).

[452] La orden europea de detención y entrega crea desde enero de 2004 un nuevo procedimiento judicial transfronterizo, simplificado y sin intervención del Ejecutivo, que permite la entrega de personas, incluso de nacionales, a efectos de enjuiciamiento o de ejecución de una pena, superando con ello muchas de las limitaciones propias del tradicional procedimiento de extradición. Disponible en: https://e-justice.europa.eu/content_european_arrest_warrant-90-es.do (18/11/2023).

[453] Tratado de Niza por el que se modifica el Tratado de la Unión Europea, los Tratados Constitutivos de las Comunidades Europeas y determinados actos conexos, firmado en Niza el 26 de febrero de 2001. Publicado en Diario Oficial de las Comunidades Europeas 2001/C 80/01, de 10 de marzo de 2001. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2001:080:FULL&from=PT (18/11/2023).

[454] El Tratado de Atenas entra vigor el 1 de mayo de 2004 y supone la mayor ampliación de la UE hasta la fecha con la adhesión de República Checa, Hungría, Polonia, Eslovaquia, Eslovenia, Lituania, Letonia, Estonia, Chipre y Malta.

[455] Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (DO L63 de 06/03/2002). Posteriormente es sustituida por el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (DO L 295/138 de 21/11/2018). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1727 (18/11/2023).

[456] República Checa, Hungría, Polonia, Eslovaquia, Eslovenia, Lituania, Letonia, Estonia, Chipre y Malta.

Ediciones Universidad de Salamanca | CC BY-NC-ND

facilitado por la ausencia de controles en las fronteras internas de la mayor parte de su territorio (SIMANCAS, 2003, pág. 38).

Consciente de ello, el Consejo Europeo acuerda en el Programa de La Haya de noviembre de 2004 las diez prioridades de la Unión para reforzar el ELSJ en los siguientes cinco años, entre ellas, la lucha contra el terrorismo tanto desde el plano preventivo como reactivo, la gestión de la migración con un enfoque común europeo que atienda a delitos conexos como el contrabando y la trata de seres humanos, o el intercambio transfronterizo de información entre los servicios de seguridad bajo el principio de disponibilidad[457]. Para alcanzar este objetivo deben aprovecharse las nuevas tecnologías disponibles y desarrollar bases de datos centralizadas a escala europea que supongan un valor añadido a la cooperación policial, para poder intercambiar con agilidad y eficiencia la información necesaria y proceder a operativizarla.

En este contexto de impulso europeista y sobre las propuestas de la Convención Europea sobre el futuro de Europa[458], el Consejo Europeo y el Parlamento Europeo aprueban en 2004 el Proyecto de Tratado por el que se instituye una Constitución para Europa[459] que, finalmente, fracasa por el rechazo en los referéndums de ratificación de Francia y Países Bajos en 2005. Días antes de estas dos consultas plebiscitarias, el 27 de mayo de 2005, Alemania, Francia, España, Países Bajos, Bélgica, Luxemburgo y Austria firman el Tratado de Prüm[460] para, desde los principios de la confianza mutua y de la disponibilidad de la información[461], fortalecer la cooperación policial en ámbitos sensibles como el intercambio de datos de los ficheros de ADN, dactiloscópicos y de matriculación de vehículos, la prevención en grandes actos o eventos de dimensión transfronteriza, la lucha contra el terrorismo, la inmigración ilegal y la colaboración operativa transfronteriza sobre la base de lo estipulado en Schengen (ZILLER, 2007, págs. 22-23).

[457] Conforme al considerando 4 de la Decisión 2008/615/JAI del Consejo de 23 de junio de 2008 sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, el principio de disponibilidad significa que el agente de los servicios de seguridad de un Estado miembro de la Unión que necesite información para llevar a cabo sus funciones debe poder obtenerla de otro Estado miembro, y que las autoridades de los servicios de seguridad del Estado miembro que tenga dicha información deben ponerla a su disposición para el fin declarado, teniendo en cuenta las necesidades de las investigaciones pendientes en dicho Estado miembro.

[458] La Convención Europea sobre el futuro de Europa se convoca por el Consejo Europeo celebrado en Laeken en diciembre de 2001, con el objetivo de estudiar las posibles vías de avance en común de la Unión a corto, medio y largo plazo, entre ellas la elaboración de una Constitución Europea.

[459] Proyecto de Tratado por el que se instituye una Constitución para Europa. Diario Oficial de la Unión Europea 2003/C 169/01, de 18 de julio de 2003. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52003XX0718(01)&qid=1700322244878 (18/11/2023).

[460] Como señala Jacques Ziller, el Tratado de Prüm es *una verdadera-falsa cooperación reforzada* porque aunque no cumple con los requisitos formales que establece el artículo 20.2 TUE, como el número de Estados miembros –al menos nueve-, sin embargo por su contenido y objetivo pretendido responde a dicho formato y puede considerarse una verdadera cooperación reforzada.

[461] El principio de disponibilidad de la información conlleva que los servicios policiales se obligan a compartir la información de que dispongan a requerimiento, salvo que concurra alguna de las causas expresamente acordadas para no hacerlo.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En junio de 2008, apenas tres años después de su firma, el Consejo adopta la conocida como Decisión Prüm[462], para incorporar al marco jurídico de la Unión los aspectos esenciales del referido Tratado, siendo ésta la base para avanzar en proyectos de diverso tipo y alcance como, por ejemplo, el de Comisarías Europeas a través del que "se establecen acuerdos entre los diferentes países firmantes para organizar patrullas conjuntas en distintos territorios europeos durante breves periodos de tiempo" (CRISTIAN VELILLA, 2022, pág. 21), principalmente en periodos vacacionales o con motivo de dispositivos específicos para atender a concentraciones masivas de público, mediante agentes que portan su uniformidad reglamentaria para favorecer la visibilidad ante los ciudadanos de sus respectivos países[463] y prestar así un servicio de proximidad y calidad.

3.4.2. El Tratado de Lisboa y la comunitarización del Tercer Pilar

El jarro de agua fría que supone el descalabro de la Constitución Europea no impide que en diciembre de 2007, tras un periodo de análisis y reflexión horizontal sobre los retos futuros que quiere asumir la Unión, se salve la mayor parte de ese proyecto constitucional y se esquive aquella otra que pudo llevar a su fracaso, culminando con la firma del Tratado de Lisboa que, a modo de alternativa edulcorada del malogrado Tratado de Roma, entra en vigor el 1 de diciembre de 2009 tras ser ratificado por los veintisiete Estados miembros. El *Tratado de la Unión Europea* (TUE) y el *Tratado de Funcionamiento de la Unión Europea* (TFUE) que se aprueban en Lisboa son las actuales normas de referencia que comunitarizan y consolidan definitivamente las políticas del espacio de libertad, seguridad y justicia, *suprimiendo definitivamente la antigua estructura de pilares para la colaboración JAI*, lo que conlleva, entre otras, dos consecuencias relevantes "como son una mayor participación del Parlamento Europeo en los asuntos de interior, así como que ya no será necesario aplicar en estas decisiones la regla de la unanimidad para avanzar y llegar a acuerdos en las materias de seguridad, salvo en cuestiones muy específicas como los aspectos eminentemente operativos" (VILLALGORDO GARCÍA, 2011, pág. 32)

La firme apuesta que la Unión hace por su seguridad interior tiene reflejo en el respaldo económico de las acciones que permiten avanzar en la defensa del ELSJ, a través de distintos instrumentos cuyos principales exponentes son el Fondo de Seguridad Interior (FSI) y el Fondo de Asilo, Migración e Integración (FAMI)[464]. Estos fondos se gestionan a

[462] Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. Diario Oficial de la Unión Europea L210/1 de 06/08/2008. Disponible en: eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008D0615
Al tiempo, el Consejo adopta la Decisión 2008/616/JAI, de igual fecha, relativa a la ejecución de la anterior. Diario Oficial de la Unión Europea L210/12 de 06/08/2008. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:ES:PDF (21/11/2023).

[463] Estos acuerdos comienzan por parte de España en el año 2008 con la Policía francesa, siguiendo en el año 2012 el acuerdo con la Policía de Segurança Pública Portuguesa, en el año 2014 con la Polizia di Stato italiana, en el 2020 con la Landespolizei alemana y en 2022 con la Politie de Países Bajos.

[464] Otros mecanismos de financiación son las Acciones Específicas para acometer la compra de equipos y medios, las Acciones de Emergencia para hacer frente a acontecimientos extraordinarios no previstos, y

Ediciones Universidad de Salamanca | CC BY-NC-ND

través de programas plurianuales gestionados conjuntamente por la Comisión Europea y los EEMM, que deben designar una autoridad nacional responsable para la gestión y el control de la ejecución de los proyectos, representada en España por la Subdirección General de Planificación y Gestión de Infraestructuras y Medios para la Seguridad (SGPGIMS), dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior (GARCÍA & TIRADO, 2022, págs. 4-15). El FSI[465] en concreto tiene como objetivo político contribuir a la seguridad de la Unión financiando dos tipos de proyectos: los que ayuden a desarrollar la política europea de visados, el control fronterizo y la lucha contra la inmigración ilegal, que se financian con el denominado *FSI Fronteras y Visados*; y aquellos otros que fomenten la cooperación transfronteriza a través de la prevención y la lucha contra el terrorismo y la radicalización, la delincuencia grave y organizada y la ciberdelincuencia, que reciben financiación del conocido como *FSI Policía*[466]. Por su parte, el FAMI[467] contribuye al refuerzo y desarrollo de la política común de asilo e inmigración y la aplicación de los principios de solidaridad y reparto de responsabilidades entre los EEMM y de cooperación con terceros Estados. Sus objetivos de financiación alcanzan tanto a la dimensión exterior de la lucha contra la inmigración ilegal, como a la atención de las necesidades económicas y sociales derivadas de la acogida e integración de los migrantes llegados a suelo europeo.

Respecto a la base jurídica del ELSJ debemos dirigirnos a ambos Tratados. La primera referencia es el artículo 3 TUE que, al enunciar los grandes objetivos de la Unión, le otorga a este concepto una prioridad de la que no disponía en los Tratados de Niza y Ámsterdam, estableciendo que "la Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores"[468], al tiempo que define sus componentes esenciales: la eliminación de las fronteras interiores, la garantía de la libre circulación de personas, la prevención y lucha contra la delincuencia y la definición de una política común para el control de las fronteras exteriores, el asilo y la inmigración.

las Acciones de la Unión con las que la Comisión dirige el programa de acción que específicamente quiere subvencionar para alcanzar sus objetivos de seguridad.

[465] El FSI para el Marco Financiero Plurianual 2021-2027 tiene un presupuesto de 1.931 millones de euros, de los que España cuenta con una asignación inicial de casi 85 millones. Disponible en: https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-de-seguridad-interior/ (18/11/2023).

[466] En el FSI hay acciones específicas como, por ejemplo, la de *Fraude de Medios de Pago* destinada a financiar la cooperación policial internacional en esta materia, el intercambio de información, la asistencia a víctimas y las acciones de prevención al fraude. Otra acción específica del FSI es la de *Crimen Organizado*, con seis áreas temáticas dedicadas a la mejora de la inteligencia sobre redes criminales, el favorecimiento de las investigaciones transfronterizas, de las investigaciones financieras, de las medidas de prevención del crimen organizado, de la lucha contra el tráfico de drogas y contra la trata de seres humanos.

[467] El FAMI para el Marco Financiero Plurianual 2021-2027 tiene un presupuesto de 9.882 millones de euros, contando España con una asignación inicial de más de 482 millones. Disponible en: https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-asilo-migracion-e-integracion/ (18/11/2023).

[468] El artículo 3.2 TUE señala que "La Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia".

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por su parte, el TFUE en el artículo 4 declara la naturaleza de competencia compartida del ELSJ[469], y en el Título V[470] procede a su desarrollo normativo a través de cinco capítulos en los que atiende a materias dedicadas, respectivamente, a disposiciones generales, a las políticas sobre controles en las fronteras, asilo e inmigración, a la cooperación judicial en materia civil, a la cooperación judicial en materia penal y a la cooperación policial.

En relación con el objeto de nuestro estudio deben señalarse varias cuestiones relevantes que contempla el Título V TFUE. La primera de ellas es la puesta en valor que en el artículo 67 TFUE se hace del respeto a los derechos fundamentales y a los distintos sistemas jurídicos de los EEMM, la garantía de la ausencia de controles en las fronteras interiores y el desarrollo de una política común de asilo, inmigración y fronteras, la garantía de un elevado nivel de seguridad sobre la base de la colaboración policial y judicial en materia penal, y la tutela judicial efectiva a través de la garantía principal del reconocimiento mutuo de las resoluciones judiciales y extrajudiciales en materia civil.

Seguidamente, el artículo 68 TFUE estipula la competencia del Consejo Europeo para definir la orientación estratégica del ELSJ, mientras que el artículo 70 adjudica al Consejo la capacidad de establecer el procedimiento para la evaluación de la aplicación por los EEMM de las políticas de la Unión en el marco del ELSJ.

Se crea en el artículo 71 TFUE el Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI)[471], para garantizar la eficaz coordinación y cooperación policial y de gestión de fronteras, llevar a cabo la evaluación de la amenaza y de las prioridades nacionales y de la Unión en cada ciclo político, preparar, supervisar y aplicar la estrategia de seguridad interior, coordinar y supervisar a los grupos de trabajo del ámbito JAI del Consejo y potenciar la cooperación y la coordinación entre la seguridad interior y la seguridad exterior a través del COPS (SÁNCHEZ PELÁEZ, 2021, pág. 148). El COSI está integrado por altos funcionarios de los Ministerios de Justicia o Interior de cada EEMM, junto con representantes de la Comisión y del SEAE. Su ciclo político es de cuatro años y, para ser alcanzadas durante el mismo, define una serie de prioridades estratégicas con sus correspondientes planes de desarrollo operativo, para lo que se muestra esencial la cooperación y coordinación de las distintas agencias JAI[472] a través de reuniones periódicas y del establecimiento de procedimientos y métodos de trabajo consensuados. En este sentido, han representado objetivos prioritarios de la agenda del COSI desde sus inicios en 2011 el terrorismo, el crimen organizado, la trata de seres humanos y el tráfico ilícito de personas, el fraude fiscal intracomunitario, las

[469] El artículo 4.2.j TFUE dispone que "Las competencias compartidas entre la Unión y los Estados miembros se aplicarán a los siguientes ámbitos principales: j) el espacio de libertad, seguridad y justicia".
[470] El Título V TFUE "Espacio de libertad, seguridad y justicia", ocupa del artículo 67 al 89, tratando cuestiones antes dispersas entre el Título IV del Tratado de Roma (TCE) y el Título VI del Tratado de Ámsterdam (TUE).
[471] El artículo 71 TFUE se desarrolla a través de la Decisión del Consejo de 25 de febrero de 2010 por la que se crea el Comité permanente de cooperación operativa en materia de seguridad interior. Diario Oficial de la Unión Europea L52/50 de 03/03/2010. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010D0131&qid=1700337686330 (18/11(2023).
[472] La Red de Agencias JAI la componen nueve organismos de la UE del ámbito de justicia y asuntos de interior.

Ediciones Universidad de Salamanca | CC BY-NC-ND

operaciones financieras delictivas, el fraude documental, el tráfico de estupefacientes, la ciberdelincuencia y los delitos medioambientales (SÁNCHEZ PELÁEZ, 2021, pág. 150).

A continuación, los artículos 72 y 73 TFUE confirman una de las cuestiones esenciales de la estructura de funcionamiento de la Unión: el mantenimiento del orden público, la salvaguarda de la seguridad interior y la protección de la seguridad nacional siguen constituyendo una *responsabilidad exclusiva de cada uno de los EEMM*. Sobre esta premisa se construye, desde sus inicios y hasta ahora, la seguridad interior de la Unión.

También es relevante el desarrollo que el artículo 85 TFUE hace de las funciones de la agencia Eurojust[473], dentro de la Red de agencias JAI, destinada a reforzar la coordinación y la cooperación entre las autoridades policiales y judiciales, tanto de los EEMM como de terceros países con acuerdos de colaboración, en los casos de delincuencia organizada grave y transnacional en que se solicite su intervención a instancia de la autoridad competente nacional, cuando el delito afecte a dos o más EEMM, a un EEMM y a un tercer Estado, o a la propia UE. En la práctica Eurojust "centra su actividad en una serie de ámbitos prioritarios, por ser los delitos identificados por el Consejo como de mayor riesgo para la Unión Europea: el terrorismo, el tráfico de drogas, el tráfico de seres humanos, el fraude, la corrupción, el delito informático, el blanqueo de capitales y otras actividades relacionadas con la presencia de grupos delictivos organizados en la economía" (ALONSO MOREDA, 2012, pág. 123).

El artículo 86 TFUE va más allá al disponer que, con el fin de combatir los delitos que afectan a los intereses financieros de la Unión -fraude, corrupción, blanqueo de capitales, fraude del IVA- y ejercer la acción penal contra sus autores, el Consejo, mediante reglamentos adoptados con arreglo a un procedimiento legislativo especial, podrá crear una Fiscalía Europea (EPPO)[474] a partir de Eurojust. Ubicada en Luxemburgo y habiendo iniciado sus operaciones el 1 de junio de 2021, actualmente forman parte de ella veintidós de los veintisiete EEMM[475]. Se integra también en la Red de Agencias JAI.

Finalmente, es el artículo 88 TFUE el que da continuidad a Europol como un instrumento supranacional de apoyo a las autoridades policiales para la prevención y la represión de la delincuencia grave que afecte a dos o más EEMM, del terrorismo y otras formas de delincuencia con afectación a un interés común europeo. La actividad operativa de

[473] Eurojust se desarrolla mediante el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que sustituye y deroga la Decisión 2002/187/JAI del Consejo. Diario Oficial de la Unión Europea L 295/138, de 21 de noviembre de 2018. Disponible en: https://www.eurojust.europa.eu/sites/default/files/AboutUs/EULegalframework/2018-11-21_Eurojust-Regulation_2018-1727_ES.pdf (19/11/2023).

[474] La EPPO (European Public Prosecutor´s Office) se desarrolla mediante el Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea. Diario Oficial de la Unión Europea L283/1 de 31 de octubre de 2017. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017R1939 (19/11/2023).

[475] Hasta ahora Hungría, Polonia y Suecia no se han unido a la EPPO, y Dinamarca e Irlanda mantienen su opción de no participación en el ELSJ. Para facilitar la cooperación judicial y el intercambio estratégico de información, el 6 de abril de 2021 entró en vigor un acuerdo de trabajo con la Fiscalía General de Hungría y el 31 de agosto de 2023 entró en vigor un acuerdo de trabajo con el Ministerio de Justicia danés. Disponible en: https://www.eppo.europa.eu/en/members (19/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Europol se lleva a cabo conforme a los procedimientos del EEMM afectado y, en cuanto a la aplicación de medidas coercitivas derivadas, estas corresponden exclusivamente a las autoridades nacionales competentes, de acuerdo a lo establecido en los artículos 72 y 73 TFUE. A partir del Tratado de Lisboa, Europol se erige en agencia de referencia de la Unión "a la hora de garantizar la seguridad interior y mejorar la cooperación policial" (ANGUITA OSUNA, 2021, pág. 336), coordinando organizaciones, instituciones y cuerpos policiales, y liderando operaciones contra estructuras de crimen organizado y transnacional de gran valor, como analizaremos a continuación.

3.4.3. La Red de Agencias de Justicia y Asuntos de Interior: Europol y Eurojust

3.4.3.1. Europol

La cooperación policial en la UE se desempeña en un doble nivel complementario: a través de las relaciones bilaterales o multilaterales entre EEMM, en base al *principio de confianza* que se genera entre las unidades policiales que trabajan juntas en el ámbito operativo, y a través de las agencias de la Unión especializadas en temáticas concretas, como Europol, encargada de dar apoyo y reforzar la cooperación en materia de prevención y lucha contra el terrorismo, el crimen organizado y otras formas graves de delincuencia que afecten a dos o más socios y requieran una actuación policial común debido a su alcance, gravedad o consecuencias derivadas.

Respecto a la naturaleza jurídica de las agencias, convenimos con el profesor Fernández de Casadevante que estas:

> "[…] son organismos regulados por el Derecho de la Unión dotados de personalidad jurídica propia y creados por una disposición de Derecho derivado para desempeñar una labor científica o técnica concreta. Existen agencias de varios tipos: reguladoras (FRONTEX, Agencia para el Control de la Pesca, Agencia de los Derechos Fundamentales, etc.); de política exterior (Agencia Europea de Defensa); cooperación judicial (Europol, Eurojust y la Escuela Europea de Policía) y otras de carácter ejecutivo (Agencia Ejecutiva de Sanidad y Consumo o la de Investigación)" (FERNÁNDEZ DE CASADEVANTE ROMANI, CARRERA HERNÁNDEZ, GARRIDO REBOLLEDO, & GONZÁLEZ MARÍN, 2023, págs. 208-209).

En virtud de ello, podemos entender que las agencias de la UE[476] son entidades jurídicas creadas específicamente para llevar a cabo tareas especializadas según la legislación de la UE y, en concreto, la Red de Agencias de Justicia y Asuntos de Interior tiene encomendada una relevante tarea de protección ciudadana y de garantía de sus derechos fundamentales, a través de su desempeño en áreas como la migración y la gestión de fronteras, la lucha contra el crimen organizado, la ciberdelincuencia y el terrorismo, entre otras. Esta Red, supervisada en sus avances y logros por el COSI, se

[476] Página oficial UE sobre Agencias Europeas. Disponible en: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies_es?f%5B0%5D=oe_organisation_eu_type%3Ahttp%3A//publications.europa.eu/resource/authority/corporate-body-classification/AGENCY_DEC (25/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

compone de nueve agencias[477]: Europol, Eurojust, Frontex, eu-LISA[478], CEPOL[479], EIGE[480], EMCDDA[481], EUAA[482] y FRA[483]. En atención a la naturaleza de nuestro estudio, nos centraremos en el análisis de Europol con una breve referencia final a Eurojust, por su estrecha vinculación con el ELSJ.

Como ya se expuso anteriormente, es el Tratado de Maastricht el que acuerda la creación de la Oficina Europea de Policía -Europol- como respuesta necesaria de coordinación ante "la disparidad de normativas legales existentes, las barreras culturales lingüísticas y el hecho de que los Estados miembros afrontaran el fenómeno de la criminalidad desde un ámbito estrictamente nacional y no con una visión común europea" (MUJICA RUIZ, BARBOSA DE MIGUEL, GARCÍA ALAS, & MARTÍN PÉREZ, 2017).

El desarrollo de la propuesta encomendada por Maastricht se lleva a cabo en el Convenio Europol de 26 de julio de 1995[484], que busca mejorar la cooperación policial de los EEMM sin afectar a otras formas de cooperación bilateral o multilateral, para lo que define una serie de objetivos y asigna unas funciones a las Unidades Nacionales y Oficiales de Enlace que lo conforman, estableciendo las bases para el Sistema de Información SIS a través del cual gestionar el intercambio de información, auténtica pieza clave del proyecto.

Posteriormente, la Decisión del Consejo 2009/371/JAI[485] sustituye al anterior Convenio y resuelve la creación de una Oficina Europea de Policía (Europol) como ente de la Unión financiado con cargo a su presupuesto general, con el objetivo de simplificar y mejorar su funcionamiento, por ejemplo, facilitando su integración en los equipos conjuntos de investigación (ECI), garantizando su apoyo a los EEMM interesados sin la limitación de la existencia de indicios concretos de una estructura delictiva organizada o habilitándola para celebrar acuerdos con otras instituciones, organismos y agencias para aumentar la eficacia mutua en la lucha contra la delincuencia grave y evitar duplicidades.

El actual marco normativo de la Agencia lo conforman el artículo 88 TFUE y un Reglamento de desarrollo, la disposición legislativa de más alto rango en el ámbito de la

[477] Página oficial de Eurojust: Disponible en: https://www.eurojust.europa.eu/es/node/2273 (25/11/2023).
[478] European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice (Agencia de la UE para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud).
[479] European Union Agency for Law Enforcement Training (Agencia Europea para la Formación Policial).
[480] European Institute for Gender Equality (Instituto Europeo para la Igualdad de Género).
[481] European Monitoring Centre for Drugs and Drug Addiction (Centro Europeo de Monitorización de Drogas y Toxicomanías).
[482] European Union Agency for Asylum (Agencia Europea para el Asilo).
[483] Fundamental Rights Agency (Agencia de Derechos Fundamentales).
[484] Acto del Consejo, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K3 del Tratado de la Unión, por el que se crea una Oficina Europea de Policía (Convenio Europol). Diario Oficial de las Comunidades Europeas 95/C 316/01, de 27/11/1995 Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995F1127(01) (21/11/2023).
[485] Decisión del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol). Diario Oficial de la Unión Europea 2009/371/JAI L121/37. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:ES:PDF (21/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

UE[486], cuestión que pone de relieve su prioridad dentro del esquema de seguridad unionista, con competencias crecientes y poderosos instrumentos de soporte a las distintas policías nacionales. Ello, sin embargo, no debe llevarnos a concluir, erróneamente, que nos hallamos ante una suerte de *Policía europea al estilo del FBI estadounidense* con capacidades ejecutivas autónomas y verdadero poder supranacional. Europol *no es una Policía europea* sino un modo de colaboración de las policías europeas (OTERO SORIANO, 2011, pág. 122).

Continuando con el examen del marco normativo, el artículo 88 TFUE tiene su desarrollo, como decíamos, mediante el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo[487], en vigor desde mayo de 2017 y modificado por el Reglamento (UE) 2022/991[488], por el que se crea la European Union Agency for Law Enforcement Cooperation[489] (en adelante Reglamento de Europol), que sustituye y sucede a la Europol creada por la Decisión 2009/371/JAI, y que incide en cuestiones como la gestión anticipativa de la respuesta ante la amenaza terrorista y de la delincuencia organizada, basada en el análisis de inteligencia y la explotación conjunta de bases de datos a través de SIENA[490], el desarrollo de reuniones operativas para compartir información y planificar actuaciones coordinadas para el desarrollo de las operaciones[491], el impulso de los ECI, la celebración de los *joint action days*[492], la financiación por parte de Europol de las necesidades operativas de las unidades policiales implicadas, así como el

[486] El artículo 288 TFUE dispone que "para ejercer las competencias de la Unión, las instituciones adoptarán reglamentos, directivas, decisiones, recomendaciones y dictámenes".

[487] Reglamento 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo. Diario Oficial de la Unión Europea L135/53, de 24/05/2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0794 (21/11/2023).

[488] Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, 8 de junio de 2022, por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación. Diario Oficial de la Unión Europea L169, de 27/06/2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R0991 (23/11/2023).

[489] Agencia de la Unión Europea para la Cooperación Policial (Europol).

[490] Secure Information Exchange Network Application (SIENA) es la herramienta de Europol para el intercambio seguro de información entre los cuerpos policiales tanto de la Unión como de países terceros y organizaciones internacionales asociados, que establece unos códigos de manejo de la información y tutela el respeto de los datos personales conforme a los principios de necesidad y proporcionalidad en su uso, bajo la auditoría del Supervisor Europeo de Protección de Datos.

[491] Estas reuniones operativas, conocidas como *sprint meetings*, se llevan a efecto cuando diferentes unidades policiales están investigando a nivel nacional un mismo objetivo sin tener constancia de ello hasta que, en un momento dado, se genera un cruce en las bases de datos de Europol a raíz de la información que cada uno de ellos graba. A partir de aquí las unidades contactan y se propone un sprint meeting liderado por uno de los cuerpos policiales intervinientes para poner en común los avances nacionales en relación con ese actor de la amenaza de carácter trasnacional.

[492] Los *joint action days* (jornadas de acción conjunta) son coordinados por Europol y consisten en focalizar una prioridad investigativa conjunta, por ejemplo, los fraudes mediante la compra de billetes de vuelo con tarjetas de crédito falsas, fijando un día en el que todos los cuerpos policiales recibirán la información de qué personas van a viajar en el ámbito de su jurisdicción, para proceder a la detención de todas ellas al mismo tiempo, en el marco colaborativo de la Agencia. De esta operación se hace nota de prensa de Europol explicando los objetivos, los participantes y los resultados obtenidos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

asesoramiento de expertos y la formación en conocimientos y buenas prácticas que mejoren las capacidades de las Unidades policiales.

La principal función de la Agencia tradicionalmente ha sido y sigue siendo el análisis, tanto operativo como estratégico, de toda la información recopilada en sus bases de datos sobre investigaciones de los servicios policiales de los EEMM y de aquellos terceros Estados con quienes existen acuerdos de cooperación[493], para generar productos de inteligencia con los que desempeñar su función de apoyo e identificación de temas clave de investigación. También se nutren sus bases de datos de la información procedente de organizaciones internacionales[494] y otras agencias europeas del ELSJ[495] y entidades privadas[496].

Sobre el desarrollo de las capacidades de la Agencia y, en particular, del análisis como su cometido esencial, es pertinente mencionar la última reforma del Reglamento de junio de 2022 ya citado que, entre otras, incorpora las siguientes novedades:

1. Habilita a Europol para tratar ingentes volúmenes de datos mediante tecnologías avanzadas como la IA y el *machine learning*.
2. Ofrece un marco normativo garantista y de nuevo cuño para acceder a datos personales en poder de actores privados que, a partir de ahora, podrán trasladar paquetes de información relevante de manera directa para su análisis y tratamiento por parte de la Agencia.
3. Articula mecanismos de cooperación directa con terceros países y organizaciones internacionales para el intercambio de datos personales, así como con la nueva Fiscalía Europea, con quien Europol debe mantener una estrecha relación de apoyo y cooperación, al igual que con Eurojust.

Y todo ello en el marco de una exigente regulación de protección de datos personales, con sometimiento pleno a la ley y al Supervisor Europeo de Protección de Datos (EDPS), quien ejerce una función de permanente monitorización y control de legalidad sobre el tratamiento de los datos personales en el ámbito de la UE.

En cuanto al análisis de carácter estratégico de la Agencia, hay que mencionar que se lleva a cabo por más de una centena de analistas altamente especializados que se apoyan en el Europol Analysis System (EAS)[497], el cual alberga los datos aportados por las partes interesadas para la identificación de tendencias y amenazas emergentes. Con toda esta información elabora Europol sus informes, ya sean de carácter general, como

[493] Los acuerdos de cooperación pueden ser operativos, estratégicos o de trabajo. En la actualidad Europol cuenta con Oficinas de Enlace en la sede central de La Haya de los veintisiete Estados miembros y de más de veinte países no pertenecientes a la Unión, como por ejemplo Australia, Canadá, EE.UU., Ucrania o Colombia. Sólo Estados Unidos ha acreditado hasta once agencias federales para que compartan información a través de Europol, como el Federal Bureau of Investigation (FBI), el Secret Service (USSS), la Drug Enforcement Administration (DEA) o el Customs and Border Protection (CBP), entre otros.

[494] Organizaciones internacionales como Interpol o la United Nations Office on Drugs and Crime (UNODC).

[495] Agencias como Eurojust, Frontex, CEPOL, EMCDDA, la Oficina Europea de Lucha contra el Fraude (OLAF) o la European Union Agency for Cybersecurity (ENISA).

[496] Empresas, asociaciones empresariales, organizaciones sin ánimo de lucro, personas jurídicas de derecho privado, etc.

[497] Sistema de Análisis de Europol.

Ediciones Universidad de Salamanca | CC BY-NC-ND

el SOCTA[498] y el TE-SAT[499], o de tipo monográfico sobre aquellos fenómenos emergentes o complejos que requieran de un análisis y visión conjunta a nivel europeo. Entre éstos son reseñables por su calidad, complejidad e importancia estratégica el IOCTA[500], de carácter anual, y otros de índole temática como, por ejemplo, *Cryptocurrency: tracing the evolution of criminal finances* (2022)[501], *Criminal networks in migrants smuggling* (2023)[502], o *The other side of the coin* (2023)[503]. Todos estos documentos tienen en común un doble objetivo: por un lado, aportar luz en el ámbito político para apoyar la toma de decisiones y, por otro, difundir elementos de conocimiento dirigidos a los policías directamente involucrados en la prevención y respuesta a la criminalidad especializada.

En cuanto a las líneas estratégicas, el documento *Europol Strategy 2020+*[504] define estos objetivos orientados a convertir a la Agencia en el nodo europeo de información criminal aprovechando la extensa red de *partners* ya consolidada, ofrecer apoyo operativo de una forma ágil y eficiente, ser reconocida como una plataforma para la solución de problemas policiales a escala europea, situarse en una posición preeminente en materia

[498] El Informe de Amenaza de Crimen Organizado (Serious and Organised Crime Threat Assesment "SOCTA") tiene una periodicidad cuatrienal, aunque se actualiza cada dos años. En él se identifican las áreas prioritarias en que debe centrarse la respuesta operativa de la UE en cuanto a la amenaza derivada de la criminalidad organizada grave, y constituye una referencia muy importante para la determinación a nivel estratégico de las prioridades del ciclo político del Consejo.

[499] El Informe de Situación y Tendencias del Terrorismo (Terrorism Situation and Trend Report "TE-SAT") es anual y ofrece una visión general de los fenómenos terroristas o asimilados operen o puedan afectar a la seguridad de la Unión, constituyéndose en un elemento estratégico por cuanto identifica las tendencias de dicha amenaza en base a la información facilitada por los EEMM y resto de instituciones y países asociados.

[500] El Informe de la amenaza de la delincuencia organizada en Internet (Internet Organised Crime Threat Assesment "IOCTA") es elaborado por el Centro Europeo contra la Ciberdelincuencia (EC3) de Europol, y es un informe clave para la identificación de las tendencias de la ciberamenaza con afectación a gobiernos e instituciones, al sector privado y a los ciudadanos. Este informe analiza las técnicas, tácticas y procedimientos de los actores de la amenaza para poder determinar sus características y orientar la estrategia de respuesta de manera efectiva y coordinada. El IOCTA 2023 es el *Cyber-attacks: the ápex of crime-as-a-service*. Disponible en: https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023 (23/11/2023).

[501] Disponible en: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (23/11/2023).

[502] Disponible en: https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-migrant-smuggling#:~:text=The%20criminal%20networks%20involved%20are,offered%20by%20migrant%20smuggling%20networks (23/11/2023).

[503] Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf (23/11/2023).

[504] La actual Directora Ejecutiva, Catherine de Bolle, de nacionalidad belga, ha vinculado el éxito de su mandato, de ocho años (cuatro más cuatro hasta 2026), al cumplimiento de este plan estratégico vigente. Disponible en: https://www.europol.europa.eu/publications-events/publications/europol-strategy-2020 (23/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de innovación[505] e investigación policial[506] y, finalmente, servir de referencia para el modelo europeo de organización policial moderna. Cada una de estas líneas estratégicas se articula en torno a un número reducido de objetivos específicos, cuyo cumplimiento será monitorizado por el Consejo de Administración, a través de los informes periódicos de implementación.

Es necesario referirnos someramente a las vías de financiación de operaciones contra la delincuencia organizada y transnacional, que se articulan desde Europol a través de dos áreas. En primer lugar el EMPACT[507], que incorpora un presupuesto anual para invertir en la actividad operativa de los Estados miembros que lo necesiten, dentro de una aproximación a la seguridad interior de la Unión con una perspectiva integral que se centra en diez áreas delincuenciales definidas como prioritarias por la Agencia para su ciclo político de cuatro años, siendo el vigente el de 2022-2025[508]. La segunda línea de inversión es a través de los HVT/OTF (Objetivos de Alto Valor y Grupos de Acción Operativa)[509], con un presupuesto dedicado a la identificación y persecución de elementos criminales denominados *de alto valor* y vinculados a las prioridades operacionales de la UE, tanto de corte tradicional –terrorismo, drogas, tráfico de seres humanos, delincuencia financiera, etc.– como de perfil más actual, especialmente la criminalidad informática en sus diversas manifestaciones –ciberdelincuencia con finalidad económica, ciberdelincuencia con especial daño a las víctimas por su condición o edad, cibercriminalidad con afectación a infraestructuras críticas y servicios

[505] En este sentido, actualmente en Europol se está trabajando en la New Forensic Environment (NFE) como plataforma técnica de análisis e intercambio de grandes volúmenes de datos sobre actividades delictivas, para identificar y preservar evidencias que, posteriormente, puedan ser utilizadas en el oportuno procedimiento penal, todo ello conforme a lo legalmente establecido para la protección de datos personales (acceso, cesión de datos, enmascaramiento de datos, tiempo de vigencia, etc.). Información de fuentes propias.

[506] En julio de 2020 las autoridades policiales y judiciales de Francia y Países Bajos, en coordinación con Europol y Eurojust, culminaron una investigación conjunta cuyo objetivo era el desmantelamiento de una plataforma de comunicación cifrada utilizada por las estructuras de crimen organizado para el tráfico de drogas y la corrupción, entre otras. Para llevarlo a cabo se constituyó la OTF "EMMA" en la que trabajaron investigadores y analistas de Europol, los EEMM implicados y terceros países para llevar adelante la operación cuyo posterior análisis de inteligencia, de más de 115 millones de conversaciones de un número estimado de 60.000 usuarios, ha servido para presentar en junio de 2023 el primer resumen de resultados con 6.558 detenidos -197 de ellos catalogados como HVT-, 739,7 millones de euros en efectivo incautados, 154,1 millones de euros congelados en activos o cuentas bancarias, más de 270 toneladas de droga incautadas, así como vehículos, armas, barcos y aviones. Se trata de la Operación Encrochat de Europol. Disponible en: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized (23/11/2023).

[507] EMPACT corresponde al acrónimo de European Multidisciplinary Platform Against Criminal Threats (Plataforma Multidisciplinar Europea contra las Amenazas Delictivas), para la lucha contra las formas graves de delincuencia organizada e internacional. Disponible en: https://www.europol.europa.eu/crime-areas-and-statistics/empact (23/11/2023).

[508] Prioridades 2022-2025: 1) redes criminales de alto riesgo; 2) ataques cibernéticos; 3) tráfico de seres humanos; 4) explotación sexual infantil; 5) tráfico de inmigrantes; 6) tráfico de drogas; 7) fraude, delitos económicos y financieros; 8) delitos contra la propiedad organizados; 9) delitos ambientales, 10) tráfico de armas de fuego.

[509] HVT/OTF corresponde al acrónimo de High Value Targets and Operational Task Forces (Objetivos de Alto Valor y Grupos de Acción Operativa). Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2022-2024.pdf (23/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

esenciales-. En 2022 se constituye en España la *Operational Task Force* (OTF)[510] de mayor entidad hasta la fecha, llamada *Costa del Sol* por su emplazamiento en Málaga, financiada con fondos europeos y con Oficiales de Enlace desplegados de hasta 17 países con el objetivo de identificar, investigar y detener a los objetivos *de alto valor* señalados de dichas nacionalidades que operan o se refugian en la zona[511].

Por lo que respecta a la estructura española de Europol, al igual que los demás EEMM, cuenta con una Unidad Nacional que centraliza las relaciones de todos los operadores de seguridad del país, y con una Oficina de Enlace en la sede central de la Agencia, en La Haya. De acuerdo con lo establecido en el artículo 7 del Reglamento de Europol, las Unidades Nacionales se configuran como el nexo de unión entre la Agencia y las autoridades competentes designadas de los EEMM, mientras que el artículo 8 dispone la existencia de una Oficina de Enlace por país, para canalizar las peticiones de información y defender los intereses de sus respectivas Unidades Nacionales.

El encaje normativo interno de esta estructura se lleva a cabo por el Real Decreto 207/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, que determina que la División de Cooperación Internacional de la Policía Nacional, con dependencia directa de su Director General, asume entre sus funciones la gestión de la Unidad Nacional de Europol y de la Oficina SIRENE[512], conforme a lo establecido por el artículo 12.1.A) de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad[513]. Por su parte, la Unidad Nacional de Europol se constituye como el enlace entre las distintas Fuerzas y Cuerpos de Seguridad nacionales competentes y Europol, coordinando a nivel nacional la cooperación policial con la Agencia y garantizando así una postura nacional única[514], mientras que la Oficina

[510] Grupos de Acción Operativa, que son equipos multidisciplinares y especializados, integrados por miembros de los Cuerpos Policiales de los diferentes países implicados en la investigación, que se constituyen para hacer frente a las estructuras delictivas de crimen organizado transnacional.

[511] Información de fuentes propias.

[512] El artículo 3.2.e) del RD 207/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, señala que depende directamente de la persona titular de la Dirección General "la División de Cooperación Internacional, con el nivel orgánico que se determine en la relación de puestos de trabajo, a la que corresponde la gestión de la Oficina Central Nacional de INTERPOL, la Unidad Nacional de EUROPOL y la Oficina SIRENE, la dirección de la colaboración y auxilio a las policías de otros países y la coordinación de los grupos de trabajo en los que participe la Dirección General de la Policía en el ámbito de la Unión Europea y otras instituciones internacionales, así como aspectos relacionados con misiones de apoyo a terceros países y personal policial que presta servicio en el extranjero". Disponible en: https://www.boe.es/eli/es/rd/2024/02/27/207/con (23/07/2024)

[513] El artículo 12.1.A) de la LOFCS 2/1986 señala como competencia material de la Dirección General de la Policía la colaboración y el auxilio a las policías de otros países, conforme a lo establecido en los Tratados y Acuerdos Internacionales, bajo la superior dirección del Ministro del Interior. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859 (24/11/2023).

[514] En relación con el Real Decreto 734/2020, la Orden INT/859/2023, de 21 de julio, por la que se desarrolla la estructura orgánica y funciones de los servicios centrales y territoriales de la Dirección General de la Policía, determina en su artículo 3.2.d) que la Unidad Nacional de Europol "se constituye como el enlace entre las autoridades nacionales competentes y la Agencia Europol, asume un papel de coordinador nacional con respecto a la cooperación policial de los Estados miembros y la Agencia. Le corresponde garantizar la aplicación de criterios de igualdad e imparcialidad en las comunicaciones que se intercambien con la Agencia, visibilizando de este modo una postura nacional única". Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2023-17072 (24/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

SIRENE se encarga de la cooperación técnica y operativa en el ámbito del Sistema de Información Schengen, y se constituye en punto de contacto del Convenio de Prüm[515]. Respecto a la Oficina de Enlace en la sede de Europol, España despliega una de las más numerosas en cuanto a su dotación de personal, con más de diez agentes pertenecientes a la Policía Nacional, a la Guardia Civil y al Servicio de Vigilancia Aduanera. El jefe de la Oficina de Enlace actualmente es un Comisario de la Policía Nacional. Además de los Oficiales de Enlace referidos, España cuenta en Europol con el mayor número de personal[516] de todos los países de la UE, con un total de 125 puestos ocupados, seguido por Países Bajos -sede de la Agencia- con 124, e Italia, con 110[517].

Conforme a los datos aportados en el Informe Anual sobre la información facilitada por los Estados miembros en 2022[518], en lo referente a la actividad operativa España se sitúa como el cuarto país con mayor número de intercambios de información y aportación de casos -47.432.805-, tras Alemania, Francia e Italia. Sobre las áreas criminales de especial incidencia en las aportaciones españolas, la más voluminosa es el ámbito de drogas, con un 31% de toda la información remitida, seguida por los fraudes con un 25% y el blanqueo con un 18%. Por lo que concierne al nivel de complejidad de los casos aportados -aquéllos que cuentan con más de diez contribuciones aceptadas-, España se sitúa en la parte alta de la tabla, tan sólo por detrás de Chipre. El 47% de las contribuciones españolas están vinculadas a casos complejos, lo que demuestra que España, en términos generales, utiliza Europol para casos importantes, por encima incluso de la media de la UE. Este indicador es quizá uno de los más relevantes del informe y aquí España mantiene una posición muy destacada.

Durante el semestre de Presidencia española del Consejo de la UE -del 1 de julio al 31 de diciembre de 2023- se incluyen en la agenda algunos asuntos con destacado reflejo en las reuniones estratégicas de Europol, como la adopción de una política común en materia de asilo, refugio, migración y fronteras, impulsar la prevención y lucha contra las acciones terroristas y radicalizaciones violentas, afrontar el reto de una criminalidad organizada y violenta creciente, en particular la explotación sexual de menores a través de la red, fortalecer la interoperabilidad policial y favorecer el intercambio de información, monitorizar la guerra de Ucrania y sus consecuencias en el ámbito de la

[515] El artículo 3.2.e) de la citada Orden INT/859/2023 señala que la Oficina Sirene es la responsable de "las misiones de cooperación técnica y operativa en el ámbito del Sistema de Información Schengen acorde con las disposiciones de la Unión Europea que regulan su funcionamiento. Le corresponde la materialización de entregas de las personas reclamadas en virtud de una Orden Europea de Detención y Entrega. Ejerce la Coordinación funcional en el ámbito de la Dirección General de la Policía de las Comisarías Conjuntas, los Centros de Cooperación Policial Aduanera y los Centros de Cooperación Policial. Asimismo, se constituye como punto de contacto designado para el intercambio de datos post-hit de perfiles de ADN y datos dactiloscópicos según el Convenio de Prüm".

[516] El personal nacional destinado en Europol incluye no solo a los miembros de las FCS, sino también juristas, informáticos o técnicos analistas, entre otros.

[517] Datos actualizados a fecha de 9 de enero de 2023. Disponible en: https://www.europol.europa.eu/about-europol/statistics-data (24/11/2023).

[518] Consolidated Annual Activity Report 2022, analizado en la reunión del Consejo de Administración de Europol de los días 7 y 8 de junio de 2023. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202022.PDF (24/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

seguridad interior y, finalmente, la prevención y anticipación ante retos comunes como la violencia de género o la seguridad en carretera.

3.4.3.2. Eurojust

En cuanto a Eurojust, la Agencia de la Unión Europea para la Cooperación Judicial Penal, debemos comenzar señalando que aunque en el Consejo Europeo de Tampere de 1999 y en la Conferencia Intergubernamental de Niza de 2000 ya se presentan propuestas para mejorar la cooperación judicial en la Unión, son una vez más los atentados terroristas del 11 de septiembre de 2001 en Nueva York los que acaban acelerando este proceso, que se concreta con la aprobación de la Decisión del Consejo de 28 de febrero en 2002[519] por la que se crea Eurojust como Unidad de Cooperación Judicial para la lucha contra las formas graves de la delincuencia (ANGUITA OSUNA, 2021, págs. 304-307). Su actual marco jurídico está regulado por el artículo 85 TFUE y el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo[520] (en adelante Reglamento Eurojust), que le dota de estatus de Agencia.

La función de Eurojust viene recogida en el artículo 2 del citado Reglamento, el cual establece que apoyará y reforzará la coordinación y la cooperación entre las autoridades nacionales encargadas de investigar y perseguir las formas de delincuencia grave para las que la Agencia sea competente, cuando afecten a dos o más EEMM o deban perseguirse en base a las operaciones y la información proporcionada por éstos, por Europol, por la Fiscalía Europea o por la Oficina Europea Antifraude (OLAF por sus siglas en inglés)[521].

Con sede en La Haya, frente al edificio de Europol, podríamos decir que Eurojust es una reproducción de aquella adaptada al ámbito de la cooperación judicial penal, aunque existen algunas diferencias significativas que enunciaremos a continuación. Así, Eurojust

---

[519] Decisión 2002/187/JAI del Consejo de 28 de febrero de 2002 por la que se crea Eurojust para reforzar la lucha contra las formas graves de la delincuencia. Diario Oficial de las Comunidades Europeas L 63 de 06/03/2002. Disponible en: https://www.boe.es/doue/2002/063/L00001-00013.pdf (25/11/2023).

[520] Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo. Diario Oficial de la Unión Europea L 295/138 de 21/11/2018. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1727 (25/11/2023).
Este Reglamento ha sido modificado en dos ocasiones. La primera de ellas, por el Reglamento (UE) 2022/838, de 30 de mayo, del Parlamento Europeo y del Consejo de 30 de mayo de 2022 por el que se modifica el Reglamento (UE) 2018/1727 en lo que respecta a la preservación, análisis y almacenamiento en Eurojust de pruebas relativas al genocidio, los crímenes contra la humanidad, los crímenes de guerra y las infracciones penales conexas. DOUE núm. 148, de 31 de mayo de 2022. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80811 (25/11/2023).
Y la segunda, por el Reglamento (UE) 2023/2131 del Parlamento Europeo y del Consejo, de 4 de octubre de 2023, por el que se modifican el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo y la Decisión 2005/671/JAI del Consejo en lo que respecta al intercambio de información digital en casos de terrorismo. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81404 (25/11/2023).

[521] European Anti-Fraud Office.

Ediciones Universidad de Salamanca | CC BY-NC-ND

se conforma –de manera similar a Europol– con una doble estructura: de un lado las veintisiete Mesas Nacionales, a modo de las Oficinas de Enlace de Europol, lideradas por el Miembro Nacional, habitualmente un fiscal especializado en materia penal, y el resto de la delegación integrada por otros fiscales, jueces o policías designados e íntegramente financiados por su país de pertenencia. A esta estructura hay que añadir la Administración, compuesta por funcionarios europeos financiados por Bruselas y cuya función primordial es dar apoyo técnico a las Mesas Nacionales. Aquí se encuadran unidades como el servicio jurídico, la unidad de análisis, de gestión de la información, el servicio financiero y la oficina de prensa y relaciones públicas. De otro lado, cada EEMM debe designar en su territorio al menos a un Corresponsal Nacional de Eurojust para canalizar y facilitar las relaciones entre la Agencia y las autoridades nacionales y agilizar las tareas de coordinación entre las autoridades judiciales nacionales responsables de las investigaciones penales en las materias establecidas en su ámbito competencial. En este mismo sentido, por el nivel de afectación a la seguridad interior de los EEMM, debe designarse también un Corresponsal Nacional para Asuntos de Terrorismo.

Ante la necesidad de dotar a Eurojust de una estructura administrativa y de gestión para el desempeño de sus funciones, se establecen las figuras del Colegio, el Director Administrativo y el Consejo Ejecutivo. El denominado Colegio de Eurojust está formado por los respectivos miembros nacionales[522] y se reúne semanalmente para el análisis de casos y otras cuestiones de la vida organizativa -programas de trabajo, presupuesto, informe de actividad anual y acuerdos de trabajo con los socios-, teniendo en cuenta que dos de estos mismos miembros nacionales constituyen, junto con un representante de la Comisión Europea y el presidente y los dos vicepresidentes de Eurojust, el Consejo Ejecutivo, responsable de la toma de decisiones acerca de cuestiones estratégicas, administrativas y de gestión interna.

Desde el punto de vista operativo se han establecido dos formas básicas de cooperación judicial: la llamada *coordinación*, de naturaleza formal, consistente en que el país requirente determina la necesidad de organizar una reunión de coordinación con autoridades policiales y judiciales de otros EEMM o incluso países terceros, para el análisis de un caso y la exploración de las posibles dificultades legales en su resolución[523], y la *cooperación*, de carácter informal, que se organiza abriendo un caso y realizando gestiones bilaterales o multilaterales con los países requeridos a fin de articular vías de respuesta a los requerimientos que hayan sido formulados. Además, existe una tercera vía denominada *Célula de Coordinación de Emergencia*, como mecanismo de respuesta permanente con disponibilidad las 24 horas del día los 7 días de la semana, los 365 días del año, que busca potenciar la eficacia en las funciones de coordinación y cooperación que ejerce la Agencia entre las autoridades judiciales de los EEMM y otros asociados.

Las relaciones de Eurojust con los socios dentro de la Unión -Red Judicial Europea, Europol, Fiscalía Europea, OLAF, Frontex y otros- es cuestión altamente determinante

[522] El Colegio de Miembros Nacionales se regula en el artículo 10 del Reglamento (UE) 2018/1727.

[523] Dificultades como por ejemplo conflictos de jurisdicción, gestión de órdenes europeas de detención y entrega, la congelación y confiscación de activos financieros, la creación de equipos conjuntos de investigación, posibles entradas y registro o detenciones simultáneas en distintos países, etc.

Ediciones Universidad de Salamanca | CC BY-NC-ND

en la que incide el Reglamento[524] como parte crucial del desempeño de sus competencias. Atención especial requiere la cooperación operativa entre Eurojust y Europol, para la que se dispone el acceso y cruce de la información entre sus bases de datos, con las debidas garantías legales y de protección de derechos ciudadanos respecto al tratamiento automatizado de datos de carácter personal, y el conocimiento mutuo de los ECI que se articulen por necesidades investigativas.

Las reuniones operativas son la esencia del funcionamiento de Eurojust, por cuanto le permiten fomentar el intercambio inmediato de información o evidencias en el ámbito de una acción policial, planificar y coordinar la investigación y posterior fase ejecutiva simultánea bajo diferentes jurisdicciones, o localizar puntos de conexión entre investigaciones desarrolladas por distintos cuerpos policiales de manera independiente en distintos países, para valorar la posibilidad de centralizar en un solo investigador la dirección de la investigación, con el objetivo de evitar duplicidades y conflictos de jurisdicción. En este mismo sentido, la constitución de los ECI son una excelente herramienta para proporcionar a policías, fiscales y jueces un entorno controlado en el que poder gestionar de manera conjunta una investigación y compartir evidencias, impresiones y datos dentro del adecuado marco legal (ALONSO MOREDA, 2012, pág. 137).

En términos prácticos, y para entender la cooperación policial y judicial en materia penal dentro del espacio europeo, el decurso razonable de las investigaciones se inicia con la apertura del caso en Europol por el cuerpo policial investigador que corresponda, la organización de una o varias reuniones operativas entre investigadores nacionales y analistas y expertos de Europol, así como el diagnóstico de situación sobre el estado evolutivo de los casos en cuestión en los distintos EEMM. Una vez que los cuerpos policiales concernidos conforman el denominado *diagnóstico de inteligencia*, con la colaboración principalmente analítica de Europol, suele ser pertinente requerir a Eurojust, desde el ámbito nacional y por quien ostente la titularidad y el liderazgo de la investigación, para que organice una reunión de coordinación e invite a jueces, fiscales y policías. Estos exponen la investigación en curso y la situación policial en que se encuentra, correspondiendo a jueces y fiscales la identificación de problemas de orden legal, las posibles vías de solución y la propuesta de una estrategia jurídica para conseguir la más sólida imputación criminal de los sujetos investigados.

Como cuestión de orden práctico frecuente, es habitual acordar por los intervinientes la cesión de jurisdicción al país preeminente en el caso investigado de forma que, para conseguir esa mejor imputación penal de los autores del delito, lidere la gestión de las evidencias físicas y electrónicas que puedan eventualmente obtenerse cuando se operativice la información disponible, siendo el responsable de su puesta a disposición de la autoridad judicial competente para que ésta ejerza la acción penal. Para ello deviene fundamental que tanto policías como jueces y fiscales cuenten con un alto nivel de especialización en cooperación policial y judicial internacional, especialmente europea, y en sus instrumentos de cooperación para la adecuada y efectiva articulación de la estrategia de persecución penal. De otro modo, las defensas de los imputados

[524] La Sección II del Reglamento (UE) 2018/1727 está dedicada a las relaciones con los socios dentro de la Unión, y abarcar desde el artículo 48 al 51, inclusive.

Ediciones Universidad de Salamanca | CC BY-NC-ND

pueden encontrar vías legales de escape por razones de forma o fondo que pueden perjudicar, o incluso arruinar, una larga y compleja investigación policial.

Conviene resaltar que, a raíz de la guerra de Ucrania, el Reglamento de Eurojust ha sido modificado por el Reglamento (UE) 2022/838, de 30 de mayo de 2022[525], ampliando el mandato de la Agencia a la investigación de genocidios, crímenes contra la humanidad y crímenes de guerra. Esta obtención de evidencias ya se ha llevado a cabo en la guerra de Ucrania, contando para ello con el apoyo operativo de Europol, que ha creado una OTF para ayudar en las investigaciones en curso sobre los crímenes de guerra cometidos en Ucrania tras la invasión rusa de febrero de 2022[526], y trasladar las evidencias al Tribunal Penal Internacional.

A modo de conclusión, podemos convenir que en un espacio sin fronteras interiores y con libertad de movimientos como es la UE, donde la seguridad interior de cada uno de los EEMM está íntimamente vinculada con la de los demás por cuanto la amenaza trasciende la capacidad de actuar de cada uno de ellos en solitario, Europol y Eurojust representan el firme compromiso de sus miembros con la seguridad *intra lindes*, ante la evidencia de que el ELSJ "no se puede culminar si la Unión Europea no dispone de los instrumentos adecuados, tarea que se complica si los países que la componen se niegan a ceder o compartir algunas de sus competencias en este ámbito" (SÁNCHEZ PELÁEZ, 2021, pág. 172).

3.4.4. La Estrategia de Seguridad Interior de la UE: hacia un modelo europeo de seguridad (2010-2015)

En 2010, con la idea de avanzar en la consolidación del Espacio de Libertad, Seguridad y Justicia, el Consejo Europeo suscribe el *Programa de Estocolmo –una Europa abierta y segura que sirva y proteja al ciudadano*, donde, entre otras cuestiones, se fija en las posibilidades de desarrollo de Europol con un triple enfoque: 1) como eje del intercambio de información entre los cuerpos policiales de los EEMM; 2) como prestador de servicios a los ciudadanos; 3) y como plataforma de servicios policiales[527].

Al mismo tiempo, insta al Consejo y a la Comisión a definir una estrategia integral y coherente de la Unión que defina su modelo de seguridad interior y que, además, envíe a los ciudadanos el mensaje de que garantizar su seguridad es cuestión prioritaria. Para ello, este documento estratégico habrá de contener, sobre todo, los *principios rectores* de las distintas políticas nacionales de seguridad de los EEMM, las *amenazas actuales*

[525] Reglamento (UE) 2022/838, del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, por el que se modifica el Reglamento (UE) 2018/1727 en lo que respecta a la preservación, análisis y almacenamiento en Eurojust de pruebas relativas al genocidio, los crímenes contra la humanidad, los crímenes de guerra y las infracciones penales conexas. Diario Oficial de la Unión Europea L 148 de 31/05/2022. Disponible en: https://www.eurojust.europa.eu/sites/default/files/assets/celex-32022r0838-es-txt.pdf (25/11/2023).

[526] Disponible en: https://www.europol.europa.eu/media-press/newsroom/news/europol-sets-osint-taskforce-to-support-investigations-war-crimes-committed-in-ukraine (25/11/2023).

[527] Programa de Estocolmo –una Europa abierta y segura que sirva y proteja al ciudadano, del Consejo Europeo. Diario Oficial de la Unión Europea 2010/C 115/01, de 04/05/2010. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:es:PDF (23/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

que deben afrontarse y los instrumentos a través de los cuales hacerlo, así como las *líneas de futuro* (VILLALGORDO GARCÍA, 2011, págs. 32-33). Igualmente, se considera que el desarrollo, la supervisión y la aplicación de la Estrategia de Seguridad Interior de la Unión debe ser una de las tareas prioritarias del COSI y, como tal, construirse desde la sintonía con la PESC por las cada vez mayores vinculaciones entre la dimensión exterior e interior de la seguridad. Incluso se propone a la Comisión la creación de un Fondo de Seguridad Interior (FSI) para promover la viabilidad práctica del proyecto.

En este contexto de requerimiento, el Consejo Europeo aprueba el 25 de marzo de 2010 la primera Estrategia de Seguridad Interior de la UE (ESI-UE)[528], con tres ideas principales: 1) la seguridad es un factor clave de estabilización y desarrollo de la sociedad europea; 2) se articula a través de un modelo coherente con los valores y principios de la Unión; 3) y se trata de un modelo de seguridad integrador, común y de futuro.

Respecto a la primera de ellas, *la seguridad como factor de desarrollo*, la ESI-UE pone de manifiesto el problema que representa la ágil adaptación de la amenaza a la evolución científica y tecnológica que caracteriza a la era digital, para la que propone una respuesta preventiva, oportuna y adecuadamente gestionada para garantizar una sociedad europea segura no solo dentro de su territorio, sino que pueda desplazarse a terceros países con cobertura de soporte y que, además, disfrute de un acceso confiable al entorno virtual de Internet. De esta forma, la ESI-UE se aproxima a un concepto de seguridad interior amplio e integral, derivado de la imbricación multisectorial tanto horizontal como vertical[529], y sensible a la repercusión que las distintas políticas europeas pueden tener en la vida y el bienestar de los ciudadanos.

La segunda línea principal de la ESI-UE es la propuesta de un *modelo de seguridad basado en los valores y principios de la Unión* que vienen recogidos en la Carta de Derechos Fundamentales y representados en el Estado de Derecho, la transparencia y la rendición de cuentas aplicadas a la política de seguridad, la libertad de expresión, la integración e inclusión social y la lucha contra la discriminación, la solidaridad entre los EEMM y la confianza mutua como base de las relaciones. Nos parece oportuna la reflexión que el reputado investigador Félix Arteaga hace al respecto, contextualizada en ese periodo temporal, indicando que:

> "[…] se trata de principios y valores comunes a todos los modos europeos de cooperación que no haría falta afirmar si no fuera porque la cooperación JAI está permanentemente bajo la sospecha de quienes creen que la seguridad y libertad son objetos de un juego suma cero por el que los avances en un campo se hacen inevitablemente a costa de retrocesos en el otro" (ARTEAGA MARTÍN, 2010, pág. 3).

[528] Consejo de la Unión Europea, Secretaría General del Consejo, Estrategia de seguridad interior para la Unión Europea – Hacia un modelo de seguridad europeo. Marzo de 2010. Disponible en: https://data.europa.eu/doi/10.2860/87810 (23/11/2023).

[529] La dimensión horizontal de la seguridad se refiere a la colaboración policial, judicial, civil, política, económica, financiera, social, privada y de instituciones y organismos no gubernamentales, mientras que la dimensión vertical se refiere a la colaboración en diferentes planos de actuación: internacional, en el seno de la Unión, entre los EEMM, a nivel nacional, regional y local.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Puede que también influya en ello la intención de lanzar a la ciudadanía un mensaje de transparencia y protección de derechos en el ámbito del ELSJ, dando a la política JAI un toque de protagonismo ante los ciudadanos como factor estabilizador de su forma de vida.

Finalmente, el tercer eje de la ESI-UE incide en la creación de un *modelo de seguridad europeo, integrador y con visión de futuro*, para hacer frente a las amenazas y riesgos comunes. El problema en este punto radica en que, tal y como establece el artículo 72 TFUE, el ELSJ ocupa únicamente el ámbito de responsabilidad que *voluntariamente* cedan los EEMM, por cuanto el orden público y la seguridad interior es competencia exclusiva de éstos, y la ESI-UE no clarifica qué partes corresponden a las autoridades nacionales y cuáles a la Unión, de tal manera que, aunque lo pretende, *no instaura un modelo de seguridad europeo, sino un modelo de cooperación europeo en el ámbito JAI* (ARTEAGA MARTÍN, 2010, pág. 4).

En cuanto a las líneas estratégicas de acción de la ESI-UE, merece la pena destacar cinco de ellas por su relevancia y vinculación con la materia que nos ocupa:

1. El enfoque de la respuesta policial frente a la amenaza basado en la *explotación de la información disponible* a través de herramientas analíticas que permitan gestionar los riesgos desde la anticipación.
2. El desarrollo de un estándar de *intercambio de información* basado en el principio de disponibilidad y en la confianza mutua, siguiendo el modelo de Prüm.
3. La firme apuesta por la *innovación y la aplicación de la tecnología* que permita avanzar en la interoperabilidad de los sistemas, junto con la inversión en *formación y especialización* de los equipos humanos, con el objetivo de construir una cultura de la información compartida y basada en el intercambio de conocimientos, experiencias y buenas prácticas.
4. La complementariedad de las dimensiones externa e interna de la seguridad, lo cual demanda un *enfoque global de las relaciones de la Unión* con terceros países, organizaciones internacionales y, lógicamente, entre la PCSD y la política de desarrollo del ELSJ.
5. Y, finalmente, la *flexibilidad de la ESI-UE* como parámetro de adaptación a la realidad cambiante de la amenaza y del entorno en que se desenvuelve.

Dicho todo lo cual podemos concluir señalando que la ESI-UE, pese a que supone el primer intento serio del Consejo de generar un modelo de seguridad europeo, no pasa de ser un *documento de comunicación* que pone en valor los avances conseguidos en el ámbito del ELSJ, pero que *no logra alcanzar la relevancia de una auténtica estrategia de seguridad interior de la Unión*, entre otras cosas porque no puede imponer objetivos ni solicitar recursos más allá de los *voluntariamente* aceptados por los EEMM, auténticos responsables de la seguridad de sus ciudadanos (ARTEAGA MARTÍN, 2010, pág. 6).

3.4.5. La Agenda Europea de Seguridad (2015-2020)

Presentada en abril de 2015, la Agenda Europea de Seguridad (AES) es una revisión de la ESI-UE, de la que toma como referencia los objetivos estratégicos que "siguen siendo

Ediciones Universidad de Salamanca | CC BY-NC-ND

válidos y deben continuar persiguiéndose"[530], pero que deben ser actualizados ante la constante evolución de la amenaza, cada vez más compleja y transfronteriza que, en un mundo interconectado y globalizado con gran movilidad internacional, genera *retos comunes que exigen respuestas europeas comunes*. Asimismo, continua invariable el gran objetivo final de alcanzar una Europa más abierta y segura, que requiere el aporte de un valor añadido por cuenta de la Unión para suplementar a los EEMM quienes, en este demandante contexto, aunque principales responsables de la seguridad, ya no pueden garantizarla por sí solos.

Para materializar la consecución de este objetivo, la primera propuesta de la AES es un *enfoque colaborativo en materia de seguridad* junto con el *compromiso de todos los actores* implicados -agencias e instituciones UE, EEMM y autoridades nacionales- sobre la base de la responsabilidad compartida, la confianza mutua y la cooperación efectiva entre todos ellos.

El segundo área de acción de la AES es el *reforzamiento de los pilares de la actuación de la Unión*, mediante el mejor intercambio de información a través de sistemas técnicos compartidos que permitan el cruce de datos y la disponibilidad en tiempo real del resultado, la mayor cooperación operativa soportada sobre la evaluación conjunta de la amenaza y la definición de prioridades comunes, y la facilitación de la cooperación transfronteriza a través de la constitución de ECI, el apoyo en la tramitación de OED, las Operaciones Aduaneras Conjuntas, los Centros de Cooperación Policial y Aduanera y el reconocimiento mutuo de sentencias y resoluciones judiciales[531].

En tercer lugar, la AES plantea toda una línea de *acciones de apoyo a la formación, la investigación y la innovación* a través de propuestas como CEPOL, el Espacio Forense Europeo (ENFSI)[532] o los programas de inversión gestionados a través del FSI.

Conforme a estas áreas de actuación propuestas, la AES señala tres prioridades estratégicas para la Unión:

---

[530] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Agenda Europea de Seguridad. Estrasburgo, 28.4.2015. COM (2015) 185 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0185&rid=1 (02/12/2023).

[531] Esta misma idea ya se anticipa en el documento de la Comisión Europea de 2014 titulado "Una Europa abierta y segura: ha llegado la hora de hacerla realidad"[531], al afirmar que "los asuntos de Interior deben integrarse en la política exterior general de la UE, a fin de reforzar el diálogo y la cooperación con terceros países" como clave de estabilidad y seguridad.

[532] Con origen en el compromiso al que llegaron en el año 1992 los directores de los laboratorios forenses gubernamentales de Europa occidental para celebrar reuniones periódicas en las que discutir temas de interés mutuo, en diciembre de 2011 el Consejo de la UE aprueba la creación de un espacio europeo de policía científica y el desarrollo de infraestructuras para la misma, dando paso a la European Forensic Science Area (ENFSI), red integrada actualmente por cerca de setenta Institutos forenses europeos con el objetivo de garantizar que la calidad, el desarrollo y la prestación de servicios de policía científica en toda Europa estén a la vanguardia mundial. Disponible en: https://enfsi.eu/ (02/12/2023)
En este sentido es interesante el *Proyecto de conclusiones del Consejo sobre la concepción de una policía científica europea para 2020*, con la creación de un espacio europeo de policía científica y el desarrollo de infraestructuras para dicha policía en Europa, 12391/2/11 REV 2 ENFOPOL 229 COPEN 209, de 1 de diciembre de 2011. Disponible en: https://data.consilium.europa.eu/doc/document/ST-17537-2011-INIT/es/pdf (02/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

1. La lucha contra el terrorismo y la prevención de la radicalización.
2. El desmantelamiento de la delincuencia organizada.
3. Y la lucha contra la ciberdelincuencia, que escala en la gradación de las amenazas pasando a compartir el mismo nivel de atención que lacras como el terrorismo y el crimen organizado, lo que demuestra la cada vez mayor concienciación sobre este desafío en el ciberespacio, que la ESI-UE vislumbraba a través del prisma de la confiabilidad y la AES vigila ya como fuente de riesgo real y efectivo.

Para asegurar el éxito de la AES, se indica como camino a seguir el que transcurre guiado por un enfoque europeo conjunto, con una perspectiva global del entorno por el que transita y que, sobre todo, que debe recorrerse acompañado porque, de otra forma, no puede alcanzarse el destino: el *espacio europeo de seguridad*.

Cuando el Parlamento adopta la AES[533], hace una serie de consideraciones que inciden sobre la nueva realidad de la seguridad y las amenazas que la hostigan, cuya respuesta exige un esfuerzo conjunto, con un enfoque flexible y adaptativo, basado en la capacidad de reacción y en la utilización de las innovaciones tecnológicas a nuestro alcance, junto con la articulación de un procedimiento de revisión regular de las acciones fijadas para la aplicación de la estrategia de seguridad, en línea con lo establecido en el artículo 222.4 TFUE[534].

De esta forma, podemos concluir que la AES hereda el espíritu que animaba a la ESI-UE, es decir, sigue siendo un buen *documento comunicativo* de las líneas de avance orquestadas para afianzar el ELSJ y que los ciudadanos constaten la relevancia de su seguridad en el marco de las políticas europeas, pero sigue estando limitada en origen por el *carácter nacional de la seguridad interior* y su consustancial imbricación con el férreo núcleo central de la soberanía de los EEMM.

3.4.6. La Estrategia de la UE para una Unión de la Seguridad (2020-2025)

Como respuesta al rápido y cambiante contexto global que conforma unas amenazas cada vez más complejas e interconectadas, y la evidencia de que la seguridad tiene implicaciones para todos los estratos sociales y afecta a todas las políticas públicas, la Comisión presenta en julio de 2020 la Estrategia de la UE para una Unión de la Seguridad (EEUS)[535].

Ante este panorama, la EEUS plantea un *enfoque holístico de la seguridad* para tratar de obtener una visión completa del horizonte de amenazas con el objetivo de proteger a

[533] Resolución del Parlamento Europeo, de 9 de julio de 2015, sobre la Agenda Europea de Seguridad (2015/2697(RSP). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2015-0269_ES.html (02/12/2023).

[534] El artículo 222 TFUE en su apartado 4 dispone que "Para asegurar la eficacia de la actuación de la Unión y de sus Estados miembros, el Consejo Europeo avaluará de forma periódica las amenazas a que se enfrenta la Unión".

[535] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE para una Unión de la Seguridad, Bruselas 24.07.2020, COM(2020) 605 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0605 (03/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

los ciudadanos europeos, sus derechos fundamentales y su prosperidad social y económica frente a los ciberataques, la delincuencia organizada y transfronteriza, el terrorismo, la amenaza híbrida y otros retos derivados de las divergencias sociales, el clima o las crisis sanitarias mundiales. Para acometerlo se diseña un plan que pretende garantía de futuro ofreciendo una *respuesta europea multidisciplinar e integrada*, con base en los valores comunes, como apoyo de las políticas de los EEMM que, cada vez más, se muestran insuficientes para proteger a sus nacionales. Este *concepto amplio de seguridad* acomete de frente contra falsas distinciones, como la tradicional entre seguridad interior y exterior, o la moderna entre el mundo físico y el digital.

La EEUS se estructura en torno a tres grandes secciones: la perspectiva de las nuevas amenazas, la respuesta conjunta frente ellas y las prioridades estratégicas para materializarla.

En cuanto al panorama europeo de *amenazas para la seguridad* en rápida transformación, la EEUS especifica las principales causas de tensión para la forma de vida de los ciudadanos en relación con su actual dependencia de los servicios esenciales, la interconexión de las infraestructuras críticas, la exposición a la ciberdelincuencia por la digitalización de la sociedad, las divergencias sociales y la polarización ideológica, el desafío industrial y la pugna por la propiedad intelectual entre los competidores sistémicos y, también, la propia evolución de las amenazas tradicionales, como el terrorismo y la delincuencia organizada.

Respecto a la *respuesta coordinada de la UE*, se presentan tres líneas de trabajo: la resiliencia del conjunto de la sociedad para hacer frente y resistir las crisis, la adecuada evaluación de la amenaza para orientar la respuesta y medir su resultado, y el compromiso de todos los actores públicos y privados en el esfuerzo de protegerse mutuamente.

Por lo que se refiere a las *prioridades estratégicas*, la Unión de la Seguridad se construye sobre cuatro pilares:

1. Un *pilar prospectivo*, que trata de crear un entorno de seguridad con garantías de futuro, con especial atención a la ciberseguridad que, desde la resiliencia y la respuesta ágil y adecuada a la realidad de la amenaza, integre a todos los sectores implicados, públicos y privados, de la UE y de los EEMM, la industria, la academia y otros actores interesados, a través de mecanismos de actuación conjunta como la European Union Agency for Cybersecurity (ENISA)[536] o la creación de un CERT-UE[537], y la aprobación de normas comunes y obligatorias

[536] Creada en el año 2004, la Agencia de la UE para la Ciberseguridad es la responsable de la puesta en práctica de la política de seguridad cibernética de la UE mediante programas de certificación, acciones de cooperación con EEMM y organismos europeos, el intercambio de conocimientos, la creación de capacidades, campañas de sensibilización y otro tipo de procedimientos para la mejora de la confiabilidad de los productos, servicios y procesos TIC que coadyuven a la seguridad y resiliencia de las infraestructuras de la Unión y protejan a la ciudadanía de las amenazas digitales. Disponible en: https://www.enisa.europa.eu/about-enisa/about/es (03/12/2023).

[537] El Computer Emergency Response Team de la UE (CERT-UE) es el equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE formado por expertos en seguridad informática, encargado de recopilar, gestionar y analizar las amenazas, vulnerabilidades e incidentes

Ediciones Universidad de Salamanca | CC BY-NC-ND

juntos a procedimientos coherentes como la Recomendación de la Comisión de Ciberseguridad sobre las redes 5G[538], las medidas para fortalecer la ciberseguridad de la UE[539] o la estrategia de la ciberdiplomacia[540].

2. Un *pilar adaptativo,* que se encarga de hacer frente a las amenazas cambiantes como la ciberdelincuencia, los contenidos ilícitos en línea y la amenaza híbrida, reforzando la concienciación y la preparación[541] ante las maniobras de manipulación de la información y el ataque a las bases de la democracia y la cohesión social, auténticas formas de debilitar la confianza en las instituciones europeas y en los gobiernos de los EEMM.
3. Un *pilar resiliente,* para proteger a los europeos frente al terrorismo, la radicalización y la delincuencia organizada, amenazas aún vigentes con gran coste social y una dimensión transfronteriza y multisectorial que exigen avanzar aún más en la coordinación de la respuesta de la Unión.
4. Un *pilar integrativo,* basado en un ecosistema de seguridad europeo sólido construido sobre el compromiso conjunto de los gobiernos, las fuerzas y cuerpos de seguridad, las autoridades judiciales, el sector privado, la comunidad educativa y los ciudadanos, en la idea de que todas las políticas y todos los sectores sociales tienen una dimensión de seguridad que se entrecruza y genera estrechos vínculos entre ellos.

---

relacionados con infraestructuras TIC, y coordinar las respuestas a incidentes de escala interinstitucional e institucional, prestando asistencia operativa especializada. Disponible en: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/computer-emergency-response-team-eu-institutions-bodies-and-agencies-cert-eu_es (03/12/2023).

[538] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el despliegue seguro de la 5G en la UE – Aplicación de la caja de herramientas de la UE. COM (2020) 50 final, de 29.1.2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0050 (03/12/2023).

[539] Comunicación conjunta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo y al Consejo sobre resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. JOIN (2017) 450 final, de 13.9.2017. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017JC0450 (03/12/2023).

[540] Proyecto de Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas ("conjunto de instrumentos de ciberdiplomacia"). Consejo de la Unión Europea 9916/17, de 7.7.2017. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/es/pdf (03/12/2023).

[541] Esta lucha contra las amenazas híbridas se articula a través de documentos como:

1) Comunicación conjunta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo y al Consejo sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea. JOIN (2016) 18 final, de 6.4.2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018 (03/12/2023).
2) Comunicación conjunta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo y al Consejo sobre aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas. JOIN (2018) 16 final, de 13.6.2018. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0016 (03/12/2023).
3) Informe conjunto de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo, al Consejo Europeo y al Consejo relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas de julio 2017 a junio de 2018. Bruselas, 13.6.2018. JOIN(2018) 14 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0014R(01) (03/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Para llevar a la práctica algunos de los objetivos fijados en la EEUS, la Comisión Europea presenta de manera paralela tres iniciativas referidas a la lucha contra el abuso sexual de menores[542], la lucha contra la droga[543] y el tráfico de armas de fuego[544], y posteriormente ha ido presentando otras complementarias como, por ejemplo, las referidas a la lucha contra la delincuencia organizada[545] y la trata de seres humanos[546]. Asimismo, se han ido definiendo las políticas de apoyo a la EEUS en el ámbito del terrorismo y la radicalización, el cibercrimen, la mejora de la cooperación policial o la innovación y desarrollo de la industria para la seguridad, conformando un enmarañado conjunto normativo que, a nuestro entender, no ayuda a eliminar obstáculos de ese tortuoso camino que debe transitarse para alcanzar el destino final, que no es otro que contar con una *política común de seguridad interior* que dote a la Unión Europea del ansiado papel de proveedor de seguridad fiable y creíble del que, por ahora, carece en la escena internacional.

En cualquier caso, no debemos dar por descartada la seguridad, ni tampoco la democracia ni los derechos que la sustentan, siendo su defensa una cuestión de corresponsabilidad de la sociedad europea en su conjunto.

3.4.7. Consideraciones sobre el modelo de seguridad interior de la Unión: ¿quién abre la caja de Pandora?

Mediatizada por razones prácticas, la construcción europea no consideró inicialmente la *seguridad interior* como elemento fundamental de dicho proceso, focalizando todo su esfuerzo integrador en el ámbito político y económico. Fue la necesidad de articular los pasos de fronteras y la colaboración policial en la lucha contra la delincuencia organizada la que, en el marco de las relaciones intergubernamentales, hizo avanzar de forma paralela acuerdos como los de Schengen y Prüm que, posteriormente, fueron integrados en los diferentes Tratados de la Unión, aunque sin un régimen único de aplicación.

---

[542] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores. COM (2020) 607 final, de 24.7.2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0607 (03/12/2023).

[543] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Agenda y Plan de Acción de la UE en materia de Lucha contra la Droga 2021-2025. Bruselas, 24.7.2020. COM(2020) 606 final. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:6e3562ed-cfee-11ea-adf7-01aa75ed71a1.0015.02/DOC_1&format=PDF (03/12/2023).

[544] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción de la UE sobre el Tráfico de Armas de Fuego 2020-2025. Bruselas, 24.7.2020. COM(2020) 608 final. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:65f0454e-cfef-11ea-adf7-01aa75ed71a1.0014.02/DOC_1&format=PDF (03/12/2023).

[545] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025. Bruselas, 14.4.2021. COM(2021) 170 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0170 (03/12/2023).

[546] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE en la lucha contra la trata de seres humanos 2021-2025. Bruselas, 14.4.2021. COM(2021) 171 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0171 (03/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Conscientes de que "Europa sólo puede, no ya sobrevivir sino, tener un lugar importante en el mundo, trabajando unida, cooperando, mejorando su calidad de vida y garantizando su seguridad frente a las amenazas y riesgos actuales y futuros, vengan de donde vengan" (PÉREZ RUBALCABA, 2011, pág. 14), se ha ido construyendo una estructura normativa europea cada vez más extensa y compleja para regular aquellos ámbitos de la política de seguridad que, en virtud de la naturaleza cambiante de la amenaza, superan la capacidad de respuesta independiente de cada uno de los EEMM que se ven abocados, en este contexto digital, híbrido y globalizado, a asumir líneas de acción conjunta más eficaces y apropiadas para alcanzar el objetivo de una Europa que protege los derechos fundamentales, más abierta y segura. Y ello siempre desde la consideración de que el mantenimiento del orden público, la salvaguarda de la seguridad interior y la protección de la seguridad nacional constituyen una *responsabilidad exclusiva de cada uno de los EEMM*, sin perjuicio de las posibles relaciones bilaterales o multilaterales entre ellos.

La complejidad resultante de construir el modelo de seguridad interior europeo sobre la base de la *cooperación* de los EEMM en proyectos de la Unión que tratan de identificar los objetivos de interés nacionales para centralizar la respuesta, obliga a la especialización tanto de las herramientas aplicadas como de las instituciones encargadas de llevarlas a la práctica. Un claro ejemplo de lo anterior es la Red de Agencias JAI, que desempeñan su actividad en áreas tan diferentes como la migración ilegal y la gestión de fronteras, la lucha contra el crimen organizado y el blanqueo de capitales, la trata de seres humanos, la ciberdelincuencia, el terrorismo o la gestión de bases de datos.

Esta disgregación por especialidad se apoya, a su vez, en un entramado de instrumentos de colaboración operativa y de sistemas de intercambio de información a través de los que planificar acciones policiales conjuntas y sacar mayor rendimiento a las bases de datos compartidas generando inteligencia. No obstante, ello no deja de ser un sucedáneo del *inexistente proyecto de una auténtica estrategia de seguridad interior de la Unió*n, diseñada desde la evaluación conjunta de la amenaza y el correspondiente establecimiento de las prioridades de la UE, el planeamiento de las consiguientes líneas de acción dirigidas y aplicadas por sus propias instituciones, para alcanzar los objetivos que garanticen su propia seguridad y la de sus ciudadanos, independientemente del Estado nacional de referencia. Este es un planteamiento hoy por hoy inviable, por cuanto los EEMM no están dispuestos a transferir las competencias que ello implicaría, tal y como se deduce de la ya de por sí complicada gestión de la agenda exterior europea o de la defensa común en las que, en principio, se puede ver más camino avanzado.

La constatación de que la integración europea, en este sentido, requiere un impulso y un compromiso político muy superior al ofrecido hasta ahora por los EEMM ya tiene reflejo en el Consejo Europeo de Tampere de 1999. Posteriormente, ha habido ventanas de oportunidad para profundizar en esta dimensión de la seguridad interior, como la ofrecida por el Tratado de Lisboa al suprimir el tercer pilar y llevar al marco comunitario cuestiones que tradicionalmente habían estado en el ámbito intergubernamental, o con la sustitución del espacio de colaboración judicial y asuntos de interior por uno más

Ediciones Universidad de Salamanca | CC BY-NC-ND

amplio y ambicioso de libertad, seguridad y justicia. No habiéndose aprovechado la inercia europeísta de aquellos momentos pretéritos, no parecen desde luego más favorables los tiempos presentes para abrir la caja de Pandora, cuando los distintos gobiernos nacionales luchan por gestionar el efecto acumulado de la enésima crisis económica, el golpe de realidad de la pandemia y una compleja guerra en suelo europeo que les obliga a posicionarse, "con el añadido de grupos populistas que utilizan a la Unión como el espantajo culpable de todos los males" (NÚÑEZ VILLAVERDE, 2022, pág. 16), esgrimiendo una narrativa que trata de convencer a los ciudadanos de que ya se ha abierto esa terrible caja.

Un paso al frente en la construcción de ese modelo de seguridad interior común supone la declaración del Presidente de la República Francesa, Emmanuel Macron, en su discurso de La Sorbona de abril de 2024, al referirse a la defensa que la UE debe hacer de sus fronteras, físicas y digitales, para proteger a sus ciudadanos, más allá de la inmigración, luchando contra el terrorismo, la criminalidad organizada y la delincuencia grave, la proliferación del odio y los radicalismos. Se trata de amenazas frente a las que debe actuarse de manera *integrada e integral*, donde las visiones parciales suponen una debilidad, hasta el punto de proponer que, para avanzar en ello, "el Consejo de Schengen se convierta en un verdadero Consejo de Seguridad Interior de la Unión"[547].

En vista de lo anterior, parece incuestionable que hay que seguir avanzando en la idea de una Europa unida por sus valores y su compromiso con la libertad y la justicia, cada vez más responsable y decidida con su propia seguridad interna, íntimamente vinculada a su política exterior y de defensa, en la búsqueda de esa trascendencia global que le va a exigir la gestión desenvuelta de los malestares que, inevitablemente, se producirán alentados por derivas nacionalistas cada vez más anacrónicas cuyas consecuencias habrá de estar aquella dispuesta a asumir. Para sobrevivir Europa debe seguir siendo ella misma, debe seguir creyendo en lo que la diferencia y la hace única: su defensa de los derechos del hombre, la democracia y el Estado de derecho. Es esa *cultura democrática*, cuyos postulados comparten como requisito *sine qua non* todos los socios europeos, la clave del éxito a la que se refirieron los impulsores del proyecto a mediados del siglo XX (FERNÁNDEZ-MIRANDA FERNÁNDEZ-MIRANDA, 2024, pág. 62).

En nuestra opinión, este paso adelante hay que darlo de manera decidida, más pronto que tarde, con el convencimiento de que, quienes permanezcan en la Unión, saldrán fortalecidos. Después de todo, una vez abierta, la esperanza fue lo único que quedó en el interior de la caja de Pandora.

3.5. La estrategia europea en el ciberespacio: dominio digital con valores

La Unión Europea es plenamente consciente de que su principal fortaleza radica en la defensa de sus valores y que, para ello, la estrategia a desplegar para alcanzar el papel de agente digital relevante, autónomo e independiente en la escena internacional pasa por utilizar el *soft power*, a la sazón, el *attractive power*. A fin de cuentas, "el modelo

[547] Disponible en: https://legrandcontinent.eu/es/2024/04/25/construir-un-nuevo-paradigma-el-discurso-completo-de-emmanuel-macron-en-la-sorbona/ (26/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

europeo ha demostrado ser una fuente de inspiración para muchos otros socios de todo el mundo en su lucha contra los retos políticos, lo que no debería ser diferente en el ámbito de la digitalización"[548].

Pero el recurso al *soft power* no es suficiente para alcanzar ese objetivo. Se requieren otros argumentos para conseguir la soberanía digital europea y construir las capacidades jurídicas, tecnológicas y sociales que la garanticen.

Por ello, la Unión comienza a ser más beligerante y activa a raíz de una serie de vicisitudes sufridas en el pasado más reciente, como las carencias evidenciadas por la pandemia del COVID 19 y la falta de *autonomía estratégica* para la adquisición de bienes de primera necesidad y recursos sanitarios esenciales; las fallas en cuanto al control y el tratamiento de datos de los ciudadanos europeos alojados en servidores fuera del ámbito de la Unión; la constante propagación de narrativas desinformadoras que desprestigian nuestras instituciones y desgastan nuestras democracias; las injerencias externas que tratan de condicionar nuestras políticas; los ciberataques que diariamente sufrimos en las infraestructuras y servicios esenciales que sostienen la economía de nuestras empresas y el bienestar de nuestras sociedades; o el salto cualitativo que supone la invasión rusa de Ucrania y el inicio de una nueva guerra de aspecto convencional en suelo europeo que, no por casualidad, comienza con acciones ofensivas en el ciberespacio, en el marco de una estrategia híbrida orquestada por el Kremlin que pone sobre el tablero de juego todas las piezas que se pueden mover en los diferentes niveles que conforman el moderno conflicto entre Estados: los tradicionales dominios físicos -tierra, mar y aire-, el espacio ultraterrestre, el ciberespacio y el ámbito cognitivo.

La consecuente reacción de la UE para tratar de recuperar el control sobre su dominio digital se construye en torno a dos ejes principales: 1) el alineamiento con el Derecho Internacional; 2) y la definición de una línea de acción común europea basada en el diseño de un orden normativo acorde con ella. A esto hemos añadir una consideración que pone de relieve el profesor Coello de Portugal y que, sin duda, tiene honda repercusión en el rápido avance que la Unión ha tenido en la configuración de su respuesta:

> "[…] al ser el ciberespacio un ámbito nuevo de confrontación propio de la era digital, constituye el primer espacio de posible acción bélica que nace después del diseño de una política de defensa propia de la UE, por lo que la cooperación en este entorno, no ha habido que comunitarizarla desde una actividad convencional, sino que es el primer ámbito bélico que nace ya comunitarizado entre los veintisiete, en un contexto consolidado de previa cooperación en materia de defensa" (COELLO DE PORTUGAL, 2024, pág. 104).

En cuanto al primero de los ejes de acción, referido al alineamiento con el Derecho Internacional, la Unión considera que su estrategia en el ciberespacio debe avanzar alineada con los principios de la Carta de las NNUU para alcanzar un mundo pacífico,

[548] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Configurar el futuro digital de Europa. Bruselas, 19.2.2020. COM(2020) 67 final. Página 13. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0067&from=en (05/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

justo y sostenible *dentro del marco del Derecho Internacional* no solo en el ámbito físico sino, también, en el plano digital a través de un ciberespacio global y abierto, para lo cual la Organización debe seguir promoviendo el comportamiento responsable de los Estados[549] en el *quinto dominio*, sobre la base de las consideraciones del *Grupo de Trabajo sobre desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional*[550] y el respeto de los derechos humanos fundamentales digitales conforme a lo establecido en la *Resolución del Consejo de Derechos Humanos de 28/16 sobre el derecho a la privacidad en la era digital*[551], donde se da carta de naturaleza al Relator Especial en esta materia con el objetivo de crear un entorno digital mundial más seguro.

Respecto a la definición de la *política de ciberseguridad de la UE y el marco normativo de soporte*, la clave es la *unidad de acción* para tratar de vertebrar la respuesta coordinada y conjunta frente a los nuevos riesgos emergentes a través de diferentes programas, estructuras y herramientas, entre los que merece la pena destacar los siguientes:

1. La primera cita de obligada referencia es la Comunicación Conjunta de la AR/VP, de septiembre de 2017, titulada *Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE*[552], en la que se incluyen medidas de amplio espectro para impulsar estructuras de resiliencia frente a ciberataques y capacidades de ciberseguridad, al tiempo que se procura una cobertura legislativa penal más eficaz y el refuerzo de la estabilidad global mediante la cooperación internacional, objetivos que presenta el propio documento:

> "Si bien los Estados miembros siguen siendo responsables de su seguridad nacional, la dimensión y la naturaleza transfronteriza de la amenaza constituyen un motivo poderoso para una actuación de la UE que ofrezca incentivos y respaldo a los Estados miembros a fin de desarrollar y mantener más y mejores capacidades nacionales de ciberseguridad, a la vez que se crea una capacidad a nivel europeo. Este enfoque pretende animar a todos los actores –la UE, los Estados miembros, la industria y los particulares– a otorgar a la ciberseguridad

[549] Así se manifiesta el AR/VP, por ejemplo, en su informe de junio de 2021 sobre la implantación de la Estrategia Europea de Ciberseguridad para la Década Digital, Joint Communication to the European Parliament and the Council. Report on implementation of the EU´s Cybersecurity Strategy for the Digital Decade. High Representative of the Union for Foreign Affairs and Security Policy. Brussels, 23.6.2021. JOIN(2021) 14 final. 2021/0166 (NLE). Páginas 1, 4 y 5. Disponible en: https://digital-strategy.ec.europa.eu/en/library/first-implementation-report-eu-cybersecurity-strategy (03/03/2024).

[550] Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. General Assembly. Conference room paper. A/AC.290/2021/CRP.2. 10/03.2021. Disponible en: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (03/03/2024).

[551] Resolución aprobada por el Consejo de Derechos Humanos 28/16. El derecho a la privacidad en la era digital. Asamblea General. A/HRC/RES/28/16. 1 de abril de 2015. Disponible en: https://documents.un.org/doc/undoc/gen/g15/068/81/pdf/g1506881.pdf?token=eXb0gJGhrPqnSyVKYd&fe=true (03/03/2024).

[552] Comunicación Conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 13.09.2017. JOIN(2017) 450 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017JC0450 (06/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> la prioridad que necesita para aumentar la resiliencia y dar una mejor respuesta de la UE a los ciberataques. Proporcionará medidas concretas para ayudar a detectar e investigar cualquier forma de incidente cibernético contra la UE y sus Estados miembros, así como para dar una respuesta adecuada, en particular persiguiendo a los delincuentes. Permitirá que la acción exterior de la UE promueva eficazmente la ciberseguridad a escala global. El resultado será un giro en la estrategia de la UE, que pasará de un enfoque reactivo a uno proactivo a fin de proteger la prosperidad, la sociedad y los valores europeos, así como los derechos y las libertades fundamentales, dando respuesta a las amenazas presentes y futuras"[553].

2. También es necesaria la cita a la Directiva SRI[554], primera norma jurídicamente vinculante a nivel de la UE en el ámbito de la ciberseguridad que tuvo que ser integrada en las legislaciones de todos los EEMM antes del 9 de mayo de 2018, que establece cinco tipo de medidas concretas: 1) la adopción por todos los EEMM de una estrategia de seguridad de redes y sistemas de información; 2) la cooperación para el intercambio de información entre los EEMM y la definición de una estrategia de ciberseguridad común; 3) la creación de una red CSIRT europea; 4) la definición de las condiciones de seguridad que deben cumplir los operadores de servicios esenciales y proveedores de servicios digitales; 5) y las obligaciones de las autoridades nacionales en la materia. Esta Directiva es sustituida en 2022 por una nueva, la Directiva SRI2[555] que refuerza y unifica los requerimientos de seguridad a los sujetos obligados, simplifica sus obligaciones de notificación para reducir la carga administrativa, e introduce medidas de supervisión y requisitos de aplicación más rigurosos.

3. La Comunicación de la Comisión, de febrero de 2020, denominada *Configurar el futuro digital de Europa*[556], en la que abiertamente se aboga por la soberanía tecnológica europea como forma de reducir la dependencia exterior respecto a tecnologías cruciales para nuestro desarrollo, nuestra seguridad y la defensa de nuestras normas y valores en la era digital, de forma que:

> "La soberanía tecnológica europea no se define contra nadie, se centra en las necesidades de los europeos y del modelo social europeo. La UE permanecerá abierta a quien esté dispuesto a respetar las normas y a

[553] IBIDEM, páginas 3 y 4.

[554] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Diario Oficial de la Unión Europea. 19.7.2016. L 194/1. Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf (06/03/2024).

[555] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555 (06/03/2024).

[556] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Configurar el futuro digital de Europa. Bruselas, 19.02.2020. COM(2020) 67 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020DC0067 (03/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> cumplir los estándares europeos, independientemente de su lugar de establecimiento"[557].

En este programa se incluyen iniciativas y actividades para impulsar la financiación del proceso de digitalización[558], acelerar la transformación digital de la economía, la industria y la sociedad europeas[559], promover el acceso gratuito a la conectividad WiFi en los espacios públicos[560] y favorecer la investigación a largo plazo sobre tecnologías futuras y emergentes[561], que tendrán posterior desarrollo a través de planes presupuestarios específicos.

4. La *Estrategia de Ciberseguridad de la UE para la Década Digital*, de diciembre de 2020[562], en la que se da amplio tratamiento al complejo entorno de amenazas para la seguridad de los europeos que, desde la interconexión de los sistemas de redes e información, pueden afectar a los transportes, la energía, la salud, las telecomunicaciones, las finanzas, la seguridad pública, los procesos democráticos, el espacio o la defensa nacional. Este panorama de amenazas se ve agravado por la tensión geopolítica que subyace al control de las tecnologías, el dominio de los datos y el incremento de los ciberataques como materialización de la amenaza híbrida entre Estados, concluyendo que:

> "[…] la mejora de la ciberseguridad es esencial para que las personas confíen, utilicen y se beneficien de la innovación, la conectividad y la automatización, y para salvaguardar los derechos y libertades fundamentales, incluidos los derechos a la privacidad y a la protección de los datos personales, y la libertad de expresión e información"[563].

5. En este mismo sentido, en el Informe del AR/VP sobre la *Implementación de la Estrategia de Ciberseguridad*, de junio de 2021[564], se refieren medidas concretas

[557] IBIDEM, página 2.

[558] Los siete programas presupuestarios de la UE más relevantes para el impulso de la digitalización son el Programa Europa Digital, el Mecanismo "Conectar Europ"-Digital, el Horizonte Europa, el InvestEU, la Europa Creativa MEDIA, el EU4Health y el Mecanismo de Recuperación y Resiliencia. Disponible en: https://digital-strategy.ec.europa.eu/es/activities/funding-digital (03/03/2024).

[559] Este es el Programa Europa Digital, que puede consultarse en Programa Europa Digital. Disponible en: https://digital-strategy.ec.europa.eu/es/activities/digital-programme (03/03/2024).

[560] Este es el Programa WiFI4EU. Disponible en https://digital-strategy.ec.europa.eu/es/activities/wifi4eu (03/03/2024).

[561] Este es el Programa FET FLAGSHIPS, que a fecha de consulta tiene en marcha proyectos de desarrollo de baterías de alto rendimiento, de comprensión del cerebro humano, de nuevos usos y aplicaciones para el grafeno, y de desarrollo y adopción de tecnologías cuánticas. Disponible en: https://digital-strategy.ec.europa.eu/es/activities/flagships (03/03/2024).

[562] Comunicación Conjunta al Parlamento Europeo y al Consejo. La Estrategia de Ciberseguridad de la UE para la Década Digital. Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 16.12.2020. JOIN(2020) 18 final. Disponible en: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (03/03/2024).

[563] IBIDEM, página 4.

[564] Joint Communication to the European Parliament and the Council. Report on implementation of the EU´s Cybersecurity Strategy for the Digital Decade. High Representative of the Union for Foreign Affairs and Security Policy. Brussels, 23.6.2021. JOIN(2021) 14 final. 2021/0166 (NLE). Disponible en: https://digital-strategy.ec.europa.eu/en/library/first-implementation-report-eu-cybersecurity-strategy (03/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

en el marco de la ciberseguridad, como la red de Centros de Operaciones de Seguridad (SOC) nacionales y transfronterizos de la UE para la detección temprana de ciberataques y su integración en el denominado *ciberescudo europeo*, la articulación de una respuesta colectiva, creíble y efectiva a través de la Unidad Cibernética Conjunta[565], y la acción diplomática, el intercambio de información y el diálogo con los aliados para prevenir, desalentar, disuadir y responder a la ciberamenaza[566]. Para avanzar en la *autonomía estratégica* de la UE es necesario avanzar en la *soberanía tecnológica*, para lo cual se propone aunar esfuerzos a través del impulso decidido del Centro Europeo de Competencia en Ciberseguridad (ECCC)[567], garantizar la seguridad de despliegue y funcionamiento de las redes 5G mediante la coordinación del proyecto a través de las certificaciones reguladas por la Agencia Europea de Ciberseguridad (ENISA), o el Plan de Acción de Educación Digital de la UE para formar y concienciar a los ciudadanos respecto a las ventajas y riesgos que la nueva era digital comprende[568]. Finalmente, en el plano operativo, se refiere a la mejora de la cooperación en materia de ciberdelincuencia y obtención de evidencias digitales que cristaliza en el Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas, de febrero de 2023[569]. En línea con todo ello y en el marco de la Presidencia Española del Consejo de la UE, en diciembre de 2023 el Comité de Representantes Permanentes de los Gobiernos de los EEMM (COREPER) alcanzan una posición común sobre el denominado Reglamento de Cibersolidaridad[570], que busca reforzar "las capacidades de la UE y de los Estados miembros para prepararse contra las ciberamenazas y los ataques a gran escala,

[565] La Unidad Cibernética Conjunta busca fortalecer la cooperación entre las instituciones, organismos y agencias competentes en el ámbito de la ciberseguridad en todos los EEMM, para aprovechar todo su potencial y conseguir aunar esfuerzos y capacidades frente a la ciberamenaza. Disponible en https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit (03/03/2024).

[566] Joint Communication to the European Parliament and the Council. Report on implementation of the EU´s Cybersecurity Strategy for the Digital Decade. High Representative of the Union for Foreign Affairs and Security Policy. Brussels, 23.6.2021. JOIN(2021) 14 final. 2021/0166 (NLE). Página 2. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021JC0014 (03/03/2024).

[567] European Cybersecurity Competence Centre and Network (ECCC), cuyo objetivo es aumentar las capacidades y la competitividad de la ciberseguridad en la Unión, junto con la Red de Centros Nacionales de Coordinación, apoyando la innovación y la investigación en proyectos estratégicos de ciberseguridad, para alcanzar la soberanía tecnológica europea. Disponible en: https://cybersecurity-centre.europa.eu/index_en (03/03/2024).

[568] Página oficial del Plan de Acción de Educación Digital de la UE. Disponible en: https://education.ec.europa.eu/es/focus-topics/digital-education/action-plan (03/03/2024).

[569] Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas. DOUE núm. 63, de 28 de febrero de 2023. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80291 (03/03/2024).

[570] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos. Expediente interinstitucional 2023/0109(COD). Bruselas, 20 de abril de 2023. 8512/23. Disponible en: https://data.consilium.europa.eu/doc/document/ST-8512-2023-INIT/es/pdf (06/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

prevenirlos, responder a ellos y recuperarse de ellos de una manera más eficiente y efectiva"[571].

6. En otro orden de cosas, el *Plan de Acción sobre las sinergias entre las industrias civil, de la defensa y espacial*, de febrero de 2021[572], cifra su objetivo en contribuir al desarrollo de tecnologías críticas estratégicas que permitan afrontar las ciberamenazas y los nuevos retos tecnológicos a través del aumento de las capacidades de inteligencia como, por ejemplo, la computación cuántica, cuya capacidad para procesar grandes volúmenes de información y resolver problemas de cálculo complejos suponen un salto cualitativo en la encriptación y securización de las comunicaciones[573], elementos esenciales para, entre otras cuestiones, disponer de *autonomía de mando y control* de las Fuerzas Armadas en el espacio ultraterrestre, y producir inteligencia que permita gestionar desde la anticipación y el conocimiento las crisis generadas por cualquier tipo de amenaza en los dominios del espacio y el ciberespacio.

7. Finalmente, en abril de 2023 la Comisión Europea adopta una propuesta de *Ley de Cibersolidaridad de la UE*[574] para reforzar la labor de coordinación de acciones de detección, respuesta y recuperación frente a ciberincidentes importantes o de gran escala, para lo cual se propone la puesta en funcionamiento del *Ciberescudo Europeo* -conformado por los SOC nacionales- y de un *mecanismo de emergencia de ciberseguridad* que articule medidas preventivas y preparatorias, contemple la existencia de una estructura operativa de reserva lista para intervenir en caso de necesidad, y la prestación de ayuda financiera para favorecer la asistencia mutua, todo ello apoyado desde ENISA por un mecanismo de revisión de incidentes de ciberseguridad para sacar lecciones aprendidas y compartir el conocimiento. Al mismo tiempo, la Comisión presenta la propuesta de la *Academia de Cibercapacidades*, orientada al impulso de capacidades y la gestión coordinada del talento, como requisitos previos para impulsar la resiliencia de la Unión.

---

[571] Comunicado de Prensa del Consejo de la UE, de 20 de diciembre de 2023, haciendo referencia a las declaraciones del Ministro de Transformación Digital de España, José Luis Escrivá. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/12/20/cyber-solidarity-act-member-states-agree-common-position-to-strengthen-cyber-security-capacities-in-the-eu/ (06/03/2024).

[572] Plan de Acción sobre las sinergias entre las industrias civil, de la defensa y espacial, de febrero de 2021. Bruselas, 22 de febrero de 2021. COM(2021) 70 final. Disponible en: https://commission.europa.eu/document/download/2353ded9-0e39-4d35-a46c-67c62779afe1_es?filename=action_plan_on_synergies_es.pdf (03/03/2024).

[573] En este sentido se trabaja en la iniciativa EuroQCI, para construir una infraestructura de comunicaciones cuántica segura que abarque todo el territorio de la UE, incluido ultramar, utilizando para ello las mejores tecnologías terrestres y espaciales que los EEMM de la Unión por sí mismos puedan desarrollar. A esta iniciativa se refiere el AR/VP en su informe de junio de 2021 sobre la implantación de la Estrategia Europea de Ciberseguridad para la Década Digital.
Joint Communication to the European Parliament and the Council. Report on implementation of the EU´s Cybersecurity Strategy for the Digital Decade. High Representative of the Union for Foreign Affairs and Security Policy. Brussels, 23.6.2021. JOIN(2021) 14 final. 2021/0166 (NLE). Página 2.

[574] Nota de prensa. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/cyber-solidarity (13/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

De igual forma, se antoja determinante la adecuada catalogación y distinción de las acciones en el ciberespacio que deban ser consideradas como *ataques de alto nivel*, con afectación a objetivos o valores esenciales de la Unión, de aquellos otros que por su origen, intención o consecuencias no supongan más que un simple incidente mitigado por los mecanismos de defensa ordinarios establecidos. En este sentido, el *enfoque conceptual* elegido para ubicar los ciberataques en su contexto resulta esencial, tal y como recoge el documento publicado en febrero de 2021 por la Comisión Europea y el Hybrid CoE, titulado *The Landscape of Hybrid Threats: a conceptual model*:

> "[…] In particular, cyber crisis management mechanisms could benefit from the conceptual approach in order to put cyber-attacks into the right context. It is important to distinguish between cyber activities that are uncoordinated and isolated events, and cyber activities that form part of a wider plan with the objective to extract critical information about infrastructures or the personal data of political leaders and decision- makers. At the EU level, there are already some elements in this direction with the «Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises»"[575] (GIANNOPOULOS, SMITH, & THEOCHARIDOU, 2021, pág. 44).

En lo que respecta a la amenaza híbrida y la desinformación, fuente de grave inquietud para la Unión, su respuesta se viene configurando desde 2016 a través de la *Comunicación Conjunta del AR/VP sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea*[576] en la que expresamente se reconoce que "la lucha contra las amenazas híbridas constituye un asunto de defensa y seguridad nacional y de mantenimiento del orden público"[577] por lo que recae en el marco de responsabilidad de cada uno de los EEMM, lo cual no implica que dicha amenaza no pueda ser combatida de manera más eficaz desde un *enfoque integral a escala de la UE* desde los principios de solidaridad y asistencia mutua que estipula el TUE. Propone veintidós ámbitos de actuación desde los que afrontar la amenaza híbrida y desarrollar la resiliencia tanto de la Unión como de los EEMM y sus socios internacionales.

Abundando en este planteamiento, se busca la cooperación con la Alianza Atlántica, estructura coincidente en miembros integrantes e intereses en la lucha contra esta amenaza, al menos hasta ahora. Elemento esencial para articular esta política de defensa común es la creación del Centro Europeo de Excelencia Contra las Amenazas

[575] "En concreto, los mecanismos de gestión de crisis cibernéticas podrían beneficiarse del enfoque conceptual para situar los ciberataques en el contexto adecuado. Es importante distinguir entre las actividades cibernéticas que son eventos descoordinados y aislados, y las actividades cibernéticas que forman parte de un plan más amplio con el objetivo de extraer información crítica sobre infraestructuras o datos personales de líderes políticos y tomadores de decisiones. A nivel de la UE, ya existen algunas herramientas en esta dirección con el «Plan para la respuesta coordinada a incidentes y crisis de ciberseguridad transfronterizos a gran escala»" (Traducción propia).

[576] Comunicación Conjunta al Parlamento Europeo y al Consejo, sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea. Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 6.4.2016. JOIN (2016) 18 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018 (04/03/2024).

[577] IBIDEM, página 2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Híbridas (Hybrid CoE)[578], en cuyo seno se organizan grupos de interés[579], se programan ejercicios de entrenamiento y formación, y se llevan a cabo tareas de análisis e investigación con el objetivo de avanzar en el conocimiento del entorno, la naturaleza compleja de la amenaza híbrida y las opciones de respuesta.

En línea con esta estrategia, en 2018 se presenta por la Comisión Europea y la AR/VP la Comunicación Conjunta titulada *Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas*[580], en la que se hace especial hincapié en la desinformación como herramienta "perniciosa para nuestras democracias, pues merma la capacidad de los ciudadanos para decidir con conocimiento de causa y participar en el proceso democrático"[581], buscando intensificar la respuesta conjunta ante estas amenazas cambiantes a través de la mejora de la capacidad de detección y de la comunicación estratégica de la información, y el desarrollo de resiliencia frente a las actividades de inteligencia hostiles, entre otras.

También debemos referirnos a la Brújula Estratégica para la Seguridad y la Defensa, que integra esta visión europea de la ciberseguridad, señalando específicamente la creación de una *EU Hybrid Toolbox*[582] y la apuesta por una política de ciberdefensa común en todos los ámbitos:

> "5. Crearemos un conjunto de instrumentos de la UE contra las amenazas híbridas que reúna diferentes herramientas para detectar una amplia gama de amenazas híbridas y responder a ellas. En este contexto, desarrollaremos un conjunto de instrumentos específicos para hacer frente a la manipulación de información y la injerencia por parte de agentes extranjeros.
> 6. Seguiremos desarrollando la política de ciberdefensa de la UE para estar mejor preparados ante los ciberataques y responder mejor a ellos; reforzaremos nuestras acciones en los ámbitos marítimo, aéreo y espacial, en particular ampliando las presencias marítimas coordinadas a otras regiones, empezando por el Indo-Pacífico, y desarrollando una estrategia espacial de la UE para la seguridad y la defensa"[583].

[578] El European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), constituido en abril de 2017 y con sede en Helsinki, es un centro internacional autónomo e independiente conformado por una red de profesionales y expertos en la materia, cuya misión es fortalecer la seguridad de los Estados y organizaciones participantes, proporcionando experiencia, conocimiento y capacitación a sus miembros para contrarrestar la amenaza híbrida. El Hybrid CoE promueve desde la UE y en colaboración con la OTAN un enfoque integral y conjunto contra las amenazas híbridas que pueden afectar a sus Estados miembros -36 en la actualidad-, con la misión de fortalecer la seguridad desde la prevención y, al mismo tiempo, preparar la respuesta proporcionando experiencia y capacitación, y compartiendo información frente a las interferencias externas hostiles. Disponible en https://www.hybridcoe.fi/ (04/03/2024).

[579] Estas comunidades de interés se refieren a la influencia híbrida, la estrategia y defensa, o las vulnerabilidades y la resiliencia.

[580] Comunicación Conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo. *Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas*. Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 13.6.2018. JOIN(2018) 16 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0016 (04/03/2024).

[581] IBIDEM, página 4.

[582] Puede traducirse como Caja de Herramientas Híbridas de la UE.

[583] Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales. Bruselas,

Ediciones Universidad de Salamanca | CC BY-NC-ND

Para dar seguimiento a esta declaración de intenciones, en noviembre de 2022, el AR/VP lanza una Comunicación Conjunta sobre la Política de Ciberdefensa de la UE[584], en un contexto de guerra en territorio europeo con la agresión militar injustificada de Rusia contra Ucrania, que la Unión interpreta como claro exponente de la intención del Kremlin de "cuestionar y socavar el orden internacional basado en normas en el ciberespacio, convirtiéndolo en un ámbito cada vez más discutido, al igual que la tierra, el mar, el aire y el espacio"[585] y en la que se incide en la desdibujada frontera entre las dimensiones civil y militar de la confrontación en el ciberespacio, que exige definir la ciberdefensa de la Unión sobre cuatro pilares: 1) la asunción de mayor responsabilidad en la propia defensa a través de unas fuerzas armadas europeas modernas e interoperables; 2) afianzar la soberanía tecnológica y digital; 3) la cooperación civil y militar en el ciberespacio; 4) y la importancia del enfoque preventivo y la detección temprana de la amenaza.

Finalmente, debemos referirnos al Libro Blanco de la Defensa Europea de marzo de 2025 que, al referirse al actual entorno de competencia sistémica, señala a las amenazas híbridas como desafíos de naturaleza estratégica que requieren de respuestas de igual carácter, basadas en el desarrollo conjunto y colaborativo de capacidades bajo una línea directiva única, donde las alianzas y asociaciones defensivas tienen una importancia vital. Estas amenazas híbridas se vinculan, entre otras, con los ciberataques, el sabotaje de infraestructuras críticas submarinas, la interferencia en sistemas satelitales, la desinformación, el espionaje político e industrial o la instrumentalización de las migraciones como elemento de presión política. Frente a ellas el Plan ReArm Europe, que acompaña al Libro Blanco de la Defensa Europea, propone como requisito imprescindible el desarrollo del sector industrial europeo, incidiendo en la innovación disruptiva en campos de aplicación directa a la seguridad y la defensa como la IA, la computación cuántica, la conectividad avanzada con criptografía, las fuentes de energía alternativa y la robotización de los sistemas autónomos de defensa y ataque, entre otras. Se trata de capacidades de doble uso, donde la distinción entre lo civil y lo militar se diluye por la propia naturaleza de la tecnología. De ahí la importancia de diseñar una hoja de ruta tecnológica europea y de simplificar y armonizar la normativa reguladora.

Podemos de esta forma concluir que la Unión Europea dispone actualmente de una ambiciosa estrategia de ciberdefensa, construida sobre la asertividad y la toma de conciencia de sus pretensiones a medio y largo plazo en el ciberespacio común y global, cuyo alcance pasa, entre otras, por reducir su *dependencia digital y tecnológica* y apostar por el fortalecimiento de la base industrial interna, máxime cuando en febrero de 2024 la propia presidenta de la Comisión Europea, Úrsula von der Leyen, advierte al Parlamento Europeo que "la amenaza de guerra puede no ser inminente, pero no

21 de marzo de 2022. 7371/22. Página 3 (versión en español). Disponible en: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf (26/08/2024).

[584] Comunicación Conjunta al Parlamento Europeo y al Consejo sobre la Política de Ciberdefensa de la UE. Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 10.11.2022. JOIN(2022) 49 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022JC0049 (06/03/2024).

[585] IBIDEM, página 1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

imposible”[586]. La asertividad del complejo entorno digital y multipolar ha servido, nuevamente, de acicate para la reacción de los veintisiete.

[586] Palabras de la presidenta de la Comisión Europea ante el Parlamento de la Unión el 28 de febrero de 2024, en el contexto de las declaraciones de Putin amenazando con el uso de armas nucleares si la UE envía tropas a Ucrania. Disponible en: https://www.aquieuropa.com/noticia/72706-von-der-leyen-advierte-de-que-la-amenaza-de-guerra-puede-no-ser-inminente-pero-no-imposible https://www.publico.es/internacional/von-der-leyen-llama-al-rearme-ue-amenaza-guerra-no-sea-inminente-no-imposible.html https://www.msn.com/es-es/noticias/internacional/von-der-leyen-la-guerra-no-es-imposible/ar-BB1j33I4 (03/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 4. LA SEGURIDAD ESPAÑOLA: MODELO INTEGRAL E INTEGRADO DE RESPUESTA A LOS DESAFÍOS TRADICIONALES Y DEL CIBERESPACIO

Hasta aquí hemos presentado, en primer lugar, el concepto de *soberanía* y su correlación con la autonomía del Estado nación moderno, tradicionalmente reconocido como el único detentador del ejercicio del *imperium* para la administración del Estado, promovedor de los intereses comunes y guardián de los medios y las fuerzas que garantizan su seguridad y le permiten, incluso, limitar la libertad individual de sus ciudadanos (MEINECKE, 2014, págs. 3-16) los cuales, a cambio, quedan amparados por la égida de la *nacionalidad* que, en el sentido de ciudadanía del Estado, "refleja la tradición anglosajona y francesa de la Nación como territorio del pueblo soberano" (GÖRLITZ, 1980, pág. 403) y proyecta su contenido a través de la *seguridad nacional*.

Sin embargo, como lógica consecuencia de la aparición del ciberespacio como dominio común y global en el que se desarrollan nuevas formas de relaciones humanas, con sus pros y sus contras, el clásico enfoque del *poder soberano* se enfrenta al desafío de buscar su encaje en esta extraña dimensión que no juega con las mismas reglas acostumbradas hasta finales del siglo XX, para lo cual evoluciona hacia el concepto de *soberanía digital* tratando de hacer efectivo su rol prevalente entre todos los actores involucrados en la gobernanza de Internet, como forma de asegurar los derechos de sus ciudadanos y de procurar el beneficio de la sociedad en su conjunto.

Continuamos nuestro estudio considerando los efectos catárticos de la evolución y el aumento de esta nueva amenaza que, superando los intereses exclusivos del Estado, va centrando el foco de atención en los derechos individuales de la persona hasta llegar a mediados de la década de 1990 al concepto de *seguridad humana*, a partir del cual, con el apoyo de los informes de Naciones Unidas sobre el Desarrollo Humano como marco teórico, se consolida una nueva visión de la seguridad nunca antes analizada que cristaliza en la Agenda 2030 y los ODS, que añaden al tablero de juego un nuevo concepto: la *resiliencia* (GARCÍA CANTALAPIEDRA, 2023, págs. 61-62).

Seguidamente hemos tenido ocasión de ahondar en el actual orden mundial y los retos que lo definen a través de la perspectiva que aportan estructuras supranacionales nacidas no ya de la soberanía sino, al contrario, del compromiso cooperador entre aquellos otrora Estados egoístas únicamente guiados por su propio interés que, ahora, miden su éxito ganando perfil e influencia en el escenario político mundial, posición que les permite consolidar la seguridad y el bienestar de sus ciudadanos impulsando esa interdependencia que les resta autonomía al tiempo que, paradójicamente, les hace ganar soberanía (BECK, 2003, págs. 48-50).

Es así que, como señala la profesora Serra Cristóbal, los riesgos globales del siglo XXI obligan a los Estados a enfrentar un nuevo entorno estratégico abierto, incierto y generador de inseguridad, para cuya respuesta "las medidas a adoptar pueden ser de

Ediciones Universidad de Salamanca | CC BY-NC-ND

distinta naturaleza, pero casi todas ellas han venido auspiciadas por la necesidad de garantizar la seguridad nacional" (SERRA CRISTÓBAL, 2015, pág. 75)

Por ello, en esta era digital, de riesgos deslocalizados y amenazas multidimensionales, el único camino hacia la seguridad nacional parece ser, precisamente, trascender la dimensión nacional del Estado para enfocar su supervivencia a través de la cooperación intergubernamental y la resiliencia como capacidad de las sociedades y las estructuras del Estado para resistir y recuperarse lo antes posible ante las crisis. Ha sido en este contexto de transformación global y permanente adaptación a los modernos desafíos donde se han analizado organizaciones internacionales como NNUU, la OTAN y la UE que, entre otras, definen el marco geopolítico y cultural en el que arraiga el entramado de relaciones de poder e influencia, políticas, económicas y estratégicas a través de las que España articula la defensa de sus intereses nacionales.

Es por todo ello que debamos ahora centrarnos en el estudio de la *seguridad nacional*, acotando nuestra investigación al ámbito de España que, como Estado democrático y europeista, debe disponer de una estrategia que ofrezca una respuesta integral a los riesgos y amenazas actuales de carácter multifacético entre los que, junto a los tradicionales, como tendremos ocasión de analizar más adelante, se encuentran nuevas preocupaciones como el cambio climático, la energía, la estabilidad económica, el ciberespacio, las redes de transporte o la credibilidad de las instituciones democráticas y sus procesos atacados, cada vez más, por estrategias híbridas de nuevo cuño a las que nunca antes nos hemos enfrentado y donde ocupa un lugar preferente la desinformación, punto focal de la hipótesis que sustenta nuestra tesis.

Finalmente, debemos señalar que la toma de decisiones en materia de seguridad nacional se ve influenciada por distintos factores, de carácter específico e íntimamente ligados a cada país, como su cultura estratégica -relaciones internacionales, alianzas, historia militar, cultura social de seguridad, etc.-, las amenazas de seguridad tanto internas como externas, reales o percibidas -contexto geoestratégico y políticosocial propio-, la disposición de presupuesto y medios para afrontar dichas amenazas, las limitaciones particulares para articular la respuesta -normativas, políticas, culturales-, o la voluntad de gobierno que, en cada momento, determina cuál es la decisión estratégica a adoptar (VEIGA GASALLA, 2024, pág. 6).

4.1. La seguridad como concepto y la Policía como institución en el constitucionalismo histórico español

Visto ya el encaje de la seguridad en el marco de poder estatal, donde se percibe como una necesidad humana que aquel está obligado a garantizar, procede ahora analizar su inclusión en el texto constitucional, a cuya razón de ser podemos acercarnos a través del artículo 16 de la Declaración de Derechos del Hombre y del Ciudadano, aprobada por la Asamblea Nacional constituyente francesa de 26 de agosto de 1789, que advierte:

> "Una Sociedad en la que no esté establecida la garantía de los Derechos, ni determinada la separación de los Poderes, carece de Constitución".

Ediciones Universidad de Salamanca | CC BY-NC-ND

Es por ello que la clave del arco de bóveda constitucional sea la pieza que representa la división de poderes, emplazados en órganos independientes que se controlan entre sí para garantizar los derechos de los ciudadanos. Este es el contexto que nos permite aproximarnos a la definición de la Constitución en sentido positivo y de manera amplia como:

> "[…] la ley fundamental de un Estado, fijada –casi sin excepción- en un documento sólo modificable en condiciones muy estrictas, y en la que (reconociendo el principio de división y limitación de los poderes legislativo, ejecutivo y judicial) se establecen normas jurídicas que regulan la distribución, la estructura, las competencias y las funciones de los más altos órganos del Estado y que, además, garantizan las importantísimas libertades individuales frente a los tres poderes públicos" (GÖRLITZ, 1980, pág. 115).

Las constituciones modernas son herederas del liberalismo burgués cuyos más tempranos exponentes son las constituciones de Estados Unidos de 1787 y de Francia de 1791, que se ocupan de la *paz del pueblo* anticipando lo que hoy entendemos como *seguridad ciudadana y nacional*. El objeto de estas primeras constituciones no es otro que organizar la estructura del Estado en aras a la mejor garantía posible de los derechos y libertades por entonces recién definidos, para lo cual se entiende necesaria la división de poderes y la prevalencia de la ley frente a todos. Gracias a ello, en la segunda mitad del siglo XX ya existe "una tradición jurídica de la que echar mano para formular la irrenunciabilidad del derecho a la seguridad de todo ser humano y la obligación del Estado de respetar la libertad de la persona y su patrimonio, de *proteger* frente a terceros tales bienes jurídicos y de garantizar *todos los demás derechos* del ciudadano" (MARTÍNEZ QUINTEIRO, 2018, pág. 51).

Por su parte, el parlamentarismo español está jalonado de Constituciones *partidistas* que tratan de reflejar en su articulado el ideario político de turno, ignorando aquellos sectores de la sociedad que no se sienten representados y que, por ello, conforme cambia el signo del partido en el poder buscan aprobar una nueva norma fundamental con la que identificarse (Dirección de Estudios, Análisis y Publicaciones de la Secretaría General del Congreso de los Diputados, 2022)

4.1.1. De la Constitución de Cádiz a la II República

La Constitución de Cádiz de 1812 es la primera Constitución propiamente española, aprobada en el periodo de la Guerra de la Independencia y, lógicamente, marcada por el hecho de la invasión napoleónica y las tendencias jurídicas afrancesadas[587]. Aunque no define expresamente un catálogo de derechos del que puedan disfrutar los ciudadanos españoles, que son soberanos, sí considera que el objeto principal del gobierno es procurar la *felicidad* y el *bienestar colectivo*, en clara alineación de intenciones con el reconocimiento que tanto la *Declaración de Derechos de V*irginia de 1776 como la *Declaración de los derechos del hombre y del ciudadano* de 1789 hacen de

[587] Para el análisis de la evolución histórica constitucional española de este capítulo se ha recurrido a la documentación que ofrece en su página web el Congreso de los Diputados. Disponible en: https://www.congreso.es (10/05/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

los derechos a la vida, a la libertad, a la propiedad y a la búsqueda de la felicidad y la seguridad, dentro de una concepción hobbesiana de la sociedad orientada al bienestar de sus componentes.

Merece destacada mención que apenas doce años después de nuestra primera Constitución, y también influida por la tradición francesa, por Real Cédula de 13 de enero de 1824 se crea la *Superintendencia General de Policía del Reino*, que "diseña las coordenadas de actuación y competencias de la policía como organización, como institución del Estado que se ha mantenido desde 1824 hasta hoy" (HERRERO FERNÁNDEZ-QUESADA & TURRADO VIDAL, 2023, pág. 60) y que, por ello, constituye el origen histórico de la moderna Policía Nacional española.

Estas competencias, influidas por el momento histórico de transición en el que se definen, serán para "entre otras, reprimir el espíritu de sedición, extirpar los elementos de discordia y desobstruir todos los manantiales de prosperidad" (DE ANTÓN LÓPEZ, 2000, pág. 22)[588], como Policía de naturaleza civil, autónoma y laica, con dos vertientes diferenciadas, la primera y fundamental de ellas relacionada con la función disuasoria y orientada a la resolución de conflictos ciudadanos, y la segunda vertiente relativa a la Policía administrativa, en cuanto encargada de la expedición y control de los documentos de identidad y viaje (TURRADO VIDAL M. , 2023, págs. 42-47), en lo que viene a ser un intento de asegurar un entorno pacífico que permita el progreso que las ideales liberales de la época buscan alcanzar, paradójicamente utilizadas por Fernando VII, impulsadas por la necesidad institucional en materia de seguridad pública que se había dejado sentir tanto en el Sexenio Absolutista como en el Trienio Constitucional[589].

Esta *Superintendencia General de Policía*, conforme al desarrollo dado por el Reglamento de Policía de 22 de febrero de 1824, se despliega por todo el Estado a través de *Intendencias* y *Subdelegaciones*[590], conforme a la mayor o menor entidad del territorio afectado:

[588] Como recoge Julio de Antón en su libro *Historia de la Policía Española*, página 22, "entre las atribuciones privativas de esta Policía figuran formar padrones de vecindario, expedir y visar pasaportes de viajeros nacionales, venta ambulante en la calle, hospederías, armas, caza y registro de vehículos. Otras atribuciones que comparte esta Policía con otras Policías similares serían el registro de establecimientos, casas de prenda y cambios, vagos, mendigos, menores abandonados y gitanos sin domicilio, imprenta, documentación ilegal y entradas no procedentes, moral pública, persecución de ladrones y de cuadrillas, reuniones tumultuarias y asociaciones secretas, contrabando, lavadores públicos, salud pública e higiene en establecimientos y empresas, prevención de incendios, control de serenos y celadores nocturnos, y los abastos de los pueblos".

[589] El propio autor, Martín Turrado Vidal, en conversación particular el 09/03/2024 nos aporta más detalles indicando que, en el Trienio Constitucional, se culpó al Ministerio de la Gobernación de la falta de seguridad en todo el país y de no poder mantener el orden en los procesos electorales, pero se le negó una Policía a su disposición para poder darle solución. Fernando VII, de vuelta por tanto al poder absoluto, a finales de 1823 recoge estas ideas y crea un cuerpo de Policía, con lo que refuerza a los más moderados de sus partidarios (el Conde de Ofalia y Luis López Ballesteros, el Ministro de Hacienda) y llena el vacío institucional existente utilizando ideas liberales.

[590] La *Superintendencia General de Policía del Reino* conforma su despliegue a través de treinta y dos *Intendencias* de 1ª, 2ª y 3ª categoría, y ciento veintitrés *Subdelegaciones.*

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "Entre otras cosas, y justamente por eso, las estructuras policiales que se crearon en 1824 representan la primera Policía Española, el primer cuerpo policial civil y las primeras estructuras implementadas en un marco territorial amplio, en todo el reino, formándose a modo de tela de araña un sistema policial común que interactuaba y llevaba a cabo actuaciones policiales con los mismos criterios que fomentaba la progresiva profesionalización de los agentes" (HERRERO FERNÁNDEZ-QUESADA & TURRADO VIDAL, 2023, pág. 55).

Sin embargo, no todo fueron parabienes. La *Superintendencia General de Policía* nace compartiendo competencias con otras instituciones como la judicatura, el Ejército e, incluso, la Iglesia, que se ven obligadas a convivir con la nueva estructura y, lo que es peor, viendo cómo competencias que consideraban exclusivamente propias e intransferibles dejaban de serlo. Esto era cuestión seria puesto que, en muchos casos, la disminución de competencias equivalía a la reducción de ingresos[591].

Un año después, en 1825, se crea el *Regimiento de Celadores Reales:*

> "[…] como embrión de una fuerza militar que debería desplegarse por todo el territorio nacional como elemento de apoyo a las Intendencias respectivas, lo que lo convierte en el antecedente más remoto de las Unidades de Policía uniformada. Por tanto, y sin lugar a dudas, podemos considerar a los Celadores Reales como la Unidad uniformada más antigua que ha prestado servicios en la Policía Española, constituyendo un antecedente directo, también, debido a su orgánica y función, de las Unidades de Caballería de la actual Policía Nacional" (FERNÁNDEZ BARALLOBRE, 2023, pág. 49).

Por su parte, la Constitución de 1837, al igual que su predecesora, ha de vivir tiempos políticos agitados e inestables, pero ello no supone obstáculo para incorporar por primera vez en la historia constitucional del país una declaración expresa, sistemática y homogénea de derechos como, por ejemplo, el de imprimir y publicar libremente las ideas sin previa censura y con sujeción a las leyes[592], o no ser detenido ni preso sino en los casos que prescriba la ley[593], aunque en el siguiente capítulo se excepciona este derecho si la seguridad del Estado lo exige por concurrir *circunstancias extraordinarias*[594]. Igualmente, se regula el derecho de garantía jurisdiccional en base a la competencia de los Tribunales y la seguridad jurídica conforme a la necesaria existencia de ley previa al delito[595]. Es patente la referencia al Artículo 7 de la *Declaración de los derechos del hombre y del ciudadano* de 1789 en cuanto a los requisitos de la detención, con sometimiento a la ley y conforme a los procedimientos

[591] Aclaración del propio autor, Martín Turrado Vidal, en conversación particular el 09/03/2024.

[592] El artículo 2 de la Constitución de la Monarquía Española de 1837 dice que "Todos los españoles pueden imprimir y publicar libremente sus ideas sin previa censura, con sujeción a las leyes. La calificación de los delitos de imprenta corresponde exclusivamente a los Jurados".

[593] El artículo 7 por su parte establece que "No puede ser detenido, ni preso, ni separado de su domicilio ningún español, ni allanada su casa, sino en los casos y en la forma que las leyes prescriban".

[594] El artículo 8 señala que "Si la seguridad del Estado exigiese en circunstancias extraordinarias la suspensión temporal en toda la Monarquía, o en parte de ella, de lo dispuesto en el artículo anterior, se determinará por una ley".

[595] El artículo 9 garantiza que "Ningún español puede ser procesado ni sentenciado sino por el Juez ó Tribunal competente, en virtud de leyes anteriores al delito y en la formas que estas prescriban".

Ediciones Universidad de Salamanca | CC BY-NC-ND

formales estipulados, que el Estado debe garantizar en su función protectora de la seguridad del individuo salvo que, excepcionalmente, sea su propia existencia la que corra riesgo por algún tipo de amenaza interna o, incluso, externa, caso en el que primará sobre todo lo demás el superior interés de lo público.

Respecto a la seguridad ciudadana, desde el reconocimiento a la labor de la Policía y en el convencimiento de su necesidad, se decide cambiar su organización y dependencia para asimilarlas al resto de la Administración Civil del Estado. Para ello, por Real Decreto de 4 de octubre de 1835, se suprime la dirección de la *Superintendencia General de la Policía* como cabeza de la institución, no así la Policía, que sigue acometiendo sus funciones "en el mismo ámbito urbano, con las mismas competencias y procedimientos, y en el mismo marco territorial y estructural que en 1824, llegando a resultados que con asiduidad tenían eco en la prensa periódica" (HERRERO FERNÁNDEZ-QUESADA & TURRADO VIDAL, 2023, pág. 74). El resto de las dependencias policiales del reino, al haberse suprimido el *Superintendente*, pasan a depender directamente del Ministerio de la Gobernación y de los Gobernadores Civiles de las provincias. El 18 de agosto de 1836 -unos días después del triunfo del motín de los sargentos de La Granja- se le cambia también el nombre, primero en Madrid, pasándose a llamar *Protección y Seguridad Pública*, para después continuar gradualmente en todas las provincias. El primer documento oficial que se refiere a la Policía con ese nombre de *Protección y Seguridad Pública* es la circular del Ministerio de la Gobernación de 18 de diciembre de 1836, que señala como su principal y único objeto la protección de los ciudadanos y la conservación de la tranquilidad pública, recortándole importantes competencias como policía administrativa para la gestión de cartas de seguridad y pasaportes, entre otras (TURRADO VIDAL M. , 2023, págs. 42-47).

En 1845, en la denominada *década moderada* tras la Guerra Carlista, se firma una Constitución que trata de encontrar el justo medio entre revolucionarios y conservadores. Fruto de este entente cordial se redacta una norma que, aunque inicialmente solo pretende perfeccionar el texto antecesor del que acepta con alguna matización su declaración de derechos[596], acaba definiendo un nuevo modelo de Estado sustentado sobre la Corona, que comparte su soberanía con las Cortes, en un tiempo histórico de reformas tributarias, educativas y administrativas que son la constatación del esfuerzo del liberalismo burgués por cerrar definitivamente el ciclo conservadurista con olor a Antiguo Régimen, y donde la estructura de la Policía está igualmente sujeta a continuas modificaciones, siendo que en 1852 se vuelve a cambiar el nombre al ramo de *Protección y Seguridad Pública* por el de *Cuerpo de Vigilancia*, con la figura del *celador de barrio*[597], que venía prestando sus funciones de protección y seguridad a la

[596] El artículo 2 de la Constitución de 1845 mantiene la numeración de su predecesora al estipular que "Todos los españoles pueden imprimir y publicar libremente sus ideas sin previa censura, con sujeción a las leyes", pero acaba con la jurisdicción de los Jurados para la calificación de estos delitos de imprenta. Los artículos 7, 8 y 9, referidos a la detención y a su excepción por razón de la seguridad del Estado, y a la garantía jurisdiccional, permanecen sin embargo idénticos en su redacción.

[597] La labor de investigación histórica de Julio de Antón nos permite saber que el celador de barrio identificaba su domicilio con un letrero, iluminado por la noche con un farol, donde se leía en grandes caracteres *celaduría de protección y seguridad*. "Este funcionario percibía cuatro mil reales de vellón al año (…). Vestía de uniforme frac azul, simbolizando su autoridad y profesionalidad mediante un bastón de borlas con puño de marfil; y si ascendía a Comisario, sustituiría aquel bastón por otro con puño de oro

Ediciones Universidad de Salamanca | CC BY-NC-ND

ciudadanía desde 1824, como verdadero antecedente de la labor civil de la Policía española. El Reglamento del *Cuerpo de Vigilancia* se promulga el 9 de marzo de 1852 y se publica en la Gaceta de Madrid el día 14 de ese mismo mes. Como viene sucediendo desde 1835, esta estructura policial depende del Ministerio de la Gobernación y de los Gobernadores Civiles. Para centralizar y poder mejor aprovechar toda la información proveniente de la Policía se establece en el Ministerio un negociado llamado de *Policía* y, poco tiempo después, *Secciones de Orden Público*[598]. Seis años más tarde se reglamenta el nuevo *Cuerpo de Vigilancia Pública,* que dota a cada distrito de Madrid con un Inspector Jefe en representación del Gobernador. Para el mantenimiento del orden público se apuesta por el Ejército y la Guardia Civil en detrimento de la Policía, a consecuencia de la prevalencia de los intereses militares que, incluso, llevan a la pérdida de poder de los Gobernadores Civiles en las provincias en favor de los Gobernadores Militares (DE ANTÓN LÓPEZ, 2000, pág. 61).

La Constitución de 1869 representa la llave para la entrada de la democracia en España a través del sufragio universal masculino cuya literalidad luce orgullosa en su corto Preámbulo[599], compartiendo protagonismo con la primera mención expresa a la seguridad, preciadas conquistas del liberalismo democrático que avalan una amplia declaración de derechos fundamentales inspirada en textos como la Carta Magna norteamericana o la belga de 1831 y que, también por primera vez, fija la responsabilidad de la autoridad pública que conculque tales garantías[600] y, lo que es más novedoso, no amparando la obediencia debida como eximente de responsabilidad para los funcionarios públicos que infrinjan la norma constitucional[601]. Es así como los derechos del ciudadano, que de nuevo vuelve a ser el único soberano, se reivindican frente al poder del Estado que, consecuentemente, adquiere un perfil mucho más de utilidad pública y de protección hacia el pueblo, a cuyo servicio dispone una Policía que para salvaguardar el orden público y, con ello, el orden político del Estado, debe actuar

y portaría una faja en la cintura con los colores amarillo y encarnado. El celador contaba con el auxilio de cinco agentes, que era la dotación para cada barrio de Madrid". En *Historia de la Policía Española*, página 61.

[598] En entrevista personal con Martín Turrado Vidal el 09/03/2024 nos amplía esta información indicando que las oficinas de los celadores y las comisarías tenían un horario de apertura al público. El farolillo rojo indicaba que los ciudadanos podían dirigirse a ellas en caso de emergencia, lo cual indica que estaban abiertas de forma permanente al público, siendo las primeras en hacerlo dentro de la administración. El celador gozó de muy buena reputación entre los ciudadanos y la prensa, hasta el punto de que en un artículo publicado en La Revista Española, el 27 de febrero de 1835, se pedía para ellos un aumento de sueldo. Unos años después, en 1844, salió muy bien parado en el libro titulado "Los Españoles pintados por sí mismos".

[599] "La nación española y en su nombre las Cortes Constituyentes elegidas por sufragio universal, deseando afianzar la justicia, la libertad y la seguridad, y proveer al bien de cuantos vivan en España, decretan y sancionan la siguiente Constitución".

[600] El artículo 9 de la Constitución de 1869 establece que "La autoridad gubernativa que infrinja lo prescrito en los artículos segundo (garantías de la detención), tercero (límites temporales de la detención), cuarto (garantías para ingreso en prisión), y quinto (inviolabilidad del domicilio y las comunicaciones) incurrirá, según los casos, en delito de detención arbitraria ó de allanamiento de morada, y quedará además sujeta á la indemnización prescrita en el párrafo segundo del artículo anterior".

[601] El artículo 30 determina que "No será necesaria la previa autorización para procesar ante los tribunales ordinarios a los funcionarios públicos, cualquiera que sea el delito que cometieren. El mandato del superior no eximirá de responsabilidad en los casos de infracción manifiesta, clara y terminante de una prescripción constitucional. En los demás, solo eximirá a los agentes que no ejerzan autoridad".

Ediciones Universidad de Salamanca | CC BY-NC-ND

al amparo de las leyes. Se produce un nuevo cambio de denominación a *Cuerpo de Orden Público*, que se despliega primeramente en Madrid y en 1870 en el resto del país, siendo su carácter militar -principalmente en la capital- hasta 1872, cuando por obra de Manuel Ruiz Zorrilla pasa a ser civil. En 1873, en la I República, se intenta desdoblar esta estructura policial en dos -*Cuerpo de Vigilancia* y *Cuerpo de Seguridad*-, pero la falta de medios impidió que fraguase la propuesta, por lo que continuó con su denominación de *Cuerpo de Orden Público* hasta 1886[602].

La Restauración española abre una etapa política de estabilidad que posibilita la redacción de la Constitución de 1876, conocida por reintegrar la soberanía a la diarquía del Rey y las Cortes y posibilitar la alternancia pactada en el poder de conservadores y liberales. Se consolidan derechos fundamentales como los referidos a la detención, al ingreso en prisión, a la inviolabilidad del domicilio y las comunicaciones, al disfrute de la propiedad privada, a la libertad de credo y a la libertad de opinión, reunión y asociación, entre otros. A su vez, la autoridad del Rey es ejecutada por las estructuras de gobierno con el fin de preservar el orden público y la seguridad de la nación[603], lo que confirma la interpretación de la seguridad desde la perspectiva del Estado, ya sea para garantizar la paz pública frente a los delitos en el ámbito interior como para preservar la integridad territorial frente a las amenazas exteriores.

En Madrid en 1877, retomando el proyecto de la I República, se da forma a la Policía con un cuerpo uniformado y de carácter militar, el *Cuerpo de Seguridad*, con funciones preventivas y de orden público, y otro de naturaleza civil orientado a tareas de investigación y control de la delincuencia, el *Cuerpo de Vigilancia*, extendiéndose este último al resto del territorio en 1886, que hasta entonces mantuvo al *Cuerpo de Orden Público*.

La aparición del movimiento de la clase obrera y del anarquismo hace del terrorismo un mal endémico en la década de 1890, acompañado también por violencia de carácter rural, especialmente en Andalucía, situación que hace que se deba replantear la estructura policial española. En este sentido, en 1896 se crea en Madrid y Barcelona el *Cuerpo de Policía Judicial*, que en 1906 se integra en el *Cuerpo de Vigilancia*[604]. En este periodo la autonomía policial es muy escasa a resultas de la alternancia en el poder político que genera continuos cambios en su estructura, reducida de por sí y concentrada en las dos grandes urbes -Madrid y Barcelona- con funciones prioritarias de orden público, como la supervisión de la reglamentación de espectáculos y establecimientos, la higiene, la hospedería y otros de consideración municipal (DE ANTÓN LÓPEZ, 2000, págs. 28-29). Así lo atestigua la Ley de 27 de febrero de 1908, de organización de la Policía Gubernativa, que se constituye por el *Cuerpo de Vigilancia* y el *Cuerpo de Seguridad*, a las órdenes del Gobernador Civil en cada provincia[605]. No

[602] Aportaciones de Martín Turrado Vidal en entrevista personal, el 09/03/2024.

[603] El artículo 50 señala que "La potestad de hacer ejecutar las leyes reside en el Rey, y su autoridad se extiende á todo cuanto conduce á la conservación del orden público en lo interior y á la seguridad del Estado en lo exterior, conforme á la Constitución y á las leyes".

[604] Aportaciones de Martín Turrado Vidal en entrevista personal, el 09/03/2024.

[605] Así lo establece el artículo 1 de la Ley de Policía Gubernativa, de 27 de febrero de 1908, que en su artículo 2 precisa la composición de ambos Cuerpos, indicando que el de Vigilancia lo constituirán un Comisario General y un Secretario en Madrid, un Inspector General y un Secretario en Barcelona, jefes de

Ediciones Universidad de Salamanca | CC BY-NC-ND

obstante, el afán de mejora y profesionalización de la Policía es patente y, así, esta norma dedica ocho de sus quince artículos a regular los procesos de convocatoria, ingreso, promoción, provisión de vacantes y composición de tribunales para acceder a ambos Cuerpos, un artículo a la Escuela de Policía y su profesorado, y otro al régimen disciplinario, en lo que se puede interpretar como un serio esfuerzo por vehicular la formación policial sobre un cuerpo de conocimiento técnico profesional y por unificar los requisitos de acceso a través de unas capacidades y aptitudes previas que deben demostrar los aspirantes, todo lo cual habrá de redundar en la calidad y la eficacia del servicio prestado a los ciudadanos.

La etapa de paz vivida en el periodo liberal anterior finaliza con el golpe de estado de Primo de Rivera en 1923 que, curiosamente, "es uno de los momentos más creativos de la Policía, dando la sensación como si hubiera prisa en establecer estructuras policiales para cubrir objetivos, siendo motivo prioritario el Orden Público, acabar con los atentados, secuestros y robos; así como la expendición de drogas, que se inicia, tomando consideración policial" (DE ANTÓN LÓPEZ, 2000, pág. 234). Para operativizar esta estrategia devuelve el nombre a la *Dirección General de Seguridad*[606] de la que depende, entre otras, la *Sección de Orden Público* con la función de recoger e investigar cualquier tipo de dato referido a personas, noticias o hechos, que pudiese afectar al orden social a través de la convocatoria de huelgas, la prostitución y la trata de mujeres o cuestiones similares. En la intención de seguir evolucionando las competencias y capacidades técnico profesionales de la Policía se establecen en este momento dos estructuras principales, por un lado, la *Oficina Central Nacional* necesaria para, a través de la red colaborativa de la *Comisión Internacional de Policía Criminal*[607], dar respuesta a las gestiones de información demandadas por los demás miembros y, por otro, el *Gabinete Central de Identificación*, pieza clave para la investigación policial y el aseguramiento de los identificados como autores de delitos. La Dictadura de Primo de Rivera deja un Reglamento orgánico y de servicios que perdura hasta 1975, el denominado *Reglamento de Mola* de 1930, que se convierte así en una de las disposiciones legales que más tiempo han estado en vigor en la Policía[608].

Las elecciones de 12 de abril de 1931 dan la victoria a una coalición de republicanos y socialistas y, con la proclamación de la II República, se firma el destierro de D. Alfonso XIII de Borbón. En junio se constituyen Cortes y se aprueba la nueva Constitución,

los servicios de Vigilancia y Seguridad, con autoridad propia en el ejercicio de sus funciones. El resto de personal de dichas plantillas lo componen Comisarios, Inspectores, Agentes, Aspirantes, Vigilantes, Escribientes y Ordenanzas.

[606] La Dictadura no crea la Dirección General de Seguridad, sino que le devuelve su primer nombre que había sido cambiado arbitrariamente en 1921 por el de Dirección General de Orden Público. Aportación de Martín Turrado Vidal en entrevista personal el 09/03/2024.

[607] En septiembre de 1923 se crea la Comisión Internacional de Policía Criminal (CIPC) por veinte países que ven la necesidad de facilitar la cooperación policial entre ellos para dar respuesta a la criminalidad de la época, instaurando el modelo de la Oficina Central Nacional para disponer en cada país de un único interlocutor que, a nivel nacional, organice esta tarea de coordinación, dentro de la variedad de modelos legislativos y policiales existentes en cada uno de ellos. España se une en 1929 y, en 1956, se aprueba un Estatuto modernizado de la CIPC que pasa a denominarse Organización Internacional de Policía Criminal (OIPC-INTERPOL). La Organización dispone de su propia página web donde se pueden consultar desde datos históricos hasta su actual estructura. Disponible en: https://www.interpol.int/es (10/05/2023).

[608] Aportaciones de Martín Turrado Vidal en entrevista personal, el 09/03/2024.

Ediciones Universidad de Salamanca | CC BY-NC-ND

claramente influenciada por el constitucionalismo europeo de la época representado por la Carta Magna alemana de Weimar y la austriaca, cuyos máximos exponentes programáticos son la democracia, el regionalismo, el laicismo y la economía social, que sustentan un modelo de Estado interventor y garante del supremo interés social, que se reserva en exclusiva para sí la defensa nacional y la seguridad pública, así como el control de fronteras, inmigración, emigración y extranjería[609]. También la seguridad del Estado, en casos de notoria e inminente gravedad, habilitan para la suspensión de las garantías de derechos fundamentales como los referidos a la detención, la libre circulación, expulsión de extranjeros e inviolabilidad del domicilio, la libertad de opinión y prensa, el derecho de reunión y el de asociación o sindicación[610]. Finalmente, se reserva al Presidente de la República la prerrogativa de declarar la guerra y firmar la paz, así como la de ordenar aquellas medidas urgentes que exija la defensa de la integridad o la seguridad de la nación[611].

De nuevo la estructura policial debe adaptarse a la realidad del momento, que pasa por ser rebelde y alborotadora, transformándose por esta razón una parte de ella en la *Guardia de Asalto*, contando a su vez con el respaldo de las Leyes de Orden Público y de Vagos y Maleantes, ambas de 1933[612], que en conjunto pretenden atajar los acuciantes problemas sociales existentes[613] y que obligan a la Policía a "emitir una serie de instrucciones rigurosas para mantener el orden público, muy especialmente en referencia al uso de banderas, realización de frecuentes cacheos, y restringir aquella propaganda realizada por medio de aviones, ordenando la detención de los pilotos" (DE ANTÓN LÓPEZ, 2000, pág. 94). Otras modificaciones estructurales de la *Dirección General de Seguridad* que se acometen en la II República son la creación de la *Oficina de Información y Enlace*, directamente dependiente del Director General, encargada de la

[609] El artículo 14 establece que "Son de la exclusiva competencia del Estado español la legislación y la ejecución directa en las materias siguientes: 4. Defensa de la seguridad pública en los conflictos de carácter suprarregional o extrarregional; 7. Ejército, Marina de guerra y Defensa nacional; 16. Policía de fronteras, inmigración, emigración y extranjería".

[610] El artículo 42 regula la suspensión de garantías constitucionales señalando que "Los derechos y garantías consignados en los artículos 29 -detención-, 31 -libre circulación-, 34 -libertad de opinión y prensa-, 38 -derecho de reunión- y 39 -derecho de asociación y sindicación- podrán ser suspendidos total o parcialmente, en todo el territorio nacional o en parte de él, por decreto del Gobierno, cuando así lo exija la seguridad del Estado, en casos de notoria e inminente gravedad".

[611] El artículo 76 recoge que "Corresponde también al Presidente de la República: a) Declarar la guerra, conforme a los requisitos del artículo siguiente, y firmar la paz; d) Ordenar las medidas urgentes que exija la defensa de la integridad o la seguridad de la Nación, dando inmediata cuenta a las Cortes".

[612] Estas son la Ley de Orden Público, de 28 de julio de 1933, y la Ley de Vagos y Maleantes, de 4 de agosto del mismo año, popularmente conocida como *la Gandula*.

[613] La creación de las Secciones de Vanguardia y Asalto del Cuerpo de Seguridad -denominación oficial de estas estructuras- responde a dos necesidades perentorias que se fueron acentuando con el paso del tiempo. La primera se refiere a que en casi todas las manifestaciones de la época, por irrelevante que fuera el motivo de su convocatoria e independientemente del número de asistentes, terminaban con ciudadanos muertos o heridos debido a la falta de material policial adecuado para hacerles frente, así como por la falta de preparación de los militares y guardias civiles que debían disolverlas. La segunda razón es que la frecuencia de estas manifestaciones en las ciudades obligaban a concentrar en ellas los efectivos de la Guardia Civil, dejando por tanto desprotegido el ámbito rural. Por ello, vista la experiencia exitosa de las llamadas *Brigadas del Tigre* en Francia, se copió el modelo y se crearon dentro del *Cuerpo de Seguridad* las *Secciones de Vanguardia y Asalto*. Aportaciones de Martín Turrado Vidal en entrevista personal, el 09/03/2024.

Ediciones Universidad de Salamanca | CC BY-NC-ND

gestión y control de datos de interés policial, y el definitivo impulso de la *Inspección General del Gabinete de Identificación*, cuya calidad y metodología de trabajo supuso la posibilidad de esclarecer delitos en todo el territorio nacional que, de otra forma, hubiera sido imposible llevar a buen término (TURRADO VIDAL M. , 2020, págs. 44-49).

4.1.2. La dictadura franquista

Este ambiente de inestabilidad nacional desemboca en la sublevación del Ejército contra el gobierno electo republicano y la proclamación del Alzamiento Nacional el 18 de julio de 1936, cuyo ideario busca imponer un nuevo orden social liderado en solitario por el General Franco como Jefe del Estado, que lleva a España a desangrarse en una guerra fratricida durante casi tres años fruto de la cual se establece una dictadura que permanece hasta la muerte de aquel, el 20 de noviembre de 1975. En este periodo es a través de las Leyes Fundamentales[614] como se define el marco jurídico institucional del país, que articula la forma del Estado como "Monarquía tradicional, católica, social y representativa"[615] en el que "la unidad, grandeza y libertad de la Patria es deber sagrado y tarea colectiva de todos los españoles"[616]. En coherencia con esta forma de ejercer el poder, las autodenominadas *Cortes franquistas,* en un contexto en el que no existe separación de poderes, carecen de la propia libertad de acción frente al Gobierno[617] y los inexistentes derechos fundamentales de los ciudadanos, son limitados *de facto* por el arbitrio del poder del Estado[618], que abarca toda la esfera de protección y subyuga al interés propio el resto de intereses individuales o colectivos, sin excepción[619].

Consecuencia de ello, la estructura policial se centraliza y adquiere una marcada *vis* política y represiva, acorde con un sistema autárquico que prioriza la defensa de la seguridad del Estado y del Régimen en que se sustenta. Así, la Ley de 8 de agosto de 1939 crea el Ministerio de la Gobernación del que pasa a depender la *Dirección General*

[614] Las Leyes Fundamentales incluían el Fuero del Trabajo (9/3/1938); la Ley Constitutiva de las Cortes Españolas (17/7/1945); el Fuero de los Españoles (1777/1945); la Ley de Referéndum (22/10/1946); la Ley de Sucesión a la Jefatura del Estado (26/7/1947); la Ley de Principios del Movimiento Nacional (17/5/1958) y la Ley Orgánica del Estado (10/1/1967). El Decreto 779/1967, de 20 de abril, por el que se aprueban los textos refundidos de las Leyes Fundamentales del Reino, trata de ordenar sistemáticamente este complejo entramado de normas que, a nuestro juicio, pretenden dar una falsa apariencia constitucional a la dictadura franquista.

[615] Ley de Principios del Movimiento Nacional, de 17 de mayo de 1958, apartado VII.

[616] IBIDEM, Apartado I.

[617] Ley Constitutiva de las Cortes, de 17 de julio de 1942 (modificada por la Ley Orgánica del Estado, de 10 de enero de 1967), artículo octavo: "Las Cortes funcionarán en Pleno y por Comisiones. Las Comisiones las fija y nombra el Presidente de las Cortes, a propuesta de la Comisión Permanente y de acuerdo con el Gobierno. El Presidente fija, de acuerdo con el Gobierno, el orden del día, tanto del Pleno como de las Comisiones".

[618] Fuero de los Españoles, de 17 de julio de 1945 (modificado por la Ley Orgánica del Estado, de 10 de enero de 1967), artículo treinta y tres: "El ejercicio de los derechos que se reconocen en este Fuero no podrá atentar a la unidad espiritual, nacional y social de España".

[619] Sirva como ejemplo lo que recoge el Fuero de los Españoles, de 17 de julio de 1945 (modificado por la Ley Orgánica del Estado, de 10 de enero de 1967), en su artículo doce: "Todo español podrá expresar libremente sus ideas mientras no atenten a los principios fundamentales del Estado".

Ediciones Universidad de Salamanca | CC BY-NC-ND

de Seguridad[620] y, posteriormente, es la Ley de 8 de marzo de 1941[621] la que, achacando al anterior modelo policial "un apoliticismo propio de sistemas que presenciaban impasibles su proceso de descomposición", reorganiza los servicios de Policía con el *Cuerpo General de Policía*[622] y el *Cuerpo de Policía Armada y de Tráfico*[623], con naturalezas, misiones y cometidos claramente diferenciados aunque complementarios, "para llevar a cabo la vigilancia permanente y total indispensable para la vida de la Nación, que en los Estados totalitarios se logra merced a una acertada combinación de técnica perfecta y de lealtad que permita la clasificación adecuada en sus actividades y dé vida a la Policía política, como órgano más eficiente para la defensa del Estado"[624].

Los procesos de ascenso y promoción en ambos Cuerpos exigían la tramitación de un expediente en el que se valoraba al candidato conforme a "su conducta pública o privada o por los antecedentes sociales, políticos o profesionales que así lo aconsejen" (TURRADO VIDAL M. , 2021, págs. 44-49). Es este un modelo policial sustancialmente orientado al mantenimiento del orden público, que parametriza a los ciudadanos por su adhesión al *Movimiento Nacional* o la afección a la estructura de gobierno en un complicado contexto social, primeramente, de enfrentamientos, escaramuzas y hostigamiento al Régimen por parte del *maqui* cuyo número "hacia 1949 oscila entre los 3.000 y los 15.000, generando así un efecto de ejércitos de guerrilleros que operan con gran movilidad" (DE ANTÓN LÓPEZ, 2000, pág. 407) y, más tarde, de malestar ciudadano derivado de la carestía de vida y canalizado a través de revueltas obreras concentradas en las industrias del acero, minas, astilleros y transportes que generan la consecuente respuesta policial. De esta necesidad de control parece derivar el Decreto de 2 de marzo

[620] La Ley de 8 de agosto de 1939, modificando la organización de la administración central del Estado, publicada en el BOE núm. 221 de 9 de agosto de 1939, páginas 4326 y 4327, en el artículo segundo instaura el Ministerio de la Gobernación, y en el artículo octavo establece que los hasta entonces Servicios Nacionales de la Administración Central pasen a denominarse Direcciones Generales, siendo así que se crea la Dirección General de Seguridad. Posteriormente, en la Ley de 23 de septiembre de 1939 se reorganiza dicha Dirección General, cuyo artículo segundo consigna las cuatro Comisarías Generales que la componen -la de Fronteras, la de Información, la de Orden Público y la de Identificación- y que son el origen de la actual estructura de los Servicios Centrales de la Policía Nacional.

[621] Ley de 8 de marzo de 1941 por la que se reorganizan los servicios de Policía, publicada en el Boletín Oficial del Estado de 8 de abril de 1941, núm. 98, página 2340 y ss.

[622] El Decreto de 31 de diciembre de 1941, por el que se dispone la ejecución de la Ley reorganizadora de la Policía, de 8 de marzo de 1941, señala en el artículo tercero los cometidos del Cuerpo General de Policía, de naturaleza civil, siendo el primero de ellos "Ejecutar y hacer cumplir las órdenes que se dicten por las Autoridades Gubernativas y las obligaciones sociales impuestas por las Leyes y Reglamentos en vigor, prevenir las infracciones de todas clases indagando cuantas actividades resulten contrarias a la seguridad de la Nación y del Régimen y evitar la alteraciones del orden público y político-social, adoptando las medidas previstas en las disposiciones al efecto dictadas por las Autoridades del Ministerio de la Gobernación". El segundo de sus cometidos es "Cumplir los deberes que a la Policía judicial imponen las normas procesales en vigor y prevenir, perseguir y descubrir los delitos y faltas definidos en las vigentes Leyes penales; detener a los culpables cuando proceda, incautarse del cuerpo, útiles y efectos de la infracción punible, recoger las pruebas de la misma y redactar los atestados para su curso a las Autoridades, Juzgados y Organismos competentes".

[623] En cuanto al Cuerpo de Policía Armada y de Tráfico, es el artículo decimoquinto del Decreto de desarrollo de 31 de diciembre de 1941 el que señala que su misión es la de "vigilancia total y permanente, así como de represión cuando fuere necesario". Este Cuerpo policial tiene, conforme al artículo decimoséptimo, "carácter y organización eminentemente militar".

[624] Preámbulo de la Ley de 8 de marzo de 1941, por la que se reorganizan los servicios de Policía.

Ediciones Universidad de Salamanca | CC BY-NC-ND

de 1944[625], en el que se crea el *Documento Nacional de Identidad* "por necesidad de largo tiempo sentida" al objeto de alcanzar la "eficiencia plena en la acreditación indubitada de la personalidad individual"[626], siendo obligatorio para los mayores de dieciséis años residentes en España[627] y de expedición prioritaria para reclusos con condiciones atenuadas o en libertad vigilada[628], responsabilizándose de la expedición y distribución del documento a la *Dirección General de Seguridad*[629].

El año 1968 supone un punto de inflexión en la seguridad interior del país, por cuanto la banda terrorista Euskadi Ta Askatasuna (ETA)[630] comete su primer asesinato en la persona del Cabo de la Guardia Civil José Antonio Pardines, que tuvo lugar en Guipúzcoa el 7 de junio de 1968 y, apenas dos meses después, el 2 de agosto, asesina en Irún al Inspector Jefe de Policía Melitón Manzanas. Comenzando el nuevo año, el 24 de enero de 1969, por primera vez desde el final de la Guerra Civil se decreta el Estado de Excepción en todo el país por tres meses, motivado por las sucesivas alteraciones del orden público en forma de manifestaciones universitarias, huelgas y protestas obreras, actos terroristas y sabotajes, que no hacen sino aumentar la tensión social ya existente. El 20 de diciembre de 1972 el terrorismo de ETA acaba con la vida del Presidente del Gobierno Carrero Blanco, sustituyéndole en el cargo Arias Navarro en un vano intento del Régimen por proyectar una imagen de aperturismo y acercamiento a la oposición moderada. Finalmente, el 22 de noviembre de 1975 es proclamado Rey de España Juan Carlos I de Borbón, dos días después de la muerte de Francisco Franco y de acuerdo con la Ley de Sucesión a la Jefatura del Estado de 1947, que devino en su proclamación como Príncipe de España en julio de 1969. En julio de 1976 cesa Arias Navarro y es Adolfo Suárez quien, bajo la inspiración programática del nuevo Jefe del Estado, asume la Presidencia del Gobierno para coordinar al conjunto de las fuerzas políticas hacia el objetivo común de pactar una Constitución que, al entender de todos, signifique la ruptura y el cierre del periodo anterior, pasando de un régimen autoritario a otro democrático y de uno centralista a otro autonómico.

4.1.3. La democracia española de 1978

[625] Decreto de 2 de marzo de 1944 por la que se crea el Documento Nacional de Identidad, publicado en el Boletín Oficial del Estado de 21 de marzo de 1944, núm. 81, página 2346 y ss.

[626] El preámbulo del Decreto de 2 de marzo de 1944 señala esta necesidad y, en su artículo segundo, establece que "El Documento Nacional de Identidad se hará con las mayores garantías conducentes a impedir su falsificación y contendrá los requisitos y particularidades que se determinen. Su duración será de cinco años a partir de la fecha de expedición".

[627] Por su parte, el artículo tercero señala que "Los mayores de dieciséis años residentes en España tendrán la obligación de adquirir dicho Documento, que en lo sucesivo constituirá el justificante de la personalidad individual de ellos, exigiéndose rigurosamente a tal fin. Los carnets o tarjetas tanto de Organismos oficiales como de Empresas o Entidades privadas podrán servir para acreditar el empleo y condiciones del titular en el cargo oficio o profesión a que se refieran, pero en modo alguno sustituirán al Documento de Identidad ni excusarán de adquirir éste".

[628] Artículo sexto, que define la prelación en la expedición del Documento, siendo los primeros "Los que estén o queden en prisión atenuada o libertad vigilada".

[629] El artículo primero dispone que "Se crea el Documento Nacional de Identidad. Corresponderá privativamente al Ministerio de la Gobernación, a través de la Dirección General de Seguridad, organizar, dirigir y administrar este nuevo servicio".

[630] Euskadi Ta Askatasuna se traduce al español como País Vasco y Libertad.

Ediciones Universidad de Salamanca | CC BY-NC-ND

El inicio de este proceso constituyente debemos fijarlo en la labor intelectual de quien fuera tutor del Rey, el profesor Torcuato Fernández-Miranda y Hevia, junto con la amplia aprobación por referéndum de la Ley para la Reforma Política, de enero de 1977, cuyo nombre bien expresa su intencionalidad, la cual queda patente en la consagración que su primer artículo hace del *imperio de la ley* y de la *inviolabilidad de los derechos fundamentales de la persona*[631]. Formadas las nuevas Cortes bicamerales se elige la Comisión Constituyente que, a propuesta de la Ponencia encargada de la redacción del texto, presenta el proyecto final para su discusión por el Pleno del Congreso y del Senado, siendo definitivamente aprobado por éstas y por abrumadora mayoría en el referéndum celebrado el 6 de diciembre de 1978. También son muy relevantes para el buen fin de este proceso los Pactos de la Moncloa, firmados en octubre de 1977, que incluyen un acuerdo de medidas para tratar de paliar la crisis económica del momento -caracterizada por una severa recesión junto con una elevada inflación- y otro de carácter jurídico-político para abrir vías de encuentro entre las distintas sensibilidades políticas, actuando sobre elementos cruciales como la libertad de expresión, el derecho de reunión y el de asociación, entre otros.

La perspectiva histórica confirma que la Policía ha sido un factor más de estabilidad y, con ello, de impulso al exitoso proceso de la transición española. En 1976 tanto el *Cuerpo General de Policía* como la *Policía Armada* tienen una media de edad muy joven[632] con un elevado volumen de funcionarios que han ingresado durante la etapa final del franquismo (TURRADO VIDAL M. , 2021, págs. 40-45) y que, por ello, llevan poco tiempo en el Cuerpo, lo que les concede una mejor predisposición ante los cambios de estructura necesarios para acompasar a la Policía con la nueva realidad social y política del país. Los Pactos de la Moncloa, con el programa de actuación jurídica y política, dan una nueva definición al concepto de orden público depurándolo de contenidos no democráticos y orientándolo hacia el respeto de las libertades públicas y los derechos humanos[633], a la vez que inician la reorganización de los Cuerpos y Fuerzas de Orden Público en dos sectores, uno civil, integrado en exclusiva por el *Cuerpo General de Policía* que se encarga de la investigación criminal, y otro militar, constituido por la *Policía Armada* y la *Guardia Civil* como cuerpos operativos para el mantenimiento de la paz y la seguridad ciudadana[634]. A la vez que se anuncia una distribución funcional y territorial de competencias entre la *Policía Gubernativa* -*Cuerpo General* y *Policía Armada*- y la

[631] Ley 1/1977, de 4 de enero, para la Reforma Política, publicada en el BOE núm. 4, de 5 de enero de 1977, páginas 170 a 171. Su artículo 1 dice: "Uno. La democracia, en el Estado español se basa en la supremacía de la Ley, expresión de la voluntad soberana del pueblo. Los derechos fundamentales de la persona son inviolables y vinculan a todos los órganos del Estado.
Dos. La potestad de elaborar y aprobar las leyes reside en las Cortes. El Rey sanciona y promulga las leyes"

[632] Como explica Turrado Vidal, en 1976 la edad máxima fijada para ingresar en el Cuerpo General de Policía es de 28 años, que entonces está compuesto por alrededor de 9000 agentes, 4500 de los cuales han ingresado en el periodo de cinco años comprendido entre 1969 y 1974, lo que determina la baja media de edad y de permanencia en el Cuerpo.

[633] El apartado VIII del Acuerdo sobre el programa de actuación jurídica y política, aprobado el 27 de octubre de 1977, dedicado al Orden Público, señala en su punto 2: "El orden público tendrá una proyección concreta y actual en cuanto protección del avance en la consolidación de la democracia y defensa frente a las agresiones de todo orden y especialmente las terroristas".

[634] Punto 2 del apartado IX del Acuerdo sobre el programa de actuación jurídica y política, dedicado a la Reorganización de los Cuerpos y Fuerzas de Orden Público.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Guardia Civil[635], se pretende avanzar en su coordinación[636], en la formación y especialización de sus integrantes para el adecuado desempeño de sus funciones y una mayor cercanía a los ciudadanos[637], en la distinción de funciones de los Cuerpos estatales y las policías locales[638] y, finalmente, en la reforma del Reglamento Orgánico de la Policía conforme a estos principios programáticos enunciados[639].

El proceso de unificación del *Cuerpo General de Policía* y de la *Policía Armada* se inicia poco antes con el Real Decreto 1316/1977, de 2 de junio, sobre demarcación territorial y funcional de las Fuerzas de Orden Público, que en su artículo 6 ya señala que los servicios de ambos Cuerpos se ordenarán por los *Jefes Superiores de Policía* y los *Comisarios Provinciales y Locales* de aquellos dependientes[640], incidiendo en que la *Policía Armada* actuará siempre de uniforme salvo para casos excepcionales por necesidades del servicio[641], y el doble carácter de Policía Gubernativa y Judicial del *Cuerpo General de Policía* que ejerce junto con las competencias propias de Policía Administrativa[642].

La Ley 55/1978, de 4 de diciembre, de la Policía se mantiene en vigor apenas 7 años pero, a pesar de ello, deviene en llave de paso necesaria para abrir el cauce de las modificaciones que han de sustentar el modelo actual, por cuanto encarga a los Cuerpos de Seguridad del Estado, dependientes del Ministro del Interior, la misión de "defender el ordenamiento constitucional, proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana"[643], a través de una estructura que, bajo el mando directo del Director de la Seguridad del Estado, distingue dos Direcciones Generales: la de la Policía, en la que se integran el *Cuerpo Superior de Policía* de naturaleza civil, y el *Cuerpo de la Policía Nacional* de naturaleza militar, y la de la *Guardia Civil*[644]. Aprovecha

[635] IBIDEM, Punto 3.
[636] IBIDEM, Punto 4.
[637] IBIDEM, Puntos 6, 7 y 8.
[638] IBIDEM, Punto 9.
[639] IBIDEM, Punto 10.
[640] El Real Decreto 1316/1977, de 2 de junio, sobre demarcación territorial y funcional de las Fuerzas de Orden Público, en el artículo 6 señala que: "Los Jefes superiores de Policía, Delegados especiales de la Dirección General de Seguridad y los Comisarios provinciales y locales, con la competencia y subordinación que les atribuye la legislación vigente, ordenarán los servicios de los Cuerpos Generales de Policía, Especial Administrativo y Auxiliar de Oficinas directamente, y a través de sus Jefes naturales, los del Cuerpo de la Policía Armada". BOE núm. 141, de 14 de junio de 1977. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1977-13819 (24/04/2024).
[641] IBIDEM, Artículo 8: "La Policía Armada actuará siempre de uniforme. El Director general de Seguridad podrá autorizar, directamente o por delegación, con carácter excepcional y por necesidades del servicio, que el personal de la Policía Armada desempeñe sin vestir uniforme reglamentario misiones propias del Cuerpo. Quienes realicen tales cometidos conservarán el carácter de Agentes de la Autoridad y deberán acreditar su identidad profesional, si fuere necesario".
[642] IBIDEM, Artículo 5: "El Cuerpo General de Policía realizará las funciones técnicas que lo competen en su doble carácter de Policía Gubernativa y Judicial, así como las actividades de directivas de Policía Administrativa que le están legalmente atribuidas".
[643] Artículo 2.1 de la Ley 55/1978, de 4 de diciembre, de la Policía: "Los Cuerpos de Seguridad del Estado tendrán como misión defender el ordenamiento constitucional, proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana".
[644] IBIDEM, Artículo 1: "Los Cuerpos de Seguridad del Estado están integrados por:
Uno. La Policía, integrada por: a) El Cuerpo Superior de Policía. b) El Cuerpo de la Policía Nacional.
Dos. La Guardia Civil".

Ediciones Universidad de Salamanca | CC BY-NC-ND

la norma para hacer una distribución territorial y funcional de competencias entre los Cuerpos de Seguridad del Estado y les obliga a la cooperación recíproca en el ejercicio de ellas[645]. Esta Ley es clave en la historia de la Policía por cuanto, por primera vez, dota a sus miembros de un eminente carácter profesional al considerarles en servicio permanente para intervenir en cualquier hecho o circunstancia que lo demande, exigirles dedicación exclusiva y vincularles con un riguroso régimen de incompatibilidades para el desempeño de cualquier otra función, "salvo la administración del propio patrimonio"[646] y porque, también por primera vez, convoca plazas para el acceso de mujeres al *Cuerpo Superior de Policía*, incorporándose un año después las primeras cuarenta y dos Inspectoras de Policía. Este mismo proceso se produce en 1984 en el *Cuerpo de Policía Nacional*, al que acceden cincuenta y tres mujeres[647]. Son años de transición y de cambios que obligan a una reflexión sobre la función y el modelo policial en la sociedad democrática, así como sus implicaciones para esa nueva dinámica social que está naciendo, por lo que autores como José María Rico tratan de contribuir con sus textos a la determinación de esos principios generales en que deba basarse la reforma de la institución policial española:

> "La evolución socio-política de los últimos cinco años -paso de un régimen autoritario a un modelo democrático, descentralización de las estructuras político-administrativas, creciente inquietud ante los problemas de seguridad ciudadana, difíciles perspectivas económicas, etc.-, así como los cambios inminentes que dicha evolución ha de suponer, justifican ampliamente la necesidad y la urgencia de estudios y discusiones sobre el sistema policial español de los años ochenta, el cual deberá ser, a nuestro parecer, sustancialmente diferente del aparato tradicional" (RICO, 1983, pág. 13).

La Constitución española (CE) de 1978 representa un hito en la historia parlamentaria española al ser elaborada y aceptada por todos, fruto del consenso y el espíritu conciliador de los representantes de las distintas facciones políticas que articulan la transición desde la dictadura franquista a un Estado social y democrático de Derecho, con forma de Monarquía parlamentaria, que defiende como valores superiores la libertad, la justicia, la igualdad y el pluralismo político, y que atribuye la soberanía nacional al pueblo[648]. Conviene en este sentido precisar la profundidad y el alcance de este concepto jurídico, siguiendo al profesor Alfonso Fernández-Miranda, conforme al cual:

> "[…] si hablamos de Estado social como concepto jurídico, sólo puede comprenderse como una profundización o una matización del Estado democrático como Estado de derecho. En este sentido, jurídicamente,

[645] IBIDEM, Artículo 4 puntos 1 y 2.
[646] IBIDEM, Artículo 4 puntos 4 y 5.
[647] Portal web de la Policía Nacional. Disponible en: https://www.policia.es/_es/tupolicia_conocenos_timeline (15/03/2024).
[648] Artículo 1º de la Constitución Española de 1978: "1). España se constituye en un Estado social y democrático de Derecho, que propugna como valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político. 2). La soberanía nacional reside en el pueblo español, del que emanan los poderes del Estado. 3). La forma política del Estado español es la Monarquía parlamentaria".

Ediciones Universidad de Salamanca | CC BY-NC-ND

> constitucionalmente, el Estado social o es Estado social y democrático de derecho o no es nada" (FERNÁNDEZ-MIRANDA CAMPOAMOR, 2003, pág. 142)

En línea con lo anterior, el Título I establece una carta de derechos y libertades de los ciudadanos que el Estado no solo debe respetar en el ejercicio de sus funciones materiales -legislación, jurisdicción y administración-, sino también garantizar frente a cualquier tipo de amenaza que impida o dificulte su virtualidad práctica. Este elenco de derechos y libertades dan cuerpo al alma de la CE que, como una de las más avanzadas del constitucionalismo europeo, ha permitido:

> "[…] una convivencia democrática, en el marco de un Estado de Derecho consolidado, en el que los derechos y libertades de los españoles están protegidos y, de igual modo, están garantizadas las culturas y tradiciones, lenguas e instituciones de todos los pueblos de España, en el marco de una sociedad democrática avanzada que promueve el progreso de la cultura y de la economía para asegurar a todos unas mínimas condiciones de vida. Y esto es lo que, en el marco de las constituciones de la posguerra, se propuso el Poder Constituyente; así lo declaró, de manera expresa, en su Preámbulo" (MARAÑÓN GÓMEZ & ARÉVALO GUTIÉRREZ, 2019, págs. 13-14).

Uno de los desafíos que afronta la CE en cuanto norma fundamental y fundamentadora de los valores democráticos es la gestión del equilibrio entre la *seguridad* y el respeto a la *libertad y los derechos ciudadanos*, puesto que de la primera depende poder disfrutar de estos últimos. Para ello comienza delimitando y distinguiendo claramente las funciones atribuidas a las Fuerzas Armadas en el Título Preliminar, artículo 8 CE, con eminente vocación de defensa militar de la seguridad del Estado frente a las amenazas exteriores[649] y, en el Título IV dedicado al Gobierno y la Administración, en el artículo 104, reafirmando así su naturaleza civil, las que corresponden a las Fuerzas y Cuerpos de Seguridad, responsables de la seguridad interior para la garantía y protección de los derechos y libertades ciudadanas[650]. Esta ordenación constitucional somete a las Fuerzas y Cuerpos de Seguridad a la consideración de *servicio público para la comunidad* que, en su sentido material, engloba el "servicio policial en sentido estricto, las actividades administrativas de carácter complementario e inseparable de aquél y, finalmente, las actividades que convergen en la realización de una situación de seguridad"[651].

Otro argumento relevante que trata la CE es el referido a la *seguridad pública* como competencia exclusiva del Estado, tal y como establece el artículo 149.1.29 CE, "sin perjuicio de la posibilidad de creación de policías por las Comunidades Autónomas en la

[649] Artículo 8 de la CE: "Las Fuerzas Armadas, constituidas por el Ejército de Tierra, la Armada y el Ejército del Aire, tienen como misión garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional".

[650] Artículo 104 de la CE: "1) Las Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. 2) Una ley orgánica determinará las funciones, principios básicos de actuación y estatutos de las Fuerzas y Cuerpos de seguridad".

[651] Sentencia Tribunal Constitucional (Pleno), S 30-09-1999, nº 175/1999, BOE 263/1999, de 3 de noviembre de 1999, rec. 745/1990. BOE núm. 263, de 3 de noviembre de 1999. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-1999-21324 (14/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

forma que se establezca en los respectivos Estatutos en el marco de lo que disponga una ley orgánica". La organización del Estado de las Autonomías determina la coexistencia de *Cuerpos de Policía estatales, autonómicos y locales*, cuya delimitación competencial y necesaria coordinación se vertebra al amparo de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (LOFCS). A tenor de la interpretación del Tribunal Constitucional, la seguridad pública en su *aspecto material* es competencia inalienable y exclusiva del Estado que delega, en las Comunidades Autónomas que desarrollen la competencia, el *aspecto orgánico* en cuanto servicio disponible para garantizar dicha seguridad[652]. En lo que respecta a los Cuerpos de Policía dependientes de las Corporaciones Locales resaltar, por un lado, su naturaleza civil y, por otro, que asumen competencias urbanas para el mantenimiento de la seguridad ciudadana, siendo coordinados por las Comunidades Autónomas a cuyo ámbito territorial pertenezcan.

En último lugar, dentro de en este repaso a la consideración de la seguridad pública en la CE, debemos referirnos a las fronteras de ésta con la actividad de la seguridad privada, en el marco de una realidad cambiante y cada vez más tecnificada y compleja, que exige dar entrada a los actores particulares con intereses en el sector que, apelando a la gobernanza, demandan poder implicarse en la prestación de las distintas facetas de la seguridad e intermediar entre el Estado, titular exclusivo de la competencia, y el ciudadano, legítimo titular del derecho y objetivo final de aquella.

Sobre estos cimientos, la Ley 5/2014 de Seguridad Privada interpreta la alianza público privada como la base de este sector que, aunque con entidad propia, está regulado por ley e intervenido por cuanto su actividad se somete a la autorización previa, al control permanente y a la sanción administrativa. Todo ello le confiere el carácter de parte integrante de la seguridad pública, a la que se subordina desde el respeto a la Constitución y la colaboración con las Fuerzas y Cuerpos de Seguridad, a las que tienen especial obligación de auxiliar[653] en los aspectos relativos al servicio que presten. Este diseño normativo reserva en exclusiva a las Fuerzas y Cuerpos de Seguridad las funciones esenciales de garantía de la seguridad ciudadana, permitiendo la colaboración y el auxilio de las entidades de seguridad privada. De otra forma, se contravendría el mandato constitucional "al permitir que agentes privados asumieran funciones que son propias y exclusivas del Estado; descartándose, igualmente, que la seguridad sea un servicio público cuya ejecución pueda encomendarse al sector privado" (RIDAURA MARTÍNEZ, 2014, pág. 345). Se configura así un modelo en el que la seguridad privada es un *recurso externo que complementa a la seguridad pública*, de la que forma parte.

En lo que respecta a la institución policial, la consolidación de la democracia trae consigo cuestiones de gran calado como la sustitución del concepto de *orden público* por el de *seguridad ciudadana*, la asignación de funciones proactivas para la protección y asistencia a los ciudadanos en vez de la superada acción reactiva y represiva del delito

[652] Sentencia Tribunal Constitucional (Pleno), S 05-12-1984, nº 117/1984, BOE 305/1984, de 21 de diciembre de 1984, rec. 371/1982. BOE núm. 305, de 21 de diciembre de 1984. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-1984-27958 (14/03/2024).

[653] Artículo 4.2 de la LOFCS y artículo 8 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, que establece los principios rectores de esta actividad.

Ediciones Universidad de Salamanca | CC BY-NC-ND

y, lógicamente, la consagración de la Policía *al servicio de la comunidad* para garantizar sus derechos y libertades constitucionalmente reconocidos. Esta línea de pensamiento es impulsada por los técnicos e intelectuales de la época, que publican estudios en los que sustentan estas premisas que han de conformar el nuevo modelo policial español:

> "Una sociedad democrática necesita cierto orden y seguridad, pero también precisa de libertad. De ahí la importancia de establecer un equilibrio escrupuloso entre los poderes indispensables para el cumplimiento de la misión policial y el derecho del ciudadano a ser protegido contra los abusos posibles cometidos en el ejercicio de tales poderes" (RICO, 1983, pág. 211).

De esta forma, junto a lo anterior, se presenta como concepto clave para entender el profundo cambio operado en la naturaleza, capacitación, estructura y funciones de la Policía:

> "[…] asumir la idea de que sobre las organizaciones y Cuerpos policiales existe una cúpula civil, una cúpula que emana del poder político, que a su vez emana del poder soberano del pueblo, y que esta cúpula es la que dirige toda la política policial, toda la política de seguridad" [654].

Consecuencia de este ánimo democrático que visualiza a la Policía como *servicio público*, el artículo 1 de la LOFCS sigue el principio instaurado por la CE al afirmar que la seguridad pública es competencia exclusiva del Estado y que su mantenimiento corresponde al Gobierno de la nación, pasando a definir el modelo policial actual en el que las Comunidades Autónomas y las Corporaciones Locales participan del mantenimiento de la seguridad pública. Asimismo, marca la existencia de dos Cuerpos de carácter estatal, el *Nacional de Policía*, de naturaleza civil y resultado de la unificación de los anteriores *Cuerpos Superior de Policía y Policía Nacional*, y el de la *Guardia Civil*[655], de naturaleza militar, haciendo entre ellos una distribución territorial[656] y material de competencias que han de desempeñar desde el mandato de cooperación recíproca [657].

Esta Ley muestra también su carácter innovador por cuanto aplica a todos los Cuerpos y Fuerzas de Seguridad, sean estatales, autonómicos o locales, "los principios deontológicos más avanzados que se han establecido por los legisladores internacionales de las Naciones Unidas y del Consejo de Europa"[658], imponiendo el respeto a la Constitución, la neutralidad política e imparcialidad en el cumplimiento de sus funciones, el servicio permanente a la comunidad y el respeto al honor y la dignidad de la persona, entre otros[659]. También supone un importante avance el reconocimiento a los miembros del *Cuerpo Nacional de Policía* del derecho a afiliarse y participar activamente en organizaciones sindicales profesionales, cuestión nunca antes contemplada.

[654] Diario de Sesiones del Congreso de los Diputados, núm. 259, de 10 de diciembre de 1985, p. 11730.
[655] Artículo 9 de la LOFCS.
[656] IBIDEM, Artículo 11.
[657] IBIDEM, Artículo 12.
[658] Diario de Sesiones del Congreso de los Diputados, núm. 259, de 10 de diciembre de 1985, p. 11743.
[659] IBIDEM, Artículo 5.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Fruto de este periodo democrático que da vida al *Cuerpo Nacional de Policía* como heredero de aquella *Superintendencia General de la Policía del Reino* de 1824, creada "para reprimir el espíritu de sedición, extirpar los elementos de discordia y desobstruir todos los manantiales de prosperidad" (DE ANTÓN LÓPEZ, 2000, pág. 22), hoy los ciudadanos disponen de una Policía que ha experimentado un profundo proceso de transformación en su estructura, en su organización, en las técnicas y los procedimientos operativos que aplica en el desempeño de sus funciones para cumplir con la misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, lo que le convierte en referente nacional e internacional de operadores de seguridad pública, todo lo cual tiene reflejo en su consideración como una de las instituciones mejor valoradas por la sociedad española.

Queda por tanto evidenciado que nuestra ya madura pero aún joven Constitución, siguiendo la vieja tradición liberal que fijaba como objetivo de la acción del gobierno alcanzar la felicidad de todos a través de la protección de los derechos humanos, consagra la seguridad como un derecho fundamental y que, conforme a ello, podemos concluir que en la actualidad:

> "[…] junto a la defensa nacional y las finanzas públicas la organización de la seguridad de los ciudadanos constituye uno de los monopolios incontestados del Estado" (RICO & SALAS CALERO, 1988, pág. 13).

4.2. Los distintos planos conceptuales de la seguridad en la Constitución de 1978

Conocida ya la azarosa trayectoria del constitucionalismo español, definida como se ha visto por textos ideologizados y partidistas que, cíclicamente, van dejando fuera de su foco al sector de la ciudadanía que no se siente representado por el legislador de turno, hasta llegar al último cuarto del siglo XX en que, con amplia mayoría, se aprueba una Constitución como máxima de derecho y de organización social que ha de llevar al país al más dilatado periodo de democracia y paz en libertad, se plantea ahora el análisis del sentido y el alcance de la seguridad en la vigente *norma de normas*, impregnada de ese principio democrático que "penetra todas las instancias constitucionales, lo mismo aquellas que ejercen un poder político efectivo que aquellas que ostentan una representatividad meramente formal" (COELLO DE PORTUGAL, 2020, pág. 63), como consecuencia de la lógica evolución del conjunto normativo y de la sociedad a la que se aplica. A ello debe sumarse que el verdadero éxito de la CE de 1978 es su capacidad para generar la *adhesión emocional* de la gran mayoría de los españoles (GRANDE-MARLASKA, y otros, 2019, pág. 38), cuestión nunca antes conseguida tal y como hemos podido analizar en el epígrafe anterior.

Partiendo de que "las funciones de autoridad producen de un modo necesario efectos sociales, aun sin proponérselo" (JELLINEK, 2000, pág. 549), la consideración de la seguridad como base para el desarrollo de una sociedad moderna, democrática y justa es uno de los factores que contribuye a que la Constitución la recoja en varias partes de su articulado con distintas acepciones, de manera explícita en unos casos e implícita en otros, toda vez que los ámbitos de competencia del Estado y la exigencia de fines

Ediciones Universidad de Salamanca | CC BY-NC-ND

corporativos se expanden motivados por el surgimiento de nuevos aspectos del interés público que, como consecuencia de la interrelación cada vez más profunda entre lo político, lo económico y lo social, conllevan una ampliación de la dimensión de los derechos ciudadanos, como los de libertad y propiedad, que en todo caso deben ser interpretados y modulados conforme a los valores superiores de la vida en sociedad, pues "ni el derecho de libertad puede ser absoluto ni la propiedad puede ser utilizada contrariamente a los intereses de la comunidad" (GARRIDO FALLA, 1959, pág. 15).

Inicia el Preámbulo, a modo de enunciado de los objetivos pretendidos por la nación constituyente que han de guiar la parte orgánica del texto, refiriéndose a la seguridad, la justicia, la libertad y el bien común como líneas maestras del proyecto de convivencia democrática que, bajo el modelo de Estado de Derecho, han de promover el bienestar ciudadano y la propiedad privada que conduzcan a la seguridad propia de una vida digna y de calidad. Este discurso inicial, claro homenaje a aquellas primeras Declaraciones de Derechos del último cuarto del siglo XVIII, da entrada a un concepto de seguridad amplio que envuelve múltiples aspectos del orden económico, social, político e, incluso, del ejercicio de los derechos humanos en la búsqueda del ideal moderno que, junto a la consagración de la libertad y la igualdad de todos los hombres, enarbola la bandera de la propiedad, la felicidad y la seguridad.

4.2.1. El Título Preliminar de la Constitución Española de 1978

La primera referencia implícita a la *seguridad* es a través del artículo 8.1 CE, partiendo de que "las Fuerzas Armadas son la base de la Defensa Nacional, pues son las llamadas a hacerla efectiva; ya que atienden a la seguridad y procuran la protección de los elementos humano, material y territorial en los que se asienta el Estado" (MARTÍNEZ ATIENZA, 2020, pág. 30). A continuación, les encomienda la doble misión de, primeramente, garantizar la soberanía e independencia de la nación y, en segundo lugar, la defensa de su integridad territorial y del ordenamiento constitucional. Este mandato debe a su vez interpretarse en referencia a los artículos 97 CE, por cuanto es el Gobierno quien dirige la defensa del Estado, y al 149.1.4 CE que reserva la *seguridad de la nación* como competencia exclusiva del Estado[660].

A nuestro criterio, esta alusión a la protección de la seguridad exterior del Estado pierde virtualidad hoy día ante los nuevos riesgos derivados, por un lado, del contexto geopolítico del siglo XXI que dispone las relaciones internacionales en torno a un inestable tablero de juego y, por otro, de la sociedad hiperconectada, *infoxicada* y altamente dependiente de la tecnología. Fruto de todo ello, los riesgos se han deslocalizado y las amenazas modernas son globales y transversales, se han despojado de esa clásica idiosincrasia interna o externa y obligan a definir un concepto extensivo de seguridad que tenga en consideración los riesgos para la humanidad, sin desatender tampoco a consideraciones de naturaleza civil o militar. Es así como la nueva dimensión humana de la seguridad se vincula con la defensa del Estado, por cuanto el interés general pasa necesariamente por el respecto a los derechos fundamentales

[660] El artículo 149.1.4 CE establece que "El Estado tiene competencia exclusiva sobre las siguientes materias: 4ª) Defensa y Fuerzas Armadas".

Ediciones Universidad de Salamanca | CC BY-NC-ND

constitucionalmente protegidos que, según establece el artículo 10.2 CE, han de interpretarse conforme a la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales ratificados por España.

Por su parte, el artículo 9.3 CE recoge la primera conceptualización programática del texto constitucional, en este caso a través de la *seguridad jurídica*[661], que obliga a los poderes públicos, por un lado, a la claridad destinada a dar certeza a los ciudadanos respecto de la norma o la conducta exigible para su cumplimiento y, por otro, a la previsibilidad para aquellos de los efectos de su aplicación (UGARTEMENDIA ECEIZABARRENA, 2006, pág. 22), cuestión que entronca con el resto de principios que la acompañan: legalidad, jerarquía y publicidad de la norma, irretroactividad de la no favorable o restrictiva de derechos, y prohibición de la arbitrariedad de los poderes públicos.

Estos conceptos no son estancos sino que, antes bien, se complementan conjuntamente para servir al objetivo principal, cual es promover los valores superiores del ordenamiento jurídico que propugna el Estado social y democrático de Derecho, tal y como indica la Sentencia del Tribunal Constitucional 104/2000[662]. En igual sentido se manifiesta el Consejo de Estado, una de las instituciones que debe preocuparse del cumplimiento de las garantías constitucionales, al considerar un aspecto fundamental de la seguridad jurídica:

> "[…] que todos, tanto los poderes públicos como los ciudadanos, sepan a qué atenerse; lo cual supone, por un lado, un conocimiento cierto de las leyes vigentes, y por otro una cierta estabilidad de las normas y de las situaciones que en ella se definen. Estas dos circunstancias -certeza y estabilidad de las normas- son muy importantes en un estado de Derecho, donde no cabe la posibilidad dialéctica de que se viva *sine lege certa, sine iure certo*"[663].

4.2.2. El Título I "De los derechos y deberes fundamentales"

El Capítulo Segundo "Derechos y libertades", es una auténtica declaración de derechos fundamentales que inicia consagrando la igualdad entre los iguales para, seguidamente, en los artículos 16.1 y 21.2 CE dar entrada a un renovado concepto de *orden público* como garantía del ejercicio libre y pacífico de los derechos constitucionalmente

[661] Artículo 9.3 CE: "La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos".
[662] Tribunal Constitucional (Pleno), S 13-04-2000, nº 104/2000, BOE 119/2000, de 18 de mayo de 2000, rec. 2300/1993. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2000-9229 (23/04/2024).
[663] Memoria del año 1992 que el Consejo de Estado en Pleno eleva al Gobierno, en cumplimiento de lo dispuesto en el artículo 20.3 de la Ley Orgánica 3/1980, de 23 de abril. Madrid 1993. Disponible en: https://www.consejo-estado.es/wp-content/uploads/2021/05/MEMORIA-1992.pdf (24/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

reconocidos de libertad ideológica, religiosa y de culto[664], y de reunión[665] respectivamente, que pueden ser restringidos en aquellas situaciones concretas que, de manera fundada, generen peligro para las personas o los bienes (FREIXES SANJUÁN & REMOTTI CARBONELL, 1995, pág. 148). Solo en estos dos artículos se refiere la Constitución a este nuevo concepto de orden público concreto y definido en su alcance limitador, dispuesto en torno al interés legítimo de la colectividad en el ejercicio pacífico de los derechos fundamentales y que, en definitiva, se aleja de la interpretación tradicional de orden público como habilitación amplia e indeterminada asociada al autoritarismo y a la actuación policial que "fue durante mucho tiempo una cláusula de apoderamiento de la Administración que ha servido para amparar prácticas restrictivas o ablativas de los derechos y libertades fundamentales" (CHINCHILLA MARÍN, 1986, pág. 12). No es por ello casual que la Constitución no invoque al orden público cuando, en el artículo 104 CE, asigna sus funciones a las Fuerzas y Cuerpos de Seguridad y opta por referirse a la *seguridad ciudadana* o cuando, en el artículo 149.1.29 CE, determina en exclusividad la competencia del Estado en materia de *seguridad pública*.

También desde la consideración de derecho fundamental inherente al propio Estado de Derecho, el artículo 17.1 CE protege la libertad y *seguridad personales*[666], aprovechando para poner el foco en la excepción limitativa por excelencia de la libertad individual, la detención, que debe respetar unas garantías y está sometida a un procedimiento de control judicial inmediato, el *habeas corpus*, para evitar cualquier tipo de arbitrariedad o ilegalidad que pudiera amenazar o restringir estos derechos.

Por la relevancia que tiene para la hipótesis planteada en este estudio, es necesario referirse al artículo 20.1.d CE[667] que, implícitamente, sugiere una interpretación amplia de la *seguridad aplicada al uso y consumo de información*, en cuanto protege el derecho de la ciudadanía a comunicar o recibir libremente información veraz por cualquier medio de difusión. Ampara la norma tanto el ejercicio activo como pasivo de la comunicación, singularizando en la veracidad de su contenido el criterio condicionante de su legitimidad. Sin embargo, la jurisprudencia no interpreta en sentido estricto y objetivo el carácter veraz de lo publicado o difundido, en cuanto a que no pueda resultar erróneo, sino que establece un deber de diligencia sobre el informador profesional al que exige que contraste y verifique los hechos con datos objetivos[668]. Conforme a esta

[664] Articulo 16.1 CE: "Se garantiza la libertad ideológica, religiosa y de culto de los individuos y las comunidades sin más limitación, en sus manifestaciones, que la necesaria para el mantenimiento del orden público protegido por la ley".

[665] Artículo 21 CE: "1) Se reconoce el derecho de reunión pacífica y sin armas. El ejercicio de este derecho no necesitará autorización previa.

2) En los casos de reuniones en lugares de tránsito público y manifestaciones se dará comunicación previa a la autoridad, que sólo podrá prohibirlas cuando existan razones fundadas de alteración del orden público, con peligro para personas o bienes".

[666] Artículo 17. 1. CE: "Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley".

[667] Artículo 20.1. CE: "Se reconocen y protegen los derechos: d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades".

[668] STC 297/2000, de 11 de diciembre de 2000. Recurso de amparo 1718/1997. Promovido por don Juan José Medina Roldán frente a las Sentencias de la Audiencia Provincial de Málaga y del Juzgado de lo Penal

Ediciones Universidad de Salamanca | CC BY-NC-ND

interpretación, que para algunos autores es una "diligencia que parece podría justificar incluso una información falsa" (MARTÍN REBOLLO, 2012, pág. 103), la veracidad no es equivalente a la verdad absoluta ni constituye un elemento conformador del derecho a recibir información. Como explica la profesora Serra Cristóbal:

> "La veracidad supone imponer al informador un deber de diligencia en la obtención de la información que comunica, aunque esta no sea totalmente exacta o los errores en que se incurra sean meramente circunstanciales y no afecten a la totalidad de la información" (SERRA CRISTÓBAL, 2023, pág. 23)

Pero lo anterior no significa que se amparen los bulos o la información que pretendidamente falta a la verdad, puesto que la Constitución solo protege la transmisión de información veraz. Es decir:

> "[…] pese a que, de entrada, no puede prohibirse la transmisión de hechos no veraces, -es decir, cabe mentir-, esa transmisión de hechos falsos no puede considerarse como el ejercicio de un derecho fundamental y, por lo tanto, esa transmisión de información falsa nunca puede prevalecer frente a la protección de otros derechos e intereses constitucionales con los que pudiera colisionar. En la medida en que la comunicación de hechos queridamente falsos (*fake news*) genere o pueda generar daños en ellos, cabrá establecer restricciones a la comunicación falsa y, en su caso, exigir responsabilidades" (SERRA CRISTÓBAL, 2023, págs. 23-24).

Esta matización es relevante pues, como señala el *Procedimiento de actuación contra la desinformación* aprobado por el Consejo de Seguridad Nacional:

> "[…] el acceso a información veraz y diversa es uno de los pilares que sustentan a las sociedades democráticas y que deben asegurar las instituciones y administraciones públicas, porque se conforma como el instrumento que permite a los ciudadanos formarse una opinión sobre los distintos asuntos políticos y sociales. Además, la información permite a la ciudadanía adquirir conciencia y fundamento para participar en los debates públicos y, entre otros derechos democráticos, en los procesos electorales"[669].

Avanzando en la cuestión, las libertades de expresión e información son principios fundacionales del Estado social y democrático de derecho que, en nuestra Constitución, se formulan en relación al modelo clásico de comunicación que no contempla el actual desarrollo del ciberespacio ni el nuevo rol de sujeto receptor/emisor que se asume en este proceso y que, paradójicamente, debería ser el ámbito donde tuviesen su principal

número 1 de Melilla que le condenaron por delito de injurias a causa de reportajes publicados en "El Telegrama de Melilla". Vulneración de los derechos a la libre expresión e información: polémica periodística sobre asuntos de interés público y personas con relevancia pública, mediante información comprobada, sea o no objetivamente verdadera y empleando expresiones que no añaden un plus de lesión al honor del afectado. BOE núm. 14, de 16 de enero de 2001. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-2001-1136 (12/11/2023).

[669] Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Apartado 1. Contexto. Disponible en: https://www.boe.es/eli/es/o/2020/10/30/pcm1030/con (13/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

acople (CAPODIFERRO CUBERO, 2017, págs. 704-705). No obstante, el espíritu protector de las libertades de expresión e información es el mismo tanto para el *entorno analógico como para el digital*.

En este sentido, partiendo de la premisa de que la democracia tiene uno de sus pilares en la libre afirmación de ideas y opiniones en el espacio público y que, por ello, el ejercicio del derecho de reunión y manifestación como cauces de participación ciudadana están íntimamente unidos al derecho fundamental de la libertad de expresión, algunos autores como el profesor Ricardo García han estudiado la utilización del espacio virtual como medio para articular el ejercicio de este derecho fundamental, refiriéndose a la manifestación virtual, *netstrike* o cibermanifestación. Parece que bastase el espacio virtual para la afirmación colectiva de pensamientos y opiniones, quedando incluso relegado el espacio público por cuanto no hay convocatoria que no use las nuevas tecnologías para tratar de alcanzar mayor difusión de sus consignas o lemas reivindicativos. Sin embargo, esto no es así. El espacio virtual debe analizarse como un elemento más de la convocatoria que, ahora, tiene un doble componente en el que se correlacionan la participación de los ciudadanos en las redes sociales y, al tiempo, en la movilización física comunicada previamente a la autoridad gubernativa. Conforme a ello, podemos concluir que:

> "[…] el uso de las tecnologías de la información lo que posibilita es que el derecho de reunión tenga múltiples actuaciones e interacciones antes de la reunión y manifestación -en sí misma-, antes, durante y después, de forma que el elemento espacial se modifica de forma esencial, transformándose así en uno de sus elementos claves en el ejercicio de este derecho, pero ganándose en participación y efectividad potencial del mensaje, lemas o denuncias que se persigan" (GARCÍA GARCÍA, 2019, pág. 34).

Esta es la clave para entender por qué la desinformación brota, ayudada por la evolución tecnológica y la transformación digital colectiva, en las propias grietas de la sociedad, comprometiendo de esta forma la estabilidad democrática. Se trata de un problema complejo que interrelaciona variables de distinta naturaleza y contenido como son, por ejemplo, la protección de la libertad de expresión y el derecho de información en Internet, el fenómeno de la polarización ideológica que da la espalda al consenso como argumento básico de funcionamiento de la democracia, la expansión de las plataformas y redes sociales como modernos púlpitos desde los que transmitir mensajes y narrativas para persuadir e incitar al grupo sin responsabilidad alguna por la calidad de la información allí vertida, o la pérdida del papel de intermediación de la prensa tradicional, cuya credibilidad se resintió a partir de la llegada del conocido como *periodismo ciudadano* y la concentración del sector en grandes grupos empresariales, instrumentalizados por intereses económicos y políticos que cedieron ante el producto periodístico que mezcla información con opinión.

Dentro de este Título I, el Capítulo Tercero "De los principios rectores de la política social y económica", vincula la *seguridad con las relaciones de trabajo* en su artículo 40.2 CE[670]

[670] Artículo 40.2 CE: "Asimismo, los poderes públicos fomentarán una política que garantice la formación y readaptación profesionales; velarán por la seguridad e higiene en el trabajo y garantizarán el descanso

Ediciones Universidad de Salamanca | CC BY-NC-ND

en el ánimo de reforzar la protección del ciudadano frente a los riesgos y accidentes en el entorno laboral, como criterio interpretativo y de ordenación de la realidad cotidiana en un Estado social y democrático donde el trabajo se eleva a la categoría de derecho.

A continuación, el artículo 41 CE obliga a los poderes públicos a mantener un sistema de *Seguridad Social*[671] que integra distintas facetas derivadas, a tenor de la evolución histórica, de la *seguridad nacional*, de la *seguridad física interior* y de la *seguridad jurídica* congregadas en torno al natural deseo de bienestar en relación con el sistema económico actual, que busca garantizar las prestaciones ante situaciones de necesidad o de desempleo, así como la asistencia completa sanitaria (JORDANA DE POZAS, 1951, pág. 23), que junto con el derecho de participación del artículo 129 CE y la reserva competencial del 149.1.17 CE, conforman un sistema "conscientemente pretendido de solidaridad entre personas de la misma generación, entre generaciones y territorios" (ALONSO SECO, 2020, pág. 159), que da soporte al moderno Estado del bienestar. En este sentido, la propia historia nos condiciona tal y como señala el profesor Maravall al escribir sobre la mentalidad social del Estado Moderno:

> "No cabe duda de que la medicina está íntimamente ligada a la política. Tal vez, convencido de esta idea, Felipe II, en 1566, se ocupa de reunir los varios hospitales que había en Madrid, en un solo hospital general, que aparece ya establecido en el plano de Texeira, de 1596. El Estado necesita gente fuerte y sana y solo manteniendo un excelente estado sanitario general conseguirá ese objeto: la sanidad es, pues, un fin del Estado" (MARAVALL CASESNOVES, 1986, pág. 266).

Cierra este Capítulo el artículo 51.1 CE con el compromiso de los poderes públicos de garantizar la *seguridad de consumidores y usuarios*[672], que engloba entre otras la defensa de sus legítimos intereses económicos y sociales, la protección contra los riesgos derivados de las relaciones de consumo y el derecho a obtener información oportuna, accesible y correcta que facilite el uso y disfrute de los bienes o servicios afectados por sus decisiones o intereses que, en todo caso, deben ser seguros[673].

necesario, mediante la limitación de la jornada laboral, las vacaciones periódicas retribuidas y la promoción de centros adecuados".

[671] Artículo 41 CE: "Los poderes públicos mantendrán un régimen público de Seguridad Social para todos los ciudadanos, que garantice la asistencia y prestaciones sociales suficientes ante situaciones de necesidad, especialmente en caso de desempleo. La asistencia y prestaciones complementarias serán libres".

[672] Artículo 51.1 CE: "Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos".

[673] El artículo 11 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias define el *deber general de seguridad*: "1. Los bienes o servicios puestos en el mercado deben ser seguros.

2. Se consideran seguros los bienes o servicios que, en condiciones de uso normales o razonablemente previsibles, incluida su duración, no presenten riesgo alguno para la salud o seguridad de las personas, o únicamente los riesgos mínimos compatibles con el uso del bien o servicio y considerados admisibles dentro de un nivel elevado de protección de la salud y seguridad de las personas".

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.2.3. El Título IV "Del Gobierno y la Administración"

La primera referencia en este Título IV a la *seguridad* se materializa en el artículo 102 CE al delimitar la competencia del Tribunal Supremo para determinar la responsabilidad del presidente y demás miembros del Gobierno cuando se trate de traición o delitos contra la *seguridad del Estado* en el ejercicio de sus funciones[674]. Los requisitos singulares exigidos para plantear la acusación por estos delitos ya indica que se trata de salvaguardar la *seguridad nacional*, interés general cualificado, cuando pueda verse efectivamente comprometida y en riesgo por las acciones de los miembros del Gobierno en atención al ejercicio de las actividades propias del cargo, que revelen una peligrosidad incompatible con la confianza y certeza que han de proporcionar los representantes de un Estado democrático a sus ciudadanos. Esta referencia a la seguridad del Estado entronca directamente con el artículo 30 CE que dispone que "los españoles tienen el derecho y el deber de defender España", entendiendo con ello "la protección del conjunto de la sociedad española, de su Constitución, de los valores superiores, principios e instituciones que en ésta se consagran, del Estado social y democrático de Derecho, del pleno ejercicio de los derechos y libertades, y de la garantía, independencia e integridad territorial de España"[675] así como la contribución a la paz y seguridad internacionales conforme a los compromisos por ella contraídos.

Similar consideración tiene la mención a la seguridad y defensa del Estado que hace el artículo 105.b CE al referirse a los límites de acceso de los ciudadanos a los archivos y registros administrativos, y cuyo desarrollo lleva a cabo la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que busca garantizar el acceso a la información pública de todos los ciudadanos, siempre y cuando no suponga un perjuicio para la *seguridad nacional, la defensa o la seguridad pública*, entre otras[676], atendiendo al caso concreto y de manera justificada y proporcional a su objeto y finalidad.

---

[674] Artículo 102 CE: "1) La responsabilidad criminal del Presidente y los demás miembros del Gobierno será exigible, en su caso, ante la Sala de lo Penal del Tribunal Supremo.
2) Si la acusación fuere por traición o por cualquier delito contra la seguridad del Estado en el ejercicio de sus funciones, sólo podrá ser planteada por iniciativa de la cuarta parte de los miembros del Congreso, y con la aprobación de la mayoría absoluta del mismo.
3) La prerrogativa real de gracias no será aplicable a ninguno de los supuestos del presente artículo".

[675] Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, Artículo 2 "Finalidad de la política de defensa".

[676] El artículo 14 de la citada Ley 19/2013 recoge los límites al derecho de acceso:"1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para: a) La seguridad nacional. b) La defensa. c) Las relaciones exteriores. d) La seguridad pública. e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios. f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva. g) Las funciones administrativas de vigilancia, inspección y control. h) Los intereses económicos y comerciales. i) La política económica y monetaria. j) El secreto profesional y la propiedad intelectual e industrial. k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión. l) La protección del medio ambiente.
2. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.
3. Las resoluciones que de conformidad con lo previsto en la sección 2.ª se dicten en aplicación de este artículo serán objeto de publicidad previa disociación de los datos de carácter personal que contuvieran

Ediciones Universidad de Salamanca | CC BY-NC-ND

De especial relevancia a tenor del objeto de este estudio y en el ánimo de la claridad conceptual, es la referencia al artículo 104 CE[677] que vincula la garantía de la *seguridad ciudadana* con la misión asignada a las Fuerzas y Cuerpos de Seguridad, dependientes del Gobierno, de proteger el libre ejercicio de los derechos y libertades. En este artículo se encuentra la única referencia de la Carta Magna a la seguridad ciudadana, concepto novedoso "en la historia constitucional española, en la que tradicionalmente la misión de las Fuerzas y Cuerpos de Seguridad ha sido la de proteger el denominado orden público u orden interior" (FREIXES SANJUÁN & REMOTTI CARBONELL, 1995, pág. 144). En este sentido material la *seguridad ciudadana* consiste en la ejecución por parte de las Fuerzas y Cuerpos de Seguridad de las actuaciones, distintas por su naturaleza y contenido, de carácter preventivo, investigativo, reactivo y de restitución necesarias para garantizar un entorno de tranquilidad y exento de peligros o perturbaciones en el que los ciudadanos puedan libre y pacíficamente ejercer los derechos que la Constitución y las leyes les reconocen, encomendando el desarrollo positivo de dichas funciones y de los principios básicos inspiradores de esa labor protectora a la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

Esta configuración de la *seguridad ciudadana como servicio público* implica su asignación funcional al Estado como eje vertebrador del ejercicio de la autoridad que debe garantizar su efectividad. Es decir, "la seguridad ciudadana está reservada, constitucionalmente, en exclusiva a la Administración Pública, ya que es una función de soberanía. En consecuencia, no existirá la posibilidad de encomendar su gestión a agentes externos, de los que puede predicarse su colaboración, pero no la asunción de las funciones que el texto constitucional encomienda en exclusiva a las Fuerzas y Cuerpos de Seguridad" (RIDAURA MARTÍNEZ, 2014, pág. 342). Esta caracterización de la *Policía como servicio público*, en cuanto ejercicio soberano del poder del Estado, se aprecia en los fundamentos jurídicos de la Sentencia del Tribunal Constitucional 55/1990, de 28 de marzo[678], que literalmente afirma:

> "De la Constitución se deduce que las Fuerzas de Policía están al servicio de la comunidad para garantizar al ciudadano el libre y pacífico ejercicio de los derechos que la Constitución y la Ley les reconocen, y este es el sentido del art. 104.1 CE que puede considerarse directamente heredero del art. 12 Declaración de Derechos del Hombre y del Ciudadano, configurando a la Policía como un servicio público para la comunidad, especializado en la prevención y lucha contra la criminalidad, el mantenimiento del orden y la seguridad pública y la protección del libre ejercicio de los derechos y libertades".

Continúa el alto tribunal interpretando el texto constitucional, subrayando la doble encomienda del artículo 104.1 CE, positiva respecto a la atribución a las Fuerzas y

y sin perjuicio de lo dispuesto en el apartado 3 del artículo 20, una vez hayan sido notificadas a los interesados.

[677] Artículo 104 CE:" 1. Las Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. 2. Una ley orgánica determinará las funciones, principios básicos de actuación y estatutos de las Fuerzas y Cuerpos de seguridad".

[678] Tribunal Constitucional (Pleno), S 28-03-1990, nº 55/1990, BOE 92/1990, de 17 de abril de 1990.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Cuerpos de Seguridad de la función de garantizar las libertades y derechos fundamentales, y restrictiva por cuanto su actuación protectora frente a las amenazas que puedan poner en riesgo a los ciudadanos debe en todo caso respetar esos mismos derechos y libertades por los que vela. De aquí la interpretación de la seguridad ciudadana como un elemento esencial del Estado de Derecho en cuanto bien jurídico colectivo que corresponde garantizar a los poderes públicos, entre los que se encuentra la Policía (RIDAURA MARTÍNEZ, 2014, pág. 339).

Esta consideración es igualmente recogida en el Preámbulo de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, cuando señala que "las demandas sociales de seguridad ciudadana van dirigidas esencialmente al Estado, pues es apreciable una conciencia social de que sólo éste puede asegurar un ámbito de convivencia en el que sea posible el ejercicio de los derechos y libertades, mediante la eliminación de la violencia y la remoción de los obstáculos que se opongan a la plenitud de aquellos".

4.2.4. El Título VIII "De la organización territorial del Estado"

El Título VIII de la Constitución, y en particular su Capítulo III, aborda la organización territorial del Estado y la distribución del poder conforme al *principio dispositivo*[679] en el marco del modelo descentralizado que propone, en cuyo entorno el artículo 149 CE se revela fundamental, pues define las competencias que asume el Estado en exclusiva y que, por ello, se configuran como un límite a las competencias autonómicas, si bien este enunciado es equívoco porque:

> "[…] a pesar de su enunciado inicial, el Estado no tiene sobre todas las materias de esa lista una competencia exclusiva en el sentido de competencia plena y que excluya a las Comunidades Autónomas. Eso es así porque el propio art. 149.1 CE admite en muchos casos la participación competencial de éstas" (MARTÍN REBOLLO, 2012, pág. 204).

Interesa al objeto de este estudio el reflejo que esta participación competencial de las Comunidades Autónomas tiene en el artículo 149.1.29 CE referido a la *seguridad pública*[680], inicialmente propuesta como exclusiva del Estado pero que se abre al desarrollo autonómico en el marco de una ley orgánica, en este caso la ya referida 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (LOFCS), cuyo artículo 1 atribuye el mantenimiento de la seguridad pública al Gobierno de la nación y, a continuación, arbitra la participación en dicha tarea de las Comunidades Autónomas y Corporaciones Locales, todas ellas a través de las Fuerzas y Cuerpos de Seguridad[681].

[679] El principio dispositivo hace referencia al modelo abierto que los constituyentes eligieron para el reparto de competencias, dentro del cual cada Estatuto de Autonomía podría establecer su organización y ámbito competencial, siempre dentro del respeto a la Constitución.

[680] Artículo 149.1.29 CE: "1. El Estado tiene competencia exclusiva sobre las siguientes materias: 29.ª) Seguridad pública, sin perjuicio de la posibilidad de creación de policías por las Comunidades Autónomas en la forma que se establezca en los respectivos Estatutos en el marco de lo que disponga una ley orgánica".

[681] Artículo 1 LOFCS: "1. La seguridad pública es competencia exclusiva del Estado. Su mantenimiento corresponde al Gobierno de la Nación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Así es como la *seguridad pública*, interés social constitucionalmente protegido, se presenta en una doble vertiente. La primera como *criterio delimitador de competencias* entre las distintas Administraciones Públicas, donde el Tribunal Constitucional[682] aprecia que deben ser en primera instancia las autoridades competentes autonómicas las que en el ejercicio de la potestad ordinaria se encarguen de mantener o restablecer la tranquilidad y el orden ciudadano, "y sólo muy excepcionalmente, cuando el ejercicio de estas potestades ordinarias sea insuficiente para mantener o restablecer la normalidad, es cuando han de entrar en juego los poderes extraordinarios del Estado. Y son, cabalmente, estos poderes excepcionales del Estado los que han de conectarse con la noción de *seguridad pública*, función del Estado concebida para situaciones de excepcional gravedad, tales como revueltas, asonadas, motines, levantamientos populares, y otras alteraciones muy graves de la convivencia ciudadana". Un ejemplo de la materialización de este aspecto extraordinario de la competencia del Estado en seguridad pública es la intervención del Ministerio del Interior de España con ocasión de la celebración del referéndum ilegal de independencia de Cataluña el 1 de octubre de 2017[683], con la puesta en marcha de la Operación Copérnico en el marco de la aplicación del artículo 155 CE para revertir dicha irregularidad constitucional, que supuso el despliegue en el territorio catalán desde septiembre hasta diciembre de ese año de más de cuarenta grupos de las Unidades de Intervención Policial, junto con otros miembros de distintas especialidades de la Policía Nacional y de la Guardia Civil procedentes del resto del país.

Pero el artículo 149.1.29 CE presenta una segunda vertiente, referida al *contenido material de la seguridad pública,* la cual trasciende el ámbito de actuación propio de las Fuerzas y Cuerpos de Seguridad para ampliarse a otras consideraciones relacionadas con la *seguridad humana* que puedan derivar en un daño grave para la sociedad, a través de riesgos y amenazas contra la salud, el medio ambiente, la protección civil o la seguridad vial, entre otras. Esta perspectiva integral de la seguridad pública es la línea conceptual que refleja la Sentencia del Tribunal Constitucional 25/2004, de 26 de marzo[684], al precisar que la seguridad pública "se refiere a la protección de personas y bienes y al mantenimiento de la tranquilidad u orden ciudadano" superando el ámbito funcional propio de las Fuerzas y Cuerpos de Seguridad y aplicando, por ello, en otros campos como el de la protección civil, si bien se trata de un concepto más restringido de lo que podría parecer por cuanto no engloba cualquier actividad que pueda tener una relación más o menos orientada a esa finalidad, sino únicamente aquellas situaciones

2. Las Comunidades Autónomas participarán en el mantenimiento de la seguridad pública en los términos que establezcan los respectivos Estatutos y en el marco de esta Ley.
3. Las Corporaciones Locales participarán en el mantenimiento de la seguridad pública en los términos establecidos en la Ley reguladora de las Bases de Régimen Local y en el marco de esta Ley.
4. El mantenimiento de la seguridad pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad.

[682] Tribunal Constitucional (Pleno), S 05-12-1984, nº 117/1984, BOE 305/1984, de 21 de diciembre de 1984.

[683] Declarado ilegal por sentencia del Tribunal Constitucional (Pleno), A 21-09-2017, nº 127/2017, BOE 229/2017, de 22 de septiembre de 2017.

[684] Tribunal Constitucional (Segunda), S 26-02-2004, nº 25/2004, BOE 74/2004, de 26 de marzo de 2004.

Ediciones Universidad de Salamanca | CC BY-NC-ND

"susceptibles de ocasionar graves riesgos para personas o bienes, lo que exige la adopción de medidas de especial intensidad".

Una vez analizadas las diversas formas en que la idea de *seguridad* se reparte por la Constitución española, con distintas acepciones que atienden a múltiples visiones de la realidad humana, puede concluirse que todas ellas comparten el común denominador de la búsqueda de protección frente a la amenaza de peligro o perturbación del normal desenvolvimiento de la actividad humana y, en su caso, el ofrecimiento de elementos de reparación que permitan restaurar la seguridad quebrantada.

En este sentido la Constitución, tras más de cuatro décadas en vigor de manera ininterrumpida, sigue siendo el alma de la estructura política y de gobierno que garantiza la protección de los intereses generales de la sociedad española identificados en la paz, la seguridad y la libertad como medios para alcanzar la prosperidad y el bienestar de la colectividad. Si bien es cierto que el trascurso del tiempo, los cambios sociales, los nuevos contenidos y demandas ciudadanas, incluso el contexto geopolítico en el que se desenvuelve el país configuran una realidad mucho más compleja, interdependiente y dinámica de la existente cuando se redactó la Constitución en el año 1978, convenimos con el Académico D. Pablo L. Murillo de la Cueva que:

> "[…] está lejos de haber agotado su cometido histórico. Sus principios inspiradores, los valores que propugna, los derechos que reconoce y garantiza, el diseño de la organización de los poderes públicos que traza y las bases del Estado autonómico que contiene siguen siendo válidos para un futuro prolongado" (LUCAS MURILLO DE LA CUEVA, 2021, págs. 24-25).

Ello no obsta para que, como señala el profesor Coello de Portugal, al albur de la necesaria adaptación a los modernos condicionantes que amenazan a la seguridad del orden democrático, como los nuevos ámbitos de confrontación y las amenazas híbridas, seamos conscientes de que tenemos que acometer cambios legislativos como lo ha sido, por ejemplo, la promulgación del Real Decreto 524/2022, de 27 de junio, por el que se dispone el cambio de denominación del *Ejército del Aire* por la del *Ejército del Aire y del Espacio*, que nos advierte sobre la necesaria reforma del artículo 8 de la Constitución para ajustarla convenientemente a los nuevos parámetros del ámbito militar (COELLO DE PORTUGAL, 2023, pág. 227).

4.3. La estructura de seguridad nacional española

Es un hecho que hoy día las políticas nacionales se muestran por sí solas insuficientes para defender sus intereses y afrontar los nuevos retos en el vigente escenario internacional definido por la globalización, la tecnología, la profunda interrelación de procesos de distinta naturaleza -políticos, demográficos, económicos, medioambientales- y la extrapolación de efectos a escala mundial de crisis que anteriormente tocaban techo a nivel local o regional. En este sentido, señala la profesora Serra Cristóbal que:

> "[…] más allá de los intereses nacionales, la visión de la seguridad y la defensa de un Estado no puede ya alejarse o eximirse de participar también en las

Ediciones Universidad de Salamanca | CC BY-NC-ND

> necesidades de la seguridad y defensa europeas y de aquellas otras relaciones que se mantienen en el marco de las organizaciones y alianzas internacionales" (SERRA CRISTÓBAL, 2015, pág. 89).

Quedan así superadas interpretaciones clásicas según las cuales:

> "[…] la seguridad nacional gira alrededor del paradigma realista, en virtud del cual la política mundial es invariablemente una lucha entre Estados por el poder, bajo una situación de anarquía, compitiendo por sus propios intereses nacionales. En ese contexto, los Estados confían en el poder militar para garantizar esos intereses contrarrestando las amenazas que surgen de la fuerza armada de otros Estados. Así, soberanía nacional y equilibrio de poder, entendido como la distribución del mismo entre los distintos Estados, se encuentran inequívocamente unidos a lo que se entiende por seguridad. Se trata de proteger, desde una perspectiva interna, los intereses nacionales" (LABORIE IGLESIAS M. , 2011, págs. 1-2).

Buena prueba de esta evolución representa, sin duda, la pandemia del COVID-19 que ha funcionado como elemento disruptor entre cuyos efectos destaca "la «ampliación y transformación del concepto de seguridad», que ha traspasado el límite de lo físico saltando a lo digital y a la gestión de crisis en el área sanitaria y de protección de la salud" (MUÑOZ MARTINEZ, 2022, pág. 148). Se trata ahora de un concepto orientado hacia la seguridad humana, abarcando sus siete aspectos: la seguridad económica, la seguridad alimentaria, la seguridad sanitaria, la seguridad ambiental, la seguridad física o personal, la seguridad comunitaria y la seguridad política, de manera que "el concepto de seguridad nacional que hoy manejamos está basado en el concepto de *seguridad humana* que pone su foco en el ciudadano […]. Es a él al que hay que proteger" (BALLESTEROS MARTÍN M. Á., 2020, pág. 13).

Parece, por tanto, ineludible el *enfoque integral de la seguridad* que, desde el compromiso de la sociedad en su conjunto y el vencimiento de los límites referidos al ámbito interior y exterior, ha de ensamblar las acciones generadas a todos los niveles -nacional, europeo e internacional- para dar una respuesta eficaz y adaptada al caso concreto. En este mismo sentido se pronunciaba la representante del Gobierno durante el debate de las enmiendas presentadas al proyecto de Ley de Seguridad Nacional del año 2015, manifestando que:

> "[…] hoy en día no es posible mantener una visión compartimentada de la seguridad […]. Cuando hablamos de seguridad integral debemos tener en cuenta no solo los riesgos más obvios, como son los conflictos armados, el terrorismo o el crimen organizado, o sus vínculos más habituales con las redes terroristas e incluso las catástrofes naturales, hoy hay que tener en cuenta otros factores que o bien potencian la peligrosidad de esos riesgos o representan verdaderas amenazas en sí mismos"[685].

[685] Debate del Proyecto de Ley de Seguridad Nacional. «BOCG. Congreso de los Diputados», serie A, número 158-1, de 29 de mayo de 2015. (Número de expediente 121/000158). Diario de Sesiones del Congreso de los Diputados, sesión plenaria núm. 278 (extraordinaria), de 8 de julio de 2015, página 30.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Como consecuencia la *seguridad nacional*, que tradicionalmente se vincula con la identidad, la independencia y la integridad del Estado, cuya defensa se confía principalmente a las fuerzas armadas, trasciende hoy día esta interpretación y se expande para poder afrontar con garantía de éxito el mayor número posible de los nuevos y complejos desafíos que pueden causar daños a sus intereses, a sus compromisos internacionales o a sus ciudadanos (BALLESTEROS MARTÍN M. A., 2016, págs. 269-274).

Pero antes de avanzar en nuestro análisis debemos abordar la delimitación conceptual, señalando algunas distinciones. En primer lugar, la que atañe a *riesgo y amenaza*, tratados mayormente como sinónimos cuando no lo son, correspondiendo el *riesgo* a:

> "[…] una contingencia o proximidad de daño, es algo potencial, es señal de alarma y de atención. La amenaza, en cambio, señala la inminencia de un acto agresivo y perjudicial para quien lo recibe. Los riesgos son la potencialidad de la amenaza, se calculan, se analizan y se afrontan mediante la prevención a través del estudio de las causas que los provocan. La amenaza es una acción que se ataja o se elimina" (JIMÉNEZ OLMOS, 2013).

En segundo lugar, debemos referirnos al concepto de *seguridad nacional* que, como tal, no aparece recogida en la Constitución Española, a diferencia de la *defensa nacional*[686] con la que a veces se confunde y mimetiza. Respecto a ésta, atendiendo a la Ley de Defensa Nacional de 2005, no encontramos en ella su definición sino, tan solo, su referencia como objeto de regulación normativa junto con el establecimiento de las bases de la organización militar. Lo mismo ocurre si acudimos a la Directiva de Defensa Nacional 2012[687], que no fija el marco teórico de la defensa nacional. Tenemos que esperar a la Directiva de Defensa Nacional 2020 para verla definida como:

> "[…] un servicio público que contribuye a mantener la seguridad y los derechos y libertades de los españoles en cualquier situación. Garantizar la Defensa Nacional constituye por ello una obligación de todo gobierno"[688].

El General Ballesteros, por su parte, hace una aproximación a ambos términos concluyendo que la *defensa nacional* puede definirse como "el diseño, desarrollo y ejecución de todas las acciones y fuerzas morales y materiales para oponerse a los peligros y amenazas que se plantean contra los intereses nacionales" (BALLESTEROS MARTÍN M. A., 2016, pág. 57), resaltando su carácter eminentemente reactivo, mientras que la *seguridad nacional* "es la situación en la que el normal desarrollo de la vida de la Nación está protegido contra riesgos, peligros o amenazas exteriores e interiores y

[686] Como ya se analizó en el Capítulo 1, la defensa nacional se constitucionaliza a través del artículo 8.1 CE, que legitima democráticamente a las Fuerzas Armadas y las responsabiliza de hacer efectiva la Defensa Nacional, mandato que se debe interpretar en referencia a los artículos 97 y 149.1.4 CE, por cuanto es el Gobierno quien dirige la defensa del Estado y, por ende, éste ostenta la competencia sobre la seguridad de la nación.

[687] Directiva de Defensa Nacional 2012: por una defensa necesaria, por una defensa responsable. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2012.pdf (21/12/2023).

[688] Directiva de Defensa Nacional 2020. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2020.pdf (21/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

permite al país defender sus intereses nacionales, cumplir con sus compromisos internacionales y contribuir a la paz y estabilidad internacional" (BALLESTEROS MARTÍN M. A., 2016, pág. 63), donde impera la visión preventiva y anticipativa frente al peligro.

Por otro lado, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional dispone en su artículo 3 que:

> "A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos".

Refleja esta definición una visión integral en la que encajan *las tres dimensiones de la seguridad nacional*: primeramente, la referida a las personas, sus derechos y libertades; en segundo lugar, la colectiva, representada por España como nación y los principios y valores constitucionales que se han dado todos los españoles para vivir en sociedad; y por último, la contribución al ideario mundial a través del compromiso con el Derecho Internacional y las obligaciones que conlleva. Quedan así cubiertas las necesidades tanto del Estado como de los ciudadanos por cuanto tienen cabida la defensa del territorio, la estabilidad económica, la protección de las infraestructuras críticas, la seguridad cooperativa y la confianza en las relaciones internacionales, así como las múltiples variables que conforman la seguridad humana. De la misma manera, esa acción del Estado está enfocada a la armonización de las normas que regulan las diferentes dimensiones de la seguridad, asignadas competencialmente a las distintas autoridades y Administraciones Públicas, como por ejemplo la protección de la seguridad ciudadana, la defensa nacional, la protección civil, la seguridad privada, la acción exterior o la protección de las infraestructuras críticas.

En tercer lugar, conviene que aclaremos qué entender por *crisis* en el contexto en que nos encontramos. Es éste un concepto que ha evolucionado hasta llegar hoy día a tener el sentido de situación comprometida y decisiva ante la que hay que tomar algún tipo de medida para restablecer el orden usual de las cosas, normalmente en un plazo más corto de lo deseado y, probablemente, con un acusado déficit de información sobre la que basar una decisión razonada de dicha entidad.

El diccionario de la Real Academia Española refiere en su primera acepción de *crisis* un "cambio profundo y de consecuencias importantes en un proceso o una situación, o en la manera en que estos son apreciados", y en la tercera se refiere a una "situación mala o difícil".

Es esta una definición genérica pero que apunta a cuestiones esenciales en una *crisis de seguridad,* que es la que nos compete aclarar, por cuanto se detalla la importancia de las consecuencias de la situación y de la percepción que de ella se tiene.

Aznar Fernández-Montesinos hace una aproximación al sentido de la palabra *crisis* con base en tres características principales: la amenaza que representa para valores

Ediciones Universidad de Salamanca | CC BY-NC-ND

compartidos de alta prioridad, la obligación de adoptar medidas aún a falta de información y la urgencia de los acontecimientos. Así, el autor considera que:

> "[…] las crisis amenazan valores de alta prioridad para la sociedad, el Estado o la Nación de modo que pueden afectar de forma grave a la vida o intereses de los ciudadanos, a la seguridad ciudadana, al sistema socioeconómico de la Nación o su independencia.
> Además, […] existe una carencia de información pese a la cual se deben de tomar igualmente decisiones.
> A esta circunstancia de carencia de información para la implementación de decisiones, la suele acompañar un ritmo rápido de los acontecimientos, junto con una sensación ficticia o real de escalada, lo que hace se perciba la necesidad de adoptar medidas inmediatamente" (AZNAR FERNÁNDEZ-MONTESINOS, 2024, pág. 110).

El concepto de crisis nos permite al mismo tiempo referirnos al de *resiliencia de una sociedad*, con la que se vincula íntimamente en la medida en que la crisis, como representación real o percibida de un riesgo, encarna un reto para el sistema y cuestiona su propia capacidad de adaptación y respuesta. En este sentido:

> "La resiliencia de una comunidad puede ser entendida como la capacidad de absorber la presión o las fuerzas destructivas a través de la resistencia o adaptación; la capacidad para gestionar o mantener ciertas funciones y estructuras básicas durante contingencias; y la capacidad de recuperación después de un evento" (AZNAR FERNÁNDEZ-MONTESINOS, 2024, pág. 109).

Consecuentemente, la *seguridad nacional* es un servicio público que requiere para su adecuada gestión una *política de Estado* en la que, en atención a la naturaleza de los intereses involucrados, debe estar comprometida como una sola persona toda la sociedad, con la idea de alcanzar altas cotas de *resiliencia* y fortalecer el apoyo ciudadano. De esta forma, la *Política de Seguridad Nacional* representa un objetivo compartido y, como tal, se responsabiliza de armonizar la actuación del ámbito público –a nivel estatal, autonómico y local-, del sector privado y la sociedad civil, para articular una respuesta ágil, eficaz y coherente frente a las *crisis*, asegurando "la constancia en lo necesario y la continuidad en lo fundamental, que es lo que caracteriza una verdadera política de Estado, como debe ser siempre la de seguridad"[689], clave de la defensa de los derechos y libertades ciudadanas y de los valores de una sociedad democrática.

Para llevar a efecto esta política de Estado es necesario planificar su implantación y definir sus líneas directrices, lo cual exige disponer de respaldo legal a través de un cuerpo normativo específico -la Ley de Seguridad Nacional de 2015-, arbitrar un conjunto coherente y ordenado de instituciones, métodos y procedimientos legales que den soporte a sus acciones –el Sistema de Seguridad Nacional con todos sus integrantes a distinto nivel-, definir y consensuar políticamente una estrategia para orientar y dirigir

[689] Debate del Proyecto de Ley de Seguridad Nacional. «BOCG. Congreso de los Diputados», serie A, número 158-1, de 29 de mayo de 2015. (Número de expediente 121/000158). Diario de Sesiones del Congreso de los Diputados, sesión plenaria núm. 278 (extraordinaria), de 8 de julio de 2015, página 29. Disponible en: https://www.congreso.es/public_oficiales/L10/CONG/DS/PL/DSCD-10-PL-296.PDF (21/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

toda esta actividad de respuesta coordinada frente a los nuevos desafíos –las distintas estrategias de seguridad nacional que desde el año 2011 hasta la última de 2021 se han ido sucediendo- (ZAMORA NAVARRO, 2016, págs. 16-17) y, en último lugar, contar con el compromiso colaborativo de todos los sectores involucrados y, principalmente, de los ciudadanos -fomentándolo a través de la *cultura de seguridad nacional*-.

4.3.1. La Ley de Seguridad Nacional de 2015

La Ley de Seguridad Nacional (en adelante LSN) del año 2015 representa la adaptación de la política de seguridad española a las condiciones reales y cambiantes de los desafíos que plantea el escenario internacional global, interdependiente y altamente tecnologizado. Así, esta norma ya considera la ciberseguridad y las crisis sanitarias como ámbitos de especial interés de la seguridad nacional, consolida la Estrategia de Seguridad Nacional como la base del esquema cooperativo y de complementariedad de políticas y actores para gestionar las crisis, diseña el Sistema de Seguridad Nacional como la estructura clave de coordinación y le otorga la posibilidad de acceder a unos recursos para garantizar su operatividad y, lo más importante, favorece la implicación activa de toda la sociedad en este enfoque integral de la seguridad como espacio colaborativo público-privado (GIRÓN TOMÁS, 2017, págs. 159-160).

De esta forma, protege los intereses nacionales categorizándolos como *vitales, fundamentales y estratégicos:*

> "Entre los primeros estarían: la soberanía nacional, la integridad territorial o el sistema constitucional. Entre los segundos están la libertad, o los que permiten la vida y el bienestar de los ciudadanos, como es la lucha contra las epidemias y pandemias como la del COVID-19. En la tercera categoría están los intereses estratégicos que contribuyen a la protección de los anteriores y favorecen el desarrollo de nuestro país. Entre estos están la estabilidad de las regiones de nuestro entorno como el Mediterráneo Occidental, el Sahel, las rutas de suministro energético o las zonas donde faenan nuestros pesqueros como es la cuenca somalí" (BALLESTEROS MARTÍN M. Á., 2020, págs. 12-13).

Tal y como se indicó anteriormente, el artículo 3 LSN liga con acierto en su definición los tres componentes de la seguridad nacional: la seguridad *individual* de las personas, la *colectiva* del Estado y la *global* de la comunidad internacional. Este carácter multifacético es esencial para poder entender el espíritu de la LSN, espacio común y compartido en el que concurren principios, procedimientos, instituciones y recursos cuya conjunción es garantía de seguridad, libertad, estabilidad y progreso.

Los principios que definen la Política de Seguridad Nacional, objetivo compartido por todos los actores y a todos los niveles[690], se recogen en el artículo 4 LSN y se basan en la unidad de acción de aquellos bajo la responsabilidad del Gobierno, la anticipación y la prevención en la visión estratégica, la eficiencia y sostenibilidad en el uso de los

[690] La Política de Seguridad Nacional afecta a las Administraciones estatal, autonómica y local, a los órganos constitucionales, con especial referencia al Gobierno de la Nación y las Cortes Generales, así como al sector privado y a la sociedad civil en su conjunto.

Ediciones Universidad de Salamanca | CC BY-NC-ND

recursos, la capacidad de resistencia y recuperación de las infraestructuras y las personas -la resiliencia-, la coordinación institucional y la colaboración ciudadana.

Conforme a estos principios, constituye una prioridad del Gobierno la promoción de una "cultura de seguridad nacional que favorezca la implicación activa de la sociedad en su preservación y garantía"[691], en la idea de que cuanto mayor conocimiento tengan los ciudadanos sobre las amenazas y desafíos que pueden afectar a su libertad, bienestar y derechos, mayor resiliencia tendrán para sobreponerse a las crisis de seguridad que deban afrontar.

Para concretar el modo y los medios a través de los que hacer realidad esta política, se presenta la *Estrategia de Seguridad Nacional* (ESN) como:

> "El marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes"[692].

Pieza primordial para el adecuado funcionamiento de este engranaje es la *cultura de seguridad nacional*, mediante la que alentar la corresponsabilidad de la sociedad en su conjunto que, desde luego, no debe dar por supuesta la democracia y sus libertades, sino que debe implicarse activamente en la defensa día a día de este marco de seguridad que puede verse comprometido por diferentes actores de distinta naturaleza animados por diversas motivaciones. De ahí la importancia de la LSN como pilar y de la ESN como instrumento mediante el que integrar la cooperación del Estado y las Comunidad Autónomas, la colaboración privada y la participación ciudadana.

Otro elemento clave que habla del aspecto avanzado de esta norma es la constitución de la *estructura colaborativa* del Sistema de Seguridad Nacional (SSN)[693], que es el conjunto de órganos, instituciones, autoridades, procedimientos y recursos de cualquier ámbito -estatal, autonómico, local- que, a través de la actividad coordinadora del Consejo de Seguridad Nacional (CSN), se organizan para compartir sus capacidades en orden a prevenir y, en su caso, gestionar la respuesta necesaria a los nuevos desafíos como el suministro de energía, la estabilidad económica y financiera, el control de los flujos migratorios irregulares, la emergencia climática, las crisis sanitarias y pandemias o el uso confiable del ciberespacio. Y son estos los objetivos que deben servir de guía

[691] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. BOE núm. 233, de 29 de septiembre de 2015. BOE-A-2015-10389. Artículo 5.1. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389 (21/12/2023).

[692] IBIDEM, artículo 4.3.

[693] El artículo 18 LSN dispone que: "1) El Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos, integrados en la estructura prevista en el artículo 20 de esta ley, que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones. 2) En el Sistema de Seguridad Nacional se integran los componentes fundamentales siguiendo los mecanismos de enlace y coordinación que determine el Consejo de Seguridad Nacional, actuando bajo sus propias estructuras y procedimientos. En función de las necesidades, podrán asignarse cometidos a otros organismos y entidades, de titularidad pública o privada".

Ediciones Universidad de Salamanca | CC BY-NC-ND

para la protección de los intereses nacionales a través de la redacción tanto de la ESN como de las estrategias de segundo y tercer nivel.

Por su parte, el artículo 17 LSN define el Consejo de Seguridad Nacional estableciendo que "en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, así como ejercer las funciones que se le atribuyan por esta ley y se le asignen por su reglamento".

El contexto de crisis que marca la activación de esta estructura del SSN y sus procedimientos de detección, respuesta y retorno a la normalidad se define a través de la *situación de interés para la seguridad nacional* en el artículo 23 LSN como "aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional", no pudiendo implicar en ningún caso la suspensión de derechos fundamentales o libertades públicas[694]. Estas normas y procedimientos de *gestión de crisis* que conforman el SSN deben ser en todo caso compatibles y homologables con los utilizados por las organizaciones internacionales de los que España es parte[695].

Lógicamente, toda vez que la seguridad nacional es transversal, el éxito de esta estrategia de respuesta global del Estado requiere de todas sus capacidades al completo, para lo cual es necesaria la afectación de recursos humanos y materiales, tanto públicos como privados, de carácter estatal, autonómico o local[696], con el objetivo de arbitrar un marco de prevención y respuesta que supere visiones compartimentadas y que defina una línea de acción integral y coordinada de todos los agentes e instrumentos en orden al superior interés de la seguridad nacional (MORET MILLÁS , 2017). A mayores, esta suma de recursos, competencias y voluntades se ha de identificar con el núcleo de principios que representa el *interés general de España* y que la propia CE protege: unidad, soberanía y lealtad en el modelo del Estado de las Autonomías (GONZÁLEZ HERNÁNDEZ, 2019, págs. 193-196).

[694] Artículo 23 LSN: "1) La gestión de crisis se desarrollará en la situación de interés para la Seguridad Nacional, adaptándose a las específicas circunstancias de la misma, de acuerdo con lo dispuesto en este título. 2) La situación de interés para la Seguridad Nacional es aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles, en los términos previstos en esta ley. 3) La situación de interés para la Seguridad Nacional se afrontará con los poderes y medios ordinarios de las distintas Administraciones Públicas y en ningún caso podrá implicar la suspensión de los derechos fundamentales y libertades públicas de los ciudadanos".

[695] La Disposición adicional segunda de la LSN estipula la coordinación con otros instrumentos internacionales de gestión de crisis, señalando que "las normas y procedimientos de gestión de crisis del Sistema de Seguridad Nacional deberán ser compatibles y homologables con los instrumentos de gestión de crisis de las organizaciones internacionales en las que España es parte".

[696] El artículo 28 LSN obliga al Gobierno, en coordinación con las Comunidades Autónomas, a elaborar un catálogo de recursos estratégicos para situaciones de crisis.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Dicho proceso se lleva a cabo bajo los principios de necesidad, proporcionalidad y contribución gradual conforme a la entidad de la crisis[697], habiéndose previsto al respecto la creación de un catálogo de recursos y medios materiales de los sectores estratégicos que puedan ser activados en caso de situación de interés para la seguridad nacional[698], para conocer las capacidades tecnológicas y científicas disponibles, evitar duplicidades, cubrir carencias y aprovechar los recursos de carácter transversal.

La definición de un *catálogo de recursos y medios estratégicos disponibles* es cuestión principal que requiere para su adecuada realización la colaboración entre los principales representantes políticos del país, por la transversalidad y alcance de sus efectos para el interés general. La complejidad de tan alta misión, unida a la descentralizada vertebración del Estado y la disparidad de gobiernos autonómicos, ha ralentizado el proyecto, no siendo que hasta abril de 2024, casi diez años después de la promulgación de la LSN, el Consejo de Seguridad Nacional acuerda la creación de un Grupo de Trabajo para el desarrollo de este Catálogo de Recursos de la Seguridad Nacional[699], marcando el plazo de un año para la presentación de un primer borrador que, sin duda, habrá de tener muy presentes las lecciones aprendidas en la gestión de la DANA que el 29 de octubre de ese mismo año afecta catastróficamente a la comarca de l´Horta Sud de Valencia[700].

Para esta relevante tarea, cuyo responsable es el CSN, se constituye un Grupo de Trabajo[701] *ad hoc* con dependencia directa del Comité de Situación, que asume el mandato de desarrollar un borrador de Catálogo de Recursos de la Seguridad Nacional *a nivel de la Administración General del Estado*, que habrá de ser informado favorablemente por el CSN. Una vez superada esa fase, el Consejo considerará un nuevo proceso para el desarrollo de un Catálogo de Recursos análogo *a nivel de Comunidades*

[697] El artículo 27 LSN regula la contribución gradual y proporcionada de recursos humanos y materiales para afrontar situaciones de crisis.

[698] El artículo 24 LSN define los requisitos para declarar una situación de interés para la Seguridad Nacional, incluyendo el uso de recursos del catálogo.

[699] Orden PJC/326/2024, de 14 de abril, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para el desarrollo del Catálogo de Recursos de la Seguridad Nacional. Publicada en BOE núm. 93, de 16/04/2024 (BOE-A-2024_7481). Disponible en: https://www.boe.es/eli/es/o/2024/04/14/pjc326/con (01/12/2024).

[700] Algunos de los municipios más afectados por la DANA son Algemesí, Catarroja, Xirivella, Paiporta, Alfafar, Aldaia, Benetússer, Massanassa, Sedaví o Albal, que conforman la denominada *zona 0* de la catástrofe. Disponible en: https://www.datadista.com/playa-burbuja/el-mapa-con-las-130-000-viviendas-afectadas-por-las-inundaciones-en-valencia/#:~:text=Entre%20ellos%20se%20encuentra%20la,y%20Massanassa%20(10.146%20habitantes) (01/12/2024).

[701] Este Grupo de Trabajo, presidido por la persona Directora del DSN, está integrado, como vocales, por los miembros designados por los titulares de los Ministerios de los vocales que designen los respectivos titulares del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, Ministerio de Defensa, Ministerio de Hacienda, Ministerio del Interior, Ministerio de Transportes y Movilidad Sostenible, Ministerio de Trabajo y Economía Social, Ministerio de Industria y Turismo, Ministerio de Agricultura, Pesca y Alimentación, Ministerio de Política Territorial y Memoria Democrática, Ministerio para la Transición Ecológica y el Reto Demográfico, Ministerio de Economía, Comercio y Empresa, Ministerio de Sanidad, Ministerio de Ciencia, Innovación y Universidades, Ministerio de Inclusión, Seguridad Social y Migraciones, Ministerio para la Transformación Digital y de la Función Pública, Secretaría de Estado de Comunicación y Centro Nacional de Inteligencia.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Autónomas. Finalmente, ambos registros se habrán de integrar para conformar el proyecto final de Catálogo de Recursos de Seguridad Nacional que, a propuesta del Presidente de la nación, será sometido a la aprobación del Gobierno mediante real decreto acordado en el Consejo de Ministros.

El principal objetivo de dicho Catálogo pasa por facilitar la disposición de los recursos existentes en territorio nacional para, en caso de crisis, tenerlos debidamente catalogados e identificados, planificar su adecuada movilización, evaluar su aplicabilidad al caso concreto y activarlos para su despliegue coordinado a través del procedimiento establecido en aras del bien común. Para cumplir con dicho objetivo, el Catálogo deberá incluir recursos humanos, materiales y financieros, así como el soporte de planimetría y el señalamiento de capacidades sectoriales específicas referidas, entre otras, al transporte, la energía, las telecomunicaciones, las obras públicas y la maquinaria civil. Lógicamente, para el éxito del proyecto será tan importante la integración de toda la información disponible como la identificación de las carencias para, en el marco de los escenarios que se diseñen, poder acordar instrumentos que permitan suplirlas.

Este es un claro ejemplo de cómo la estructura administrativa puede afectar a la propia acción de gobierno, por cuanto ningún Gobierno autonómico va a ser complaciente ni sumiso a la hora de poner una infraestructura crítica ubicada en su territorio a disposición del Gobierno central en una eventual situación de crisis que, por definición, también le va a afectar. El fondo no es otro que la lealtad institucional, la lucha de poderes -el central y los autonómicos-, y la disputa entre partidos políticos de muy diverso signo, no todos ellos alineados con los mismos valores e intereses que, en ocasiones, incluso discrepan en lo tocante al concepto de *nación* y lo que representa el *interés general de España*, al que explícitamente se refiere el artículo 155 CE como bien concreto que merece ser protegido (GONZÁLEZ HERNÁNDEZ, 2019, págs. 194-195).

En este sentido es relevante la reflexión del General Ballesteros, Director General del Departamento de Seguridad Nacional en el periodo 2018-2023, cuando se refiere a la evolución de nuestro SSN que, partiendo del modelo inglés, ha ido:

> "[…] adquiriendo su propia personalidad, adaptada a la estructura administrativa de nuestro país. Un país muy descentralizado que acerca la administración al ciudadano, pero que hace más compleja la gestión de las crisis donde una parte importante de los recursos están en manos de las comunidades autónomas" (BALLESTEROS MARTÍN M. Á., 2020, pág. 15).

Finalmente, destacar una vez más la acertada visión de la LSN al comprender la transversalidad y complejidad de la amenaza que actualmente puede atacar la seguridad nacional cuyo superior interés, basado en la consideración como objetivo esencial del mantenimiento de la libertad y los derechos ciudadanos bajo la forma del Estado social y democrático de derecho que ampara nuestra Constitución en su artículo 1.1, requiere un marco de colaboración y compromiso a todos los niveles que garantice la respuesta integral y coordinada de la amplia estructura de organismos, autoridades y recursos al servicio de ese interés común que es la seguridad nacional, y cuya pieza clave son los ciudadanos (Preámbulo de la Constitución Española).

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.3.2. El marco colaborativo del Sistema de Seguridad Nacional

El Sistema de Seguridad Nacional es la estructura colaborativa que permite a los órganos competentes en materia de seguridad nacional desempeñar sus funciones. Bajo la dirección del Presidente del Gobierno y asistido por el CSN, que es el responsable de articular los mecanismos de enlace y coordinación que en su seno correspondan, se integra por el Departamento de Seguridad Nacional y los Comités Especializados, en los cuales podrán integrarse los correspondientes representantes autonómicos, como se deriva de su composición[702].

En segundo lugar, forman parte del SSN los *componentes fundamentales de la seguridad nacional*[703], que son los organismos y entidades competentes en los ámbitos de la defensa nacional, la seguridad pública y la acción exterior que operan bajo sus propias estructuras y procedimientos conforme a las normas sectoriales específicas de cada uno de ellos. Estos componentes fundamentales, a su vez, están permanentemente apoyados por los Servicios de Inteligencia e Información del Estado[704] que, en el ámbito de sus respectivas competencias, aportan su conocimiento y capacidades para prevenir y dar respuesta a los riesgos y amenazas en el marco de la Seguridad Nacional[705].

En tercer lugar, en atención a la dimensión de las actuales amenazas, su transversalidad, la potencial gravedad de sus efectos y la complejidad de las acciones requeridas para contrarrestarlas, es inevitable superar la dimensión tradicional de los componentes fundamentales y que cobren relevancia los *ámbitos de especial interés de la seguridad nacional*, que son "aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales"[706]. En lista abierta la LSN enumera algunos de estos ámbitos de especial interés como la ciberseguridad, la

[702] Artículo 20 LSN.
[703] Artículo 18.2 LSN.
[704] En España, según manifiesta el Ministerio del Interior en su declaración de perfil de país ante el Comité de Expertos sobre Terrorismo "CODEXTER" del Consejo de Europa, en la "Reseña relativa a la capacidad antiterrorista de España" efectuada en la 24ª reunión, celebrada entre el 16 y 17 mayo de 2013 en Estrasburgo, páginas 8 y 9, "en virtud del RD 400/2012, las tareas relacionadas con la información y/o inteligencia y con la lucha antiterrorista, tanto de la Policía Nacional como de la Guardia Civil, las desempeñan sus respectivos Servicios de Información: 1) La Comisaría General de Información (Policía Nacional) se encarga de recabar, recibir, procesar y desarrollar la información de interés para mantener el orden y la seguridad pública dentro del ámbito de actuación de su Dirección General, así como de su aplicación o uso, especialmente en lo referente a la lucha contra el terrorismo. 2) El Servicio de Información (Guardia Civil) se encarga de organizar, dirigir y gestionar la recopilación, la recepción, el tratamiento, el análisis y la distribución de la información de interés para mantener el orden y la seguridad pública dentro del ámbito de actuación de su Dirección General, así como de su aplicación o uso, especialmente en lo referente a la lucha contra el terrorismo. 3) Estos servicios de inteligencia y/o información son, por lo tanto, órganos de gestión que dependen de las Fuerzas y Cuerpos de Seguridad del Estado, legalmente designados para luchar contra el terrorismo, tanto mediante la prevención como la represión. Todo ello sin perjuicio de las funciones asumidas, en esta materia, por el Centro Nacional de Inteligencia, dependiente del Ministerio de la Presidencia". Por ello, los Servicios de Inteligencia e Información del Estado son el Centro Nacional de Inteligencia, la Comisaría General de Información de la Policía Nacional y la Jefatura de Información de la Guardia Civil.
[705] Artículo 9 LSN.
[706] Artículo 10 LSN.

Ediciones Universidad de Salamanca | CC BY-NC-ND

seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente. Por ello, para completar el marco colaborativo del SSN, se obliga a las Administraciones Públicas competentes en estos ámbitos de especial interés a coordinarse y compartir la información[707] que permita la gestión anticipativa de los riesgos y amenazas, así como asegurar la disponibilidad de los servicios esenciales y el suministro de los recursos básicos y estratégicos -energía, agua, alimentación, productos sanitarios y médicos, entre otros-.

Como puede observarse, la gestión integral de la seguridad implica coordinar a múltiples sectores de la nación relacionados con el tejido productivo, investigativo, académico, científico, económico, o social, lo que conlleva que las funciones que tiene que desempeñar el SSN[708] adopten una triple dimensión: primeramente de evaluación de los factores y situaciones que pueden afectar a la seguridad nacional, en segundo lugar de recopilación y análisis de información de apoyo a la toma de decisiones para dirigir la respuesta conjunta ante situaciones de crisis y, finalmente, de detección de necesidades y propuesta de medidas de coordinación para garantizar la disponibilidad y funcionamiento de los recursos asignados para llevar a cabo sus funciones con éxito. Por ello, es elemento primordial del SSN la capacidad para integrar, en tiempo real, la información relevante proveniente de distintos orígenes y en diferentes formatos, para facilitar al Presidente del Gobierno la toma de decisiones en situaciones de crisis, así como la gestión anticipativa de los riesgos y amenazas para identificar su escalada y adoptar las medidas preventivas antes de que se materialicen en un ataque contra la seguridad nacional (BALLESTEROS MARTÍN M. Á., 2020, págs. 12-15).

El CSN, como estructura base del SSN en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, asiste al Presidente del Gobierno en la dirección de dicha Política mediante su planificación y coordinación, dirige la actuación de la gestión de crisis en el marco del SSN, verifica el cumplimiento de la ESN e impulsa la elaboración de estrategias de segundo nivel, organiza la contribución de recursos a la estructura de seguridad nacional, acuerda la creación de los órganos de apoyo necesarios para el desempeño de sus funciones –Comités Especializados- y aprueba el Informe Anual de Seguridad Nacional[709], entre otras[710].

En cuanto a su composición[711], más allá del Presidente, Vicepresidentes y Ministros del Gobierno, merece ser destacada la presencia permanente de la persona que ostente la Dirección del Departamento de Seguridad Nacional[712] y la discrecional, en función de los

[707] Artículo 11 LSN.
[708] Artículo 19 LSN.
[709] El Informe Anual de Seguridad Nacional es aprobado por el Consejo de Seguridad Nacional antes de su presentación a las Cortes Generales y supone un fiel análisis de la realidad de la amenaza a la seguridad nacional en la que se presenta, en un ejercicio de transparencia democrática, los factores de riesgo que se han materializado, su nivel de afectación y la respuesta que se ha construido para su desactivación. Se realizan desde el año 2013. Disponibles en: https://www.dsn.gob.es/es/estrategias-publicaciones/informe-anual-seguridad-nacional (16/12/2023).
[710] Artículo 21.1 LSN.
[711] Artículo 21.3 LSN.
[712] Artículo 21.4 LSN.

Ediciones Universidad de Salamanca | CC BY-NC-ND

asuntos a tratar, de "los titulares de los demás departamentos ministeriales y las autoridades autonómicas afectadas en la toma de decisiones y actuaciones a desarrollar por parte del Consejo"[713], así como de "aquellas personas físicas o jurídicas cuya contribución se considere relevante a la vista de los asuntos a tratar en el orden del día"[714], claro exponente de la filosofía de corresponsabilidad e implicación social en la prevención y garantía de la seguridad nacional[715].

El CSN, en el ejercicio de sus funciones, adopta en 2017 el Acuerdo de implementación de los mecanismos de enlace y coordinación del conjunto de las Administraciones Públicas para garantizar el funcionamiento integrado del SSN[716], tanto con carácter habitual como en casos de gestión de crisis, en una triple vertiente: los mecanismos de enlace y coordinación de los componentes fundamentales de la seguridad nacional, los mecanismos de coordinación e intercambio de información de los ámbitos de especial interés que sean competencia de las Administraciones Públicas, y los mecanismos de enlace y coordinación necesarios para que el SSN se active preventivamente en los supuestos de gestión de crisis.

Estos mecanismos se conciben, por un lado, como puntos focales ministeriales con funciones concretas de apoyo y, por otro, como procedimientos ágiles que garanticen el funcionamiento integrado y flexible del SSN en cualquier escenario. Para ello se designa al Departamento de Seguridad Nacional como centro receptor de estos mecanismos de enlace y coordinación permanente con los puntos de contacto ministeriales y organismos públicos, y como soporte de los procedimientos de conexión del SSN con los órganos competentes de la seguridad nacional para recibir información de manera permanente, poder tomar las decisiones pertinentes y extender su radio de acción a los ámbitos de la sociedad que se consideren necesarios.

Para coordinar la respuesta del SSN en relación con los distintos escenarios de gestión de crisis que haya de afrontar se distinguen tres clases de mecanismos:

1. Mecanismos de enlace y coordinación permanente[717].

[713] Artículo 21.5 LSN.
[714] Artículo 21.7 LSN.
[715] Esta es la clave de la Cultura de Seguridad Nacional que recoge el artículo 5 LSN, para favorecer la sensibilización de la sociedad en cuanto a los requerimientos de la seguridad nacional, los riesgos y amenazas que pueden comprometerla, el esfuerzo que para salvaguardarla hacen los organismos públicos y privados concernidos y, como tarea compartida por todos, la implicación activa y responsable de la sociedad en su mantenimiento y defensa.
[716] Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional. BOE 38, martes 14 de febrero de 2017. Disponible en: https://www.boe.es/boe/dias/2017/02/14/pdfs/BOE-A-2017-1460.pdf (16/12/2023).
[717] Red de puntos de contacto compuesta por los Directores de Gabinete de los ministerios y organismos públicos pertenecientes al Consejo de Seguridad Nacional, bajo la coordinación del Departamento de Seguridad Nacional. Asimismo, estarán apoyados permanentemente por los respectivos centros de crisis de carácter ministerial y de otros organismos públicos dependientes. Recogido en el apartado cuarto a) del Anexo del Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del SSN.

Ediciones Universidad de Salamanca | CC BY-NC-ND

2. Mecanismos de enlace y coordinación reforzada[718]
3. Y coordinación del conjunto de los mecanismos de enlace y coordinación[719].

4.3.3. El Departamento de Seguridad Nacional

Como heredero y sustituto del Departamento de Infraestructura y Seguimiento de Situaciones de Crisis (DISSC), se crea en el año 2012 el Departamento de Seguridad Nacional (DSN)[720] siguiendo la propuesta que hace la Estrategia Española de Seguridad de 2011 de crear un equipo multidisciplinar como "órgano instrumental y estructura de asistencia a la Presidencia del Gobierno para la coordinación y liderazgo en esta materia, soporte en la gestión de crisis y seguimiento de esta Estrategia"[721]. A fecha de hoy, los ámbitos de actuación del DSN vienen determinados por los diecisiete tipos de riesgos y amenazas catalogados por la vigente Estrategia de Seguridad Nacional de 2021.

Ubicado en el conocido como *búnker de la Moncloa* y dependiente del Gabinete de la Presidencia del Gobierno[722], el DSN asume la función de secretaría técnica y órgano de trabajo permanente del CSN encargado del asesoramiento y apoyo técnico al Presidente del Gobierno en materia de seguridad nacional, entre cuyas funciones se encuentran las de llevar a cabo el seguimiento de los riesgos, amenazas y situaciones de crisis nacionales e internacionales, analizar los posibles escenarios de su desarrollo y posible evolución, diseñar en coordinación con los órganos competentes los planes de contingencia que respondan a cada una de estas situaciones, contribuir a la elaboración de propuestas normativas y de fomento de la colaboración privada y la participación ciudadana, así como la elaboración, implantación y revisión de las estrategias en el ámbito de la seguridad nacional[723].

En cuanto a su estructura, la encabeza quien ostente la Dirección del DSN, con las funciones de dirección del Departamento, la toma de decisiones en el ámbito interno,

[718] Red de puntos de contacto que refuerza a los de coordinación permanente con la incorporación de representantes de los demás ministerios y organismos públicos y entidades de derecho público vinculados o dependientes de la Administración General del Estado no representados habitualmente en el Consejo de Seguridad Nacional, cuando así lo exijan las circunstancias que afecten a la Seguridad Nacional, incluidos los sectores de la sociedad civil cuya colaboración se requiera, de acuerdo con lo dispuesto en el artículo 7 de la Ley de Seguridad Nacional. Recogido en el apartado cuarto b) del Anexo del Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del SSN.

[719] El Departamento de Seguridad Nacional efectuará la coordinación del conjunto de los mecanismos de enlace y coordinación del Sistema de Seguridad Nacional de conformidad con lo dispuesto en el artículo 20.4 de la Ley de Seguridad Nacional, y con lo establecido en su regulación orgánica específica y en el Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del SSN. Recogido en el apartado cuarto c) del Anexo de dicho Acuerdo.

[720] El DSN se crea por el Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. Publicado en el BOE-A-2012-9816. Disponible en: https://www.boe.es/eli/es/rd/2012/07/20/1119 (16/12/2023).

[721] Estrategia Española de Seguridad: Una responsabilidad de todos. Capítulo 5. Año 2011. Disponible en: https://www.lamoncloa.gob.es/documents/9BED-CF7A-estrategiaespanoladeseguridad.pdf (16/12/2023).

[722] Artículo 3.2 del Real Decreto 890/2023, de 27 de noviembre, por el que se aprueba la estructura de la Presidencia del Gobierno.

[723] Disponible en: https://www.dsn.gob.es/es/sistema-seguridad-nacional/departamento-seguridad-nacional (16/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la secretaría técnica del Comité de Situación, la vicepresidencia de los Consejos de segundo nivel y Comités Especializados, y la presidencia de las Comisiones Permanentes de Ciberseguridad y Contra las Campañas de Desinformación. De la Dirección del DSN dependen la Oficina de Comunicación y Relaciones Institucionales, responsable de la política de comunicación y difusión del Departamento, de los contactos institucionales ajenos y de la proyección hacia el exterior de actividades y contenidos, y la Asesoría Jurídica, encargada del análisis jurídico de todo tipo de iniciativas, decisiones y proyectos relacionados con la Seguridad Nacional o cuya consulta proceda por guardar relación con esta.

En un nivel inmediatamente inferior se encuentra la Dirección Operativa, responsable de la gestión diaria del Departamento, del personal, los medios y sistemas, de la que depende la Secretaría, Documentación y Subregistro y el Centro de Comunicaciones, con las funciones de seguimiento y control de la entrada y salida de información de interés para el DSN, tanto ordinaria como clasificada[724].

A igual nivel entre sí y dependientes de la Dirección Operativa, se encuentran las siguientes Unidades:

1. Unidad de Protección, adscrita funcionalmente al DSN pero con dependencia orgánica de la Dirección General de la Guardia Civil, con la misión de protección y seguridad física de las instalaciones 24/7.
2. Unidad de Seguimiento y Alerta, con las funciones de seguimiento permanente de la actualidad nacional e internacional con especial incidencia en la seguridad nacional, la monitorización en tiempo real de las distintas fuentes reconocidas y oficiales, tanto públicas como privadas, y la elaboración de informes diarios de seguimiento.
3. Unidad de Gestión de Crisis y Ejercicios, responsable de la activación del SSN ante una situación de crisis, concretamente del Comité de Situación y las Células de Coordinación que procedan por la naturaleza de la amenaza. También se encarga esta Unidad de la organización de ejercicios de gestión de crisis a nivel nacional para poner a prueba las capacidades del SSN, y de la participación en ejercicios europeos, internacionales o de estructuras aliadas –OTAN- para entrenar la respuesta coordinada de gestión de crisis.
4. Unidad de Planeamiento Político-Estratégico, encargada de la elaboración de la Estrategia de Seguridad Nacional y de las Estrategias de segundo nivel. Desde esta Unidad se llevan a cabo también los Informes Anuales de Seguridad Nacional.
5. Unidad de Análisis de Seguridad Nacional, con las funciones de elaboración de análisis estratégicos por áreas de interés, principalmente orientados a las crisis o acontecimientos con incidencia en la Seguridad Nacional. Estos análisis incluyen posibles escenarios e indicadores de evaluación, y proyectan la previsión de desenlace prevista para conocimiento de Presidencia del Gobierno.

[724] El búnker donde se ubica el DSN en un edificio acreditado por la Oficina Nacional de Seguridad para el uso y manejo de todo tipo de información clasificada, incluyendo la catalogada como "secreta", por lo que todas las personas que trabajan en el mismo cuentan con la máxima acreditación de seguridad.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Desde esta Unidad se impulsa también todo lo relativo a la estrategia de Cultura de Seguridad Nacional.

6. Unidad de Ciberseguridad y Desinformación, responsable de aglutinar y coordinar a los distintos actores nacionales en el ámbito de la ciberseguridad, que debido al modelo de gobernanza español presenta una gran dispersión. Por ello, esta Unidad ejerce como punto de contacto nacional ante la UE en dicha materia. Idéntica labor de coordinación e integración de visiones se lleva a cabo en cuanto a las campañas de desinformación con afectación a la seguridad nacional, ocupándose esta Unidad de la gestión de los Foros de Ciberseguridad y Desinformación para impulsar la colaboración público privada.
7. Unidad de Sistemas e Infraestructura, con tres áreas específicas de Infraestructuras, Informática y Comunicaciones, encargadas de la gestión, la innovación y el mantenimiento del *búnker* y sus sistemas de comunicación, audio, video y redes. También gestiona las comunicaciones especiales de Presidencia del Gobierno.
8. Unidad de Apoyo y Secretaría Técnica con las funciones de apoyo a la Dirección, la gestión documental y de las salas de reuniones e instalaciones de trabajo del Departamento. Además, ejerce las tareas propias de apoyo a las Secretarías Técnicas del CSN y de los Comités Especializados que recaen en el DSN.

Mediante esta estructura el DSN lleva a cabo las funciones de secretariado técnico en los órganos interministeriales de apoyo al Consejo de Seguridad Nacional[725], y las derivadas de asumir la responsabilidad del adecuado funcionamiento del Comité de Situación del DSN que, bajo la presidencia de la persona que ostente la vicepresidencia primera del Gobierno[726], coadyuva a la mejor coordinación entre las distintas Administraciones Públicas y asesora al CSN para favorecer el seguimiento y la gestión de crisis, procurando la rapidez en la toma de decisiones a nivel político-estratégico y la flexibilidad en la respuesta a estas situaciones.

En relación con el impulso de la cultura y la concienciación de seguridad por parte de los ciudadanos como prioridad dentro de la Política de Seguridad Nacional, conforme a lo recogido en el artículo 5 LSN, y en el contexto legal de la aprobación del Plan Integral de Cultura de Seguridad Nacional[727] y la creación del Foro Integral de Seguimiento y Evaluación de la Cultura de Seguridad Nacional[728], el DSN ejerce las funciones de órgano

[725] Estos órganos interministeriales de apoyo al Consejo de Seguridad Nacional son el Consejo Nacional de Ciberseguridad (2013), el Consejo Nacional de Seguridad Marítima (2013), el Comité de Situación para la gestión de crisis (2013), el Comité Especializado de Inmigración (2014), el Comité Especializado de No Proliferación (2017), el Comité Especializado de Seguridad Energética (2017), el Comité Especializado contra el Terrorismo (2020), el Consejo Nacional de Seguridad Aeroespacial (2020) y el Comité Especializado contra el Crimen Organizado y la Delincuencia Grave (2024).

[726] Actualmente, conforme al Real Decreto 1230/2023, de 29 de diciembre, por el que se modifica el Real Decreto 829/2023, de 20 de noviembre, por el que se reestructuran los departamentos ministeriales, corresponde al Ministerio de la Presidencia, Justicia y Relaciones con las Cortes.

[727] Orden PCM/575/2021, de 8 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 25 de mayo de 2021, por el que se aprueba el Plan Integral de Cultura de Seguridad Nacional. BOE número 138 de 10 de junio de 2021. Disponible en: https://www.boe.es/boe/dias/2021/06/10/pdfs/BOE-A-2021-9631.pdf (18/12/2023).

[728] Orden PCM/1051/2022, de 1 de noviembre, por la que se publica el Acuerdo del Consejo de Ministros de 31 de mayo de 2022, por el que se crea el Foro Integral de Seguimiento y Evaluación de la Cultura de

Ediciones Universidad de Salamanca | CC BY-NC-ND

de trabajo permanente del Plan y de secretaría técnica de los órganos y grupos de trabajo que se constituyan para acometerlo. También se encarga de la presidencia del citado Foro Integral de Seguimiento y Evaluación, en cuyo seno se podrán crear grupos de trabajo para realizar estudios y propuestas sobre materias específicas. En ambos casos, el objetivo principal no es otro que «aumentar la concienciación social sobre el carácter imprescindible de la Seguridad Nacional, y de la corresponsabilidad de todos en las medidas de anticipación, prevención, análisis, reacción, resistencia y recuperación respecto a los desafíos, riesgos y amenazas»[729].

Con esta misma filosofía el DSN ha puesto en marcha otras iniciativas para impulsar en la ciudadanía un conocimiento amplio e informado del entorno de seguridad y las amenazas principales que se ciernen sobre nuestra vida cotidiana a través de su propia página web[730], en la que de forma amigable y actualizada se comparten contenidos, noticias, normativa, eventos y otras cuestiones relacionadas que, además, son apoyadas desde sus cuentas oficiales de *X* e Instagram[731] para, a través de ellas, lanzar mensajes dirigidos a los distintos perfiles de la población y fomentar su implicación en la defensa de la seguridad nacional como *algo de todos*.

En el marco del SSN y de la función de coordinación de iniciativas de colaboración público privada lideradas por el DSN, orientadas a contribuir a un mejor entendimiento de los nuevos riesgos y potenciar la cultura de seguridad, en 2020 se constituyó un grupo de trabajo integrado por más de 50 expertos de la Administración Pública y la sociedad civil –periodistas, académicos y comunicadores-, que culminó en septiembre de 2022 con la publicación del libro titulado *Lucha contra las campañas de desinformación en el ámbito de la Seguridad Nacional. Propuestas de la sociedad civil*. La buena acogida de las ponencias de este trabajo hizo ver la conveniencia de crear un espacio de debate permanente para poder llevar a cabo el seguimiento y la evaluación de la cambiante realidad de esta amenaza, lo que motivó la aprobación por el Consejo de Ministros[732] en mayo de 2022 del Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional, cuyos primeros resultados se presentaron el 12 de diciembre de ese mismo año bajo el título *Trabajos 2023*, a través de siete capítulos que abordan el

Seguridad Nacional y se regula su composición y funcionamiento. BOE número 264 de 3 de noviembre de 2022. Disponible en: https://www.boe.es/boe/dias/2022/11/03/pdfs/BOE-A-2022-18088.pdf (18/12(2023).

[729] El mensaje principal del Plan Integral de Cultura de Seguridad Nacional es que una sociedad concienciada y comprometida con su protección es más segura y resiliente. Para su desarrollo se establecen cuatro ámbitos de actuación: la formación para generar conocimiento y cultura crítica de seguridad; la divulgación y comunicación pública a través de los medios y las plataformas de comunicación; la relevancia en el exterior para transmitir una imagen positiva de España como país seguro y comprometido con la paz internacional; y la participación de la ciudadanía y las organizaciones de la sociedad civil en las actividades de fomento de la cultura de seguridad nacional.

[730] Disponible en: www.dsn.gob.es/es (18/12(2023).

[731] @dsn y dsn_es respectivamente.

[732] Orden PCM/541/2022, de 10 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 31 de mayo de 2022, por el que se crea el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional y se regula su composición y funcionamiento. BOE número 142 de 15 de junio de 2022. Disponible en: https://www.boe.es/boe/dias/2022/06/15/pdfs/BOE-A-2022-9965.pdf (19/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

fenómeno de las campañas de desinformación y las narrativas manipuladoras[733], así como posibles formas de instrumentalizar la respuesta desde el respeto a los principios democráticos y, siempre, desde el prisma de la necesaria conexión entre opinión pública y democracia como base de la participación ciudadana (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 44).

También compete al DSN mantener el sistema de comunicaciones especiales de la Presidencia del Gobierno, una malla de comunicaciones seguras de vital importancia en situaciones de crisis, por cuanto:

> "[…] su gestión implica el desarrollo y aplicación de un conjunto ordinario de actuaciones dirigidas a detectar y valorar los riesgos y amenazas concretos para la seguridad nacional, facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios" (AREN, SANZ, & CAMPOS, 2020, pág. 9).

En este proceso cobra especial relevancia la red de puntos de contactos ministeriales del DSN para el intercambio en tiempo real de información y su valoración por el Comité de Situación, auxiliado por una célula de coordinación creada al efecto e integrada por un representante de cada ministerio y organismo representado en el mismo, pudiendo incorporarse a la misma los especialistas que se consideren oportunos en función de la naturaleza de la crisis a gestionar.

En definitiva, el DSN es un organismo asesor, consultivo y de carácter estratégico, que tiene como principal objetivo asesorar al Gabinete de la Presidencia del Gobierno y al titular mismo de la Presidencia en los procesos de toma de decisiones que tengan implicación con riesgos y amenazas para la Seguridad Nacional, a través de los mecanismos, Consejos y Comités que forman parte del SSN.

4.3.4. Los Comités Especializados

Teniendo como referencia los ámbitos de especial interés de la seguridad nacional, como por ejemplo la ciberseguridad, la seguridad marítima, la seguridad aeroespacial o la seguridad energética, que requieren una atención específica por su relevancia de cara a preservar los derechos y libertades de los ciudadanos y para garantizar el suministro

[733] Los siete capítulos de "Trabajos 2023" se refieren a: 1) Metodología y buenas prácticas para la detección y verificación de la desinformación y para la respuesta en el plano de la comunicación; 2)Estudio de la desinformación rusa a nivel internacional; 3) Efectos psicológicos, radicalización y amplificación de los conflictos sociales causados por la injerencia y manipulación extranjera de la información: análisis y prevención; 4) Mapa de las capacidades de investigación en materia de desinformación en las Universidades y Centros de Investigación españoles; 5) Técnicas, metodologías y prospectiva IA para combatir la desinformación; 6) Técnicas y metodologías de ciberinteligencia para la investigación de operaciones de información y guerra cognitiva; 7) Las actuaciones de las plataformas de Internet en materia de desinformación. Del código de buenas prácticas al Reglamento de servicios digitales. Disponible en: https://es.scribd.com/document/694443774/Foro-Campanas-Desinfo-GT-2023-Accesible (20/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de los servicios esenciales, se crean los Comités Especializados como órganos técnicos de apoyo al CSN[734].

Los Comités Especializados ayudan al CSN en su cometido de dirigir e impulsar la respuesta de gestión de crisis, así como en el resto de sus funciones de coordinación y asistencia al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional y del SSN, reforzando de esta manera el enfoque multinivel y cooperativo de las distintas autoridades y Administraciones Públicas que, en el ámbito de sus competencias, integran la estructura del SSN para dar una respuesta armónica e integral a los riesgos y amenazas a la seguridad nacional, con primordial atención a los ámbitos de especial interés de la seguridad nacional.

1. El Comité de Situación

El Comité de Situación es el mecanismo de gestión de crisis por excelencia del SSN, de carácter único dentro de su estructura, conformado como un órgano colegiado de apoyo al CSN que fue creado por Acuerdo de 5 de diciembre de 2013[735] y que cuenta con el soporte del DSN y su estructura para el desempeño de sus funciones, principalmente en lo relativo a la alerta temprana y el seguimiento de las situaciones de gestión de crisis, el aseguramiento de la agilidad en el proceso de adopción de decisiones político estratégicas, y la garantía de interconexión de los mecanismos y sistemas del SSN.

Su carácter único para el conjunto del SSN le confiere la responsabilidad de coordinar el apoyo requerido por el Gobierno en los estados de alarma y excepción, así como la de valorar la amenaza, analizar los escenarios de crisis y evaluar los resultados con el apoyo del resto de Comités Especializados, además de centralizar la información que suministren las autoridades y organismos competentes en los supuestos de interés para la seguridad nacional.

La presidencia y máxima representación del Comité corresponde a la persona que ocupe el Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática[736],

[734] Aunque los nueve Comités ayudan al CSN en sus funciones, el Comité de Situación es el que ocupa un lugar prioritario y de carácter único como órgano colegiado de apoyo, mientras que los tres referidos a los espacios comunes globales -ciberespacio, espacio marítimo, y espacio aéreo y ultraterrestre- reciben la denominación de Consejo Nacional en vez de Comité Especializado, denominación que queda para aquellos cuatro vinculados a amenazas como la inmigración, la dependencia energética, la proliferación de armas de destrucción masiva, el terrorismo o el crimen organizado.

[735] En ese mismo Acuerdo del CSN también se aprueba la Estrategia de Ciberseguridad Nacional y la de Seguridad Marítima conforme a lo establecido en la Estrategia de Seguridad Nacional de 2013. Este Comité se crea con la denominación de Comité Especializado de Situación, título que cambia a Comité de Situación con la Orden PRA/32/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Comité Especializado de Situación. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-798.pdf (19/12/2023).

[736] Conforme a la Orden PCM/1396/2021, de 13 de diciembre, por la que se publica el Acuerdo de 18 de noviembre de 2021, del Consejo de Seguridad Nacional, por el que se modifica el de 1 de diciembre de 2017, por el que se regula el Comité de Situación. Dado que ese departamento ministerial es sustituido por el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes conforme al Real Decreto 1230/2023, de 29 de diciembre, por el que se modifica el Real Decreto 829/2023, de 20 de noviembre,

Ediciones Universidad de Salamanca | CC BY-NC-ND

siendo la vicepresidencia ocupada por el Director del Gabinete de la Presidencia del Gobierno y Secretario del CSN. Como vocales uno de cada departamento ministerial y organismo público con representación en el CSN, pudiendo ser requeridos los de los demás en función de los asuntos a tratar. Igualmente, con este criterio temático y funcional, se puede convocar a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante, así como los titulares de la red de puntos de contacto de seguridad nacional. Por su parte, el DSN funciona como secretaría técnica y órgano de trabajo permanente del Comité, además de como órgano de apoyo en la realización de alerta temprana y seguimiento de situaciones de gestión de crisis. Para el adecuado desempeño de sus funciones cuenta con la ayuda del Centro de Situación del DSN, que además será el responsable de garantizar su interconexión con los demás centros de crisis existentes en la red del SSN.

Entre las funciones del Comité de Situación caben destacar por su relevancia las de verificar el cumplimiento de las medidas adoptadas en materia de gestión de crisis por el CSN, promover la colaboración internacional en situaciones de crisis, facilitar la activación anticipada de los instrumentos preventivos de gestión de crisis conforme a las directrices del CSN, elevar planes de contingencia, recomendaciones y propuestas, organizar y fomentar el empleo adecuado de los medios y recursos disponibles[737], y el reforzamiento de la resiliencia nacional a través de la propuesta de objetivos y la coordinación de los planes de implementación para alcanzarlos[738].

También conviene destacar que el Comité puede crear grupos de trabajo técnicos, que serán coordinados por el DSN, con la composición, cometidos y objetivos que estime necesarios, para que le den soporte en el desempeño de sus funciones.

Como ya hemos visto, en la actualidad *ninguna crisis es unidireccional debido a que los desafíos que las provocan tienen un marcado carácter multidimensional* que, más tarde o más temprano, acaban implicando a diferentes actores y espacios competenciales cuya acción debe ser coordinada para conseguir articular una sola respuesta efectiva y adaptada al caso concreto. Y es aquí donde radica la importancia del trabajo del Comité de Situación, que es convocado en situaciones de crisis, preferiblemente de forma

por el que se reestructuran los departamentos ministeriales, entendemos que se adecua la composición del Comité de Situación a la actual organización ministerial.

[737] Apartado quinto de la Orden PRA/32/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Comité Especializado de Situación.

[738] La justificación de esta modificación es la necesidad de reforzar la resiliencia nacional, la cual requiere un enfoque de aproximación integral -de la administración y de la sociedad- para garantizar la continuidad de la acción de gobierno y de prestación de los servicios esenciales en caso de gestión de crisis. Para ello se constituye el Grupo Permanente de Coordinación de la Resiliencia Nacional. Orden PCM/714/2022, de 23 de julio, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 21 de junio de 2022, por el que se modifica el de 1 de diciembre de 2017, por el que se regula el Comité de Situación. BOE núm. 180, de 28 de julio de 2022. BOE-A-2022-12585. Disponible en: https://www.boe.es/eli/es/o/2022/07/23/pcm714 (21/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

anticipada, cuando los indicadores de Seguridad Nacional muestran una tendencia que así lo aconseje.

De esta forma, para responder a la pandemia del COVID-19, se convocó al Comité de Situación en numerosas ocasiones y se acordó la constitución diaria de una Célula de Coordinación (CelCor), a un nivel técnico inferior al de Director General, que involucrara a todos los departamentos ministeriales implicados, al objeto de que el DSN pudiera tener conocimiento en tiempo real y procesar la información de interés para apoyar la toma de decisiones del Gobierno. Se trataba no sólo de una crisis sanitaria sino que, también, implicaba un grave problema de seguridad pública, con afectación a la situación económica internacional y efectos no deseados en la opinión y la confianza ciudadana respecto a las instituciones del Estado por la profusión de narrativas desinformadoras en torno a las medidas adoptadas para su gestión y los instrumentos articulados para llevarlas a efecto.

En este mismo sentido, en el contexto de la invasión rusa de Ucrania acaecida el 24 febrero de 2022, dos o tres semanas antes de esta fecha ya existían indicadores que señalaban el alto nivel de tensión en la zona y se barajaba como escenario posible la guerra de agresión de Rusia que, indefectiblemente, tendría una afectación a la seguridad nacional española, por lo que a través del Comité de Situación se decidió la convocación diaria de la CelCor para el seguimiento de los hechos, implicando a los departamentos ministeriales afectados que, por la naturaleza de la crisis, fueron prácticamente todos.

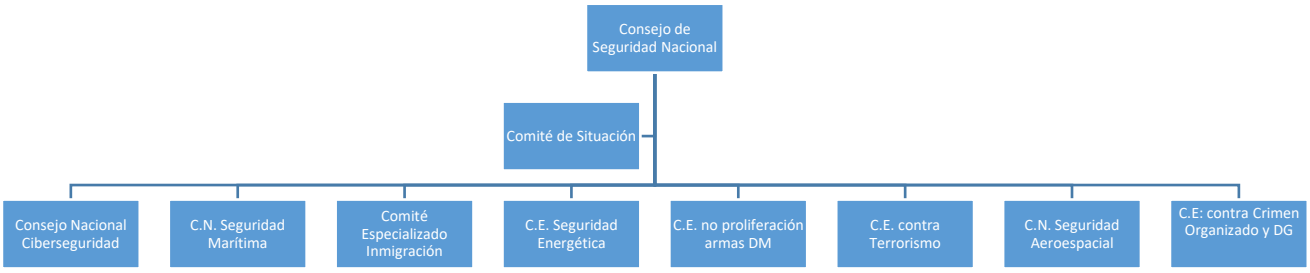


Gráfico 4.1.
Comités Especializados de apoyo al Consejo de Seguridad Nacional
Fuente: propia

En estas reuniones cada departamento ministerial actualiza la afectación temática desde su punto de vista, en base a su ámbito de actividad y el tipo de crisis de que se trate, al tiempo que se ponen en común los indicadores transversales que definan la situación. Esta CelCor y el correspondiente informe asociado, dirigido al Presidente del Gobierno, se mantiene vigente e incluye en su temática la afectación a la seguridad nacional en tanto en cuanto continúen activas amenazas como las derivadas de la guerra en Ucrania y del conflicto más reciente entre Israel y Hamás.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Podemos por todo ello concluir que lo más característico del Comité de Situación es que no se trata de un Comité Especializado por la temática, como todos los demás, sino que se activa únicamente en situaciones de crisis, sean estas del tipo que sean y siempre y cuando tengan afectación a la seguridad nacional. De él dependerán las Células de Coordinación que, en el contexto de las circunstancias concretas, se creen para gestionar dichos escenarios de crisis.

2. El Consejo Nacional de Ciberseguridad

El Consejo Nacional de Ciberseguridad es un órgano de apoyo al CSN aprobado por Acuerdo de 5 de diciembre de 2013 en el marco de la primera Estrategia de Ciberseguridad Nacional[739], para dar respuesta a la necesidad de contar con una estructura orgánica precisa que, a través de una actuación conjunta y adecuada a los principios que sustentan el SSN, atienda a la visión integral de la ciberseguridad que plantea la referida Estrategia y a la que la LSN considera un ámbito de especial interés para la seguridad nacional. De esta manera, la ciberseguridad se conceptualiza desde un enfoque holista que inicia en el Estado y, pasando por su propia estructura institucional, llega hasta los ciudadanos y las empresas, proyectándose de manera transversal en el sistema normativo y las políticas públicas, superando el ámbito nacional para integrarse a través del principio de cooperación en la estrategia defensiva de la Unión Europea en el ciberespacio (ÁLVAREZ ROBLES, 2024, pág. 270)

En lo relativo a su composición, la presidencia y máxima representación del Consejo es ejercida por la persona titular de la Dirección del Centro Nacional de Inteligencia, mientras que la vicepresidencia corresponde a la Dirección del DSN. El criterio para las vocalías es el mismo utilizado para el Comité de Situación, asignando una de cada departamento ministerial y organismo público con representación en el CSN, pudiendo ser citados otros en función de los asuntos a tratar. De la misma manera, se puede reclamar a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante. También el DSN asume aquí las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

Entre las funciones del Consejo Nacional de Ciberseguridad sobresalen las de proponer al CSN las directrices de la Política de Seguridad Nacional relacionadas con la ciberseguridad, contribuir a la elaboración de propuestas normativas y emitir informes, verificar el cumplimiento de la ESN y proponer su revisión en el marco de la ciberseguridad, analizar y proponer iniciativas de carácter nacional e internacional que

[739] Este Comité se contempla en el Capítulo 5 de la Estrategia de Ciberseguridad Nacional con la denominación de Comité Especializado de Ciberseguridad, título que cambia a Consejo Nacional de Ciberseguridad por la Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-799-consolidado.pdf (21/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

coadyuven a la toma de decisiones del CSN en materia de ciberseguridad, reforzar las relaciones con las Administraciones Públicas y las de coordinación y colaboración entre los sectores público y privado, y la valoración de riesgos y amenazas ante los posibles escenarios de crisis, con especial atención a los que pudieran derivar en una situación de interés para la seguridad nacional desde el punto de vista de la ciberseguridad. También se le otorgan competencias al Consejo Nacional de Ciberseguridad para asesorarse mediante la creación de grupos de trabajo integrados por expertos en la materia correspondiente, coordinados por el DSN.

En cuanto a la estructura operacional de la ciberseguridad en el SSN, el Consejo Nacional de Ciberseguridad cuenta con una Comisión Permanente de Ciberseguridad coordinada por el DSN en la que concurren el Ministerio de Defensa con el Estado Mayor de la Defensa (EMAD), representado con el Mando Conjunto del Ciberespacio (MCCE), y el Centro Nacional de Inteligencia (CNI), representado por el Centro Criptológico Nacional (CCN); el Ministerio del Interior con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y la Oficina de Coordinación de Ciberseguridad (OCC); y el Ministerio para la Transformación Digital y de la Función Pública a través del Instituto Nacional de Ciberseguridad de España (INCIBE) y la Secretaría de Estado de Digitalización e Inteligencia Artificial[740].

En 2020 se constituye el Foro Nacional de Ciberseguridad con el objetivo de impulsar la cultura de ciberseguridad tanto de empresas como de ciudadanos, promover la formación y el talento en competencias relacionadas con el ciberespacio, ofrecer apoyo a la industria española e impulsar la investigación, el desarrollo y la innovación como base de la soberanía digital.

3. El Consejo Nacional de Seguridad Marítima

El Consejo Nacional de Seguridad Marítima es un órgano de apoyo al CSN aprobado por Acuerdo de 5 de diciembre de 2013 en el marco de la primera Estrategia de Seguridad Marítima Nacional[741], que desarrolla las previsiones de la ESN 2013 y las adapta al medio marino como espacio ambivalente de difícil control y gran relevancia estratégica[742], la

[740] Conforme a la estructura de departamentos ministeriales publicada en el Real Decreto 1230/2023, de 29 de diciembre, por el que se modifica el Real Decreto 829/2023, de 20 de noviembre, por el que se reestructuran los departamentos ministeriales.

[741] Este Comité se contempla en el Capítulo 4 de la Estrategia de Seguridad Marítima Nacional de 2013 con la denominación de Comité Especializado de Seguridad Marítima, título que cambia a Consejo Nacional de Seguridad Marítima por la Orden PRA/34/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Seguridad Marítima. BOE número 20, de fecha 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-800.pdf (26/12/2023).

[742] Claro ejemplo de esta relevancia estratégica es la situación generada en diciembre de 2023 en el tráfico marítimo a través del Mar Rojo como consecuencia del conflicto en la Franja de Gaza que, a tenor de los acontecimientos, se convierte cada vez más en un conflicto de Oriente Medio y que impulsa a EE.UU. a liderar la coalición naval de la Operación Guardián de la Prosperidad, a la que finalmente se suma la UE a través de la Operación Atalanta, para neutralizar los ataques de los rebeldes hutíes y dar seguridad en el golfo de Adén, restaurando el Canal de Suez como puerta de entrada y salida de mercancías entre Asia y Europa. Amplio seguimiento en prensa internacional. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

cual es posteriormente relevada por la Estrategia Nacional de Seguridad Marítima 2024[743].

En lo relativo a su composición, la presidencia y máxima representación del Consejo es ejercida por el Jefe del Estado Mayor de la Defensa, mientras que la vicepresidencia corresponde al Director del DSN. Se asigna un vocal por cada departamento ministerial y organismo público con representación en el CSN y, además, uno del Ministerio de Agricultura y Pesca, Alimentación y Medio Ambiente, pudiendo ser emplazados otros en función de los asuntos a tratar. De la misma manera, se puede convocar a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante. El DSN asume las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

Como funciones del Consejo Nacional de Seguridad Marítima señalar las de proponer al CSN las directrices de la Política de Seguridad Nacional relacionadas con la seguridad marítima, contribuir en este ámbito a la elaboración de propuestas normativas, emitir informes técnicos, verificar el cumplimiento de la ESN y proponer su revisión, apoyar la toma de decisiones del CSN en materias propias de la seguridad marítima, así como reforzar las relaciones con las Administraciones Públicas concernidas y las de coordinación y colaboración entre los sectores público y privado, y la valoración de riesgos y amenazas ante los posibles escenarios de crisis, con especial atención a los que pudieran derivar en una situación de interés para la seguridad nacional desde el punto de vista de la seguridad, en coordinación con el Comité Especializado de Situación. También se le otorgan competencias al Consejo Nacional de Seguridad Marítima para asesorarse mediante la creación de grupos de trabajo integrados por expertos en la materia correspondiente, coordinados por el DSN.

4. El Comité Especializado de Inmigración

El Comité Especializado de Inmigración es un órgano de apoyo al CSN aprobado por Acuerdo de 10 de julio de 2014, modificado y actualizado por la Orden PRA/31/2018, de 22 de enero[744] para atender el carácter esencialmente transversal de la ordenación de

https://www.europapress.es/internacional/noticia-ue-une-operacion-guardian-prosperidad-mar-rojo-traves-operacion-atalanta-20231221085757.html
https://www.abc.es/economia/ataques-mar-rojo-disparan-precios-transporte-asia-20240103185433-nt.html
https://www.bbc.com/mundo/articles/c0ky0r0k01eo (03/01/2024).

[743] Orden PJC/501/2024, de 27 de mayo, por la que se publica la Estrategia Nacional de Seguridad Marítima 2024, aprobada por el Consejo de Seguridad Nacional. BOE número 130, de 29 de mayo de 2024 (BOE-A-2024-10762). Disponible en: https://www.boe.es/eli/es/o/2024/05/27/pjc501 (03/01/2024).

[744] La Orden PRA/31/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Comité Especializado de Inmigración, modifica el Acuerdo original de 2014 en lo relacionado con su naturaleza jurídica, las funciones, la composición -presidencia y procedimiento de designación de sus miembros- y otras previsiones como la emisión de informes, la creación de grupos de trabajo y el reforzamiento del enlace y coordinación con los componentes fundamentales y ámbitos de especial interés para la Seguridad Nacional dentro del marco del Sistema de

Ediciones Universidad de Salamanca | CC BY-NC-ND

flujos migratorios y, con ello, reforzar la coordinación de los componentes fundamentales y ámbitos de especial interés para la seguridad nacional dentro del esquema de funcionamiento del SSN.

Su presidencia corresponde a la persona que ejerza la titularidad de la Secretaría de Estado de Seguridad y la vicepresidencia a la Dirección del DSN. Además, se compone de un vocal por cada departamento ministerial y organismo público con representación en el CSN junto con otro del Ministerio de Empleo y Seguridad Social, pudiendo ser emplazados terceros en función de los asuntos a tratar. De la misma manera, se puede requerir a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante. Como en todos los Comités Especializados, el DSN asume las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

En cuanto a sus funciones, junto a las propias de todo Comité Especializado, cabe destacar por su relevancia la de ayudar a organizar la contribución de recursos a la seguridad nacional en el ámbito de la ordenación de flujos migratorios, cuyas crisis generan, a la par que graves consecuencias humanitarias, situaciones de tensión para el adecuado control del paso de fronteras nacionales y, por ende, de la UE.

Lógicamente, el Comité Especializado de Inmigración tiene competencia para asesorarse mediante la creación de grupos de trabajo integrados por expertos en la materia, coordinados por el DSN.

5. El Comité Especializado de Seguridad Energética

El Comité Especializado de Seguridad Energética es un órgano de apoyo al CSN regulado por Acuerdo de 1 de diciembre de 2017 y publicado por la Orden PRA/30/2018, de 22 de enero[745], en el marco de lo establecido por la Estrategia de Seguridad Energética Nacional de 2015 que califica como prioridad absoluta la salvaguarda de los intereses energéticos como base para poder proteger el resto de intereses vitales que ocupan un lugar central en la seguridad nacional, como la seguridad económica y financiera o la seguridad ambiental, y que, en su capítulo quinto, recoge la existencia de este Comité como instrumento para incardinar en el ámbito funcional del SSN la seguridad energética, planificando las actuaciones necesarias para su preservación a través de los objetivos marcados por el Gobierno.

Seguridad Nacional. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-797.pdf (26/12/2023).

[745] Orden PRA/30/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se crea y regula el Comité Especializado de Seguridad Energética. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-796.pdf (27/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Entre sus funciones, destacar las relativas al fomento de las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en el ámbito de la seguridad energética, así como entre los sectores público y privado, además de las correspondientes a la valoración de riesgos y amenazas en el marco del análisis de posibles escenarios de crisis energética susceptibles de derivar en una situación de interés para la seguridad nacional.

En lo relativo a su composición, la presidencia corresponde al Secretario de Estado de Energía y la vicepresidencia al Director del DSN. Se asigna un vocal por cada departamento ministerial y organismo público con representación en el CSN, pudiendo ser convocados otros en función de los asuntos a tratar. De la misma manera, se puede emplazar a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante. El DSN asume las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

Finalmente, el Comité Especializado de Seguridad Energética puede asesorarse mediante la creación de grupos de trabajo integrados por expertos en la materia, coordinados por el DSN.

6. El Comité Especializado de no proliferación de armas de destrucción masiva

Este Comité Especializado es un órgano de apoyo al CSN regulado por Acuerdo de 1 de diciembre de 2017 y publicado por la Orden PRA/29/2018, de 22 de enero[746], con el que se pretende coordinar y unificar los criterios de actuación de todos los grupos y comisiones interministeriales en el ámbito de la no proliferación para optimizar recursos, racionalizar estructuras y adecuar a los principios rectores de la Política de Seguridad Nacional el trabajo de todos los actores interesados, máxime cuanto la lucha contra la proliferación de armas de destrucción masiva en cada uno de sus campos -nuclear, radiológico, biológico y químico- es una materia de gran transversalidad y estrecha conexión con el terrorismo, el crimen organizado y la defensa nacional, que exigen un tratamiento integral desde la perspectiva de la seguridad nacional.

En cuanto a su composición, la presidencia es ejercida por la persona que desempeñe el cargo de Secretario de Estado de Asuntos Exteriores y la vicepresidencia es ocupada por la Dirección del DSN. Las vocalías se corresponden con cada departamento ministerial y organismo público con representación en el CSN, pudiendo ser llamadas otras personas asistentes en función de los asuntos a tratar. De la misma manera, se puede convocar a los titulares de los órganos superiores y directivos de la Administración General del

[746] Orden PRA/29/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se crea y regula el Comité Especializado de no proliferación de armas de destrucción masiva. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-795.pdf (27/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante. El DSN asume las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

Respecto a las funciones del Comité Especializado de no proliferación de armas de destrucción masiva, destacar sobre las generales de los Comités Especializados las referentes al apoyo al CSN mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional, junto con la valoración de riesgos y amenazas ante posibles escenarios de crisis susceptibles de derivar en una situación de interés para la seguridad nacional en el ámbito de la no proliferación de armas y evaluar los resultados de su ejecución, en coordinación con los órganos y autoridades directamente competentes y con el Comité Especializado de Situación. Estas dos funciones del Comité Especializado cobran especial relevancia en el contexto próximo de guerra en Ucrania, conflicto abierto en territorio europeo al que están llegando miles de armas de todo tipo que, entre el fragor de la contienda y auspiciado por las redes de crimen organizado, consiguen vías de salida del país hacia mercados alternativos que rentabilizan su bajo coste de adquisición inyectándolas en la órbita delincuencial ordinaria de los países europeos[747].

En el ejercicio de estas funciones, este Comité Especializado consideró la necesidad de proponer al CSN la elaboración de una Estrategia Nacional contra la proliferación de armas de destrucción masiva, como base para el desarrollo de las líneas concretas de acción frente a los riesgos de proliferación nuclear, radiológica, química y biológica en el ámbito nacional e internacional. Esta propuesta se materializó en el Acuerdo del Consejo de Seguridad Nacional para la elaboración de dicha Estrategia, de marzo de 2023[748], que a fecha de hoy continua su proceso de redacción.

Como todos los Comités Especializados, el de no proliferación también tiene la facultad para asesorarse mediante la creación de grupos de trabajo integrados por expertos en la materia correspondiente, coordinados por el DSN. Como ejemplo de ello, en enero de 2019 se presenta por el CSN el Plan Nacional de Biocustodia[749] con el que se establece un procedimiento de control efectivo sobre los agentes biológicos relevantes en cuanto

[747] En este sentido hay informes de carácter restringido de Europol que analizan el impacto de la guerra de agresión rusa contra Ucrania en la delincuencia y el terrorismo en Europa, que ponen en evidencia el elevado riesgo de que dicho conflicto acabe siendo una fuente de armas de fuego ilegales de contrabando para la delincuencia organizada en la UE. Tampoco los analistas de prensa son ajenos a esta realidad. Baste citar como ejemplos la perspectiva norteamericana del Washington Post y del Financial Times. Disponibles en: https://www.washingtonpost.com/national-security/2022/05/14/ukraine-weapons-trafficking/
https://www.ft.com/content/bce78c78-b899-4dd2-b3a0-69d789b8aee8 (29/12/2023).

[748] Orden PCM/207/2023, de 2 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para la elaboración de la Estrategia Nacional contra la Proliferación de Armas de Destrucción Masiva. BOE núm. 54, de 4 de marzo de 2023. Referencia BOE-A-2023-5702. Disponible en: https://www.boe.es/eli/es/o/2023/03/02/pcm207 (29/12/2023).

[749] Orden PCI/168/2019, de 22 de febrero, por la que se publica el Plan Nacional de Biocustodia, aprobado por el Consejo de Seguridad Nacional. BOE número 47 de 23 de febrero de 2019. Disponible en: https://www.boe.es/boe/dias/2019/02/23/pdfs/BOE-A-2019-2553.pdf (27/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

a su acceso, manipulación, comercialización y transporte, al tiempo que se crea la Comisión Nacional de Biocustodia encargada del seguimiento de dicho Plan Nacional.

7. El Comité Especializado contra el Terrorismo

El Comité Especializado contra el Terrorismo es un órgano de apoyo al CSN regulado por Acuerdo de 4 de marzo de 2020 y publicado por la Orden PCM/219/2020, de 13 de marzo[750], a través del que se articula la respuesta, con un enfoque holista y en el marco del SSN y de la ESN 2017, al terrorismo y a los extremismos violentos, identificados como amenazas graves para la Seguridad Nacional y el ordenamiento democrático, por su afectación a los valores y principios esenciales que rigen la convivencia en un Estado de Derecho, como son la libertad, los derechos fundamentales, la seguridad y el bienestar de los ciudadanos.

Su presidencia es ejercida por quien ostenta la titularidad de la Secretaría de Estado de Seguridad, en acción coordinada con el desempeño de la misma función en el Comité Especializado de Inmigración. La vicepresidencia corresponde al Director del DSN. En lo relativo a su composición, dada la especificidad técnica de la materia, el Comité está integrado por las personas que dirigen el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), la Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad (DGCE), la Comisaría General de Información de la Policía Nacional (CGI), la Jefatura de Información de la Guardia Civil (JIGC), así como un vocal del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (MAEC), del Ministerio de Justicia, del Ministerio de Defensa, del Centro Nacional de Inteligencia (CNI) y de la Secretaría de Estado de Comunicación.

Puede requerirse la presencia de un representante del resto de los departamentos ministeriales y organismos públicos en función de los asuntos a tratar. De igual forma, se puede convocar a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante. Como en todos los Comités Especializados, el DSN asume las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

En cuanto a las funciones del Comité Especializado contra el Terrorismo, la principal es la de proporcionar apoyo al CSN para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la lucha contra el terrorismo y los extremismos

[750] Orden PCM/219/2020, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se crea y regula el Comité Especializado contra el Terrorismo, en desarrollo de lo previsto en el Capítulo 5 de la Estrategia Nacional contra el Terrorismo 2019, en el que se establece "la creación de un Comité Especializado que aborde el terrorismo y los extremismos violentos" en apoyo al CSN para el cumplimiento de su función asesora al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito referido. BOE número 66 de 14 de marzo de 2020. Disponible en: https://www.boe.es/boe/dias/2020/03/14/pdfs/BOE-A-2020-3639.pdf (28/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

violentos. Además, reforzará las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en la materia, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo desde el enfoque político-estratégico. También es muy relevante la tarea de impulsar las actuaciones transversales de lucha contra la radicalización violenta y la definición de la estrategia contra las narrativas terroristas, así como la de apoyo al Comité de Situación ante escenarios susceptibles de derivar en una situación de interés para la Seguridad Nacional.

En último lugar señalar que también el Comité Especializado Contra el Terrorismo puede asesorarse técnicamente mediante la creación de grupos de trabajo integrados por expertos en la materia, coordinados por el DSN.

8. El Consejo Nacional de Seguridad Aeroespacial

El Consejo Nacional de Seguridad Aeroespacial es un órgano de apoyo al CSN regulado por Acuerdo de 4 de marzo de 2020 y publicado por la Orden PCM/218/2020, de 13 de marzo[751], que se crea para reforzar dentro del SSN la respuesta de seguridad coordinada frente a las amenazas que surgen en el ámbito aeroespacial -sector estratégico y elemento vertebrador del Estado- caracterizadas por su velocidad de cambio, su elevado componente tecnológico y el alto nivel de interconectividad que, en conjunto, determinan la necesidad de estipular procesos reactivos ágiles con estructuras de decisión en tiempo real apoyadas en sistemas de mando y control de alta disponibilidad, capaces, fiables y coordinados, tanto a nivel nacional como internacional.

Respecto a su composición, la presidencia y máxima representación del Consejo es ejercida por el Jefe del Estado Mayor de la Defensa, y la vicepresidencia corresponde al Director del DSN. Se asigna un vocal por cada departamento ministerial y organismo público con representación en el CSN, pudiendo ser emplazados otros en función de los asuntos a tratar. De la misma manera, se puede convocar a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante. El DSN asume las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

El Consejo Nacional de Seguridad Aeroespacial tiene encomendada, entre otras, la función de apoyo al CSN en su labor de asesoramiento al Presidente del Gobierno en la

[751] Orden PCM/218/2020, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se crea y regula el Consejo Nacional de Seguridad Aeroespacial, para dar cumplimiento a lo establecido en el Capítulo 4 de la Estrategia de Seguridad Aeroespacial Nacional de 2019, que dispone la creación de un Consejo Nacional de Seguridad Aeroespacial para dar apoyo al CSN en su labor de asistencia al Presidente del Gobierno en lo que en dicho ámbito afecte a la Política de Seguridad Nacional. BOE número 66 de 14 de marzo de 2020. Disponible en: https://www.boe.es/boe/dias/2020/03/14/pdfs/BOE-A-2020-3638.pdf (28/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

dirección y coordinación de la política de Seguridad Nacional en el ámbito de la seguridad aeroespacial, así como el fomento de las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, así como la gestión, con el soporte del DSN, de las situaciones de crisis del ámbito aeroespacial que, por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales, en especial de aquellas susceptibles de derivar en una situación de interés para la Seguridad Nacional.

El Consejo puede crear grupos de trabajo técnicos, que serán coordinados por el DSN, con la composición, cometidos y objetivos que estime necesarios, para que le den soporte en el desempeño de sus funciones.

9. El Comité Especializado contra el Crimen Organizado y la Delincuencia Grave

El Comité Especializado contra el Crimen Organizado y la Delincuencia Grave es el más reciente de los órganos de apoyo al CSN, publicado por la Orden PCJ/1290/2024, de 13 de noviembre[752], mediante el que se pretende acometer cuestiones transversales de naturaleza político-estratégica en este ámbito, aprovechando el Acuerdo de marzo de 2024 de aprobación de una nueva Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave debido a su necesaria adaptación al nuevo contexto criminal de este tipo de amenaza[753], que pone de manifiesto el paralelismo cada vez más evidente entre la delincuencia organizada y el terrorismo. En este sentido podemos referir la alerta de nuestro vecino, Francia, ante la grave amenaza que este tipo de actividades suponen para la seguridad interior del Estado, que lleva a los ministros franceses de Interior y Justicia a presentar en noviembre de 2024 un plan de lucha contra el tráfico de estupefacientes y la delincuencia organizada, basado en el reforzamiento del papel de los servicios de información e inteligencia y la especialización policial, asi como la creación de una célula de coordinación nacional para valorar el estado real de la amenaza como primer paso para establecer una estrategia al respecto[754].

Respecto a la composición de nuestro recién creado Comité Especializado contra el Crimen Organizado y la Delincuencia Grave, la presidencia y máxima representación es ejercida por la persona titular de la Secretaría de Estado de Seguridad, mientras que la

[752] Orden PCJ/1290/2024, de 13 de noviembre, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se crea y regula el Comité Especializado contra el Crimen Organizado y la Delincuencia Grave. BOE número 278, de 18 de noviembre de 2024 (BOE-A-2024-23946). Disponible en: https://www.boe.es/eli/es/o/2024/11/13/pjc1290/dof/spa/pdf (24/11/2024).

[753] El CSN acuerda en marzo de 2024 la citada revisión en la Orden PJC/327/2024, de 14 de abril, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba una nueva Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. BOE núm. 93, de martes 16 de abril de 2024. Disponible en: https://www.boe.es/boe/dias/2024/04/16/pdfs/BOE-A-2024-7482.pdf (24/11/2024).

[754] La prensa se hace eco de los violentos enfrentamientos entre distintos grupos delincuencias en el sur de Francia y la alerta generada en las autoridades galas, que acometen como respuesta una reorganización del sistema judicial y policial en lo referido a la lucha contra el crimen organizado. Disponible en: https://elpais.com/internacional/2024-11-08/francia-declara-la-guerra-al-narcotrafico-con-un-plan-especial-para-reducir-la-criminalidad.html
https://www.rfi.fr/es/francia/20241108-gobierno-franc%C3%A9s-anuncia-un-plan-de-lucha-para-combatir-el-narcotr%C3%A1fico (25/11/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

vicepresidencia corresponde a la Dirección del DSN. Por la especialización de la materia, las vocalías se conforman por las personas titulares de la Dirección del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, de la Comisaría General de Policía Judicial de la Policía Nacional (CGPJ), de la Jefatura de Policía Judicial de la Guardia Civil (JPJGC), así como un vocal del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (MAEC), del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, del Ministerio de Defensa, del Ministerio de Hacienda, del Ministerio de Transportes y Movilidad Sostenible, del Ministerio de Economía, Comercio y Empresa, del Centro Nacional de Inteligencia (CNI) y de la Secretaría de Estado de Comunicación. Puede requerirse la presencia de un representante del resto de los departamentos ministeriales y organismos públicos en función de los asuntos a tratar. De igual forma, se puede convocar a los titulares de los órganos superiores y directivos de la Administración General del Estado, de las Comunidades Autónomas y de la Administración Local, entidades y organismos públicos, del sector privado y expertos particulares cuya contribución se considere relevante o necesaria. Como en todos los Comités Especializados, el DSN asume las funciones de secretaría técnica y órgano de trabajo permanente del Consejo, además de las propias referidas a su carácter de punto de enlace único con el CSN en el ámbito de sus funciones.

Entre las funciones de este Comité Especializado se encuentran las de proponer al CSN las directrices de la Política de Seguridad Nacional relacionadas con la lucha contra el crimen organizado y la delincuencia grave, contribuir al adecuado funcionamiento del SSN en este ámbito, verificar el grado de cumplimiento de la ESN respecto a esta especialidad delincuencial y en su caso proponer su revisión, así como la elaboración de los planes estratégicos de desarrollo, apoyar la toma de decisiones del CSN aportando todo tipo de iniciativas de carácter nacional e internacional, reforzar las relaciones con las Administraciones Públicas así como asumir la coordinación y colaboración entre los sectores público y privado, apoyar al Comité de Situación ante escenarios que puedan derivar en una situación de interés para la SN y, finalmente, aprobar sus propias normas de funcionamiento y régimen interno.

Para finalizar, señalar que el Comité Especializado Contra el Crimen Organizado y la Delincuencia Grave puede asesorarse técnicamente mediante la creación de grupos de trabajo integrados por expertos en la materia, coordinados por el DSN.

4.3.5. Conclusiones sobre el Sistema de Seguridad Nacional

El Sistema de Seguridad Nacional, ha sido diseñado como una estructura colaborativa dirigida por el Presidente del Gobierno que cohesiona la acción de todos los órganos competentes en materia de seguridad nacional y garantiza su adecuada respuesta con carácter habitual y, específicamente, en casos de gestión de crisis, para lo cual se articula en torno a diferentes niveles, a saber:

1. Nivel político: en el cual se encuentra el Consejo de Seguridad Nacional. En este nivel cabe detenerse en la importancia de contar con un órgano altamente cualificado y bien comunicado, como es el DSN, para llevar a cabo sus funciones de manera ágil y conveniente.

Ediciones Universidad de Salamanca | CC BY-NC-ND

2. Nivel estratégico: está representado por el Comité de Situación que, también, cuenta con el soporte del DSN, elemento de coordinación primordial entre estos dos niveles.
3. Nivel operacional: corresponde a los Comités Especializados en cada una de los ámbitos de especial interés de la seguridad nacional.
4. Nivel técnico: ocupado por los organismos e instituciones públicas y privadas con la competencia y las capacidades de desempeño en las distintas materias que, en conjunto, conforman el amplio espectro de actividades con afectación a la seguridad nacional.

Sin embargo, aún quedan asuntos pendientes por resolver, como por ejemplo la definición del *Catálogo de Recursos de la Seguridad Nacional.* Esto conlleva la concreción y el acuerdo sobre qué recursos formarán parte del mismo, qué medios materiales de los sectores estratégicos ubicados por todo el país podrá activar el Estado en caso de situación de interés para la seguridad nacional, qué elementos técnicos facilitarán su integración y con qué autonomía podrá el decisor, en última instancia, involucrar recursos y comprometer costes teniendo presente la evidente complejidad de la estructura administrativa de nuestro país, muy descentralizada, que conlleva que dichos recursos se encuentren en el ámbito de gestión de las comunidades autónomas. Este complicado equilibrio de poder resulta patente en la gestión organizativa de la peor catástrofe sufrida por España en su historia reciente, la DANA del 29 de octubre de 2024 sobre Valencia, que hace aflorar esa falta de coordinación y de información esencial sobre los recursos disponibles en una gran crisis, cuya consecución se viene demandando desde el fin de la pandemia del COVID en el año 2020.

Otro desafío al que nos enfrentamos, también derivado de la descentralización y de la propia estructura de seguridad española que implica a actores en los tres niveles de la Administración junto con los del ámbito privado, es *la gestión de la información y el acceso al dato* para la posterior elaboración de inteligencia y la toma de decisiones estratégicas eficaces y en tiempo oportuno, donde el criterio de la *necesidad de conocer* o, aún mejor, el de la *necesidad de compartir*, se diluye entre los numerosos órganos de coordinación que, a cuenta de cumplir con su tarea, acaban generando cuellos de botella y disfunciones entre los órganos con competencias operativas aplicadas a la verdadera gestión de la seguridad, es decir, la que afecta a la protección de las personas y sus derechos.

Por otra parte, es evidente que la gestión integral de la seguridad implica necesariamente la coordinación de múltiples actores de la Administración Pública y, al mismo tiempo, de otros sectores de la industria, la economía, la investigación o la academia, por lo que cada vez cobra más significado disponer de sistemas de inteligencia y comunicación técnicamente avanzados que, en este sistema de gobernanza y de manera segura, permitan la gestión de información multidisciplinar, en cualquier tipo de formato y en tiempo real, para discriminar aquella que pueda resultar de interés de aquella otra que solo *genera ruido* y poder compartirla con los interesados para, por un lado, tomar decisiones de forma ágil y acertada y, por otra, operativizarla en tiempo oportuno para neutralizar la amenaza.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En definitiva, son estas cuestiones las que habrá que ir resolviendo de una u otra manera para conseguir dotar de mayor efectividad al SSN en el cumplimiento de sus funciones. Sin duda se trata de retos que necesitan de una amplia voluntad de acuerdo, que debe gestarse sobre la base del consenso sobre los mismos principios que han permitido a España llegar a constituirse en referencia internacional por su nivel de seguridad y su compromiso con el desarrollo de una sociedad moderna, democrática y justa. Y la propia evolución de la amenaza exige que esta voluntad de acuerdo se mantenga activa en el tiempo para articular la permanente adaptación al cambio, al margen de intereses políticos. Después de todo, se trata de una *política de Estado*.

4.4. El desarrollo del modelo de Estrategia de Seguridad Nacional como elemento integrador y de consenso frente a la amenaza

Como hemos explicado previamente, la seguridad nacional es cuestión que afecta a todos los ámbitos de actuación del Estado y compromete a múltiples actores de distinta naturaleza, tanto pública como privada, de la esfera nacional e internacional. Es por ello que su organización precisa de una estructura metodológica propia con un enfoque integral que favorezca la consecución de su objetivo principal, que no es otro que garantizar la mejor respuesta posible frente a los riesgos y amenazas con afectación a los intereses nacionales.

Ante la variedad de aproximaciones al concepto de *estrategia de seguridad nacional*, nos decantamos por dos de ellas que, por su carácter completo y ajuste a la realidad española, merecen ser destacadas.

La primera de ellas la ofrece Félix Arteaga, considerando que:

> "[…] las estrategias son documentos programáticos que sirven para integrar la respuesta de los Estados a problemas que afectan seriamente al bienestar, seguridad y futuro de las sociedades y poblaciones. Sirven para poner en marcha políticas y mecanismos de gestión de crisis en situaciones complejas que se desarrollan en varios niveles locales, nacionales, europeos e internacionales, en las que intervienen administraciones públicas y sectores privados y que precisan decisiones urgentes, por lo que requieren una planificación anticipada, estratégica, de los problemas que pueden presentarse y de las respuestas que deben ofrecerse" (ARTEAGA MARTÍN, 2011).

Esta definición nos proporciona elementos de juicio muy útiles para poder estudiar este tipo de documentos: la identificación de los principales peligros que pueden afectar a la seguridad de nuestra sociedad, el contexto nacional e internacional en que se desarrollan, los objetivos que se persiguen, los medios de que se dispone y la forma en que se debe articular la respuesta.

La segunda acepción que destacamos es la del General Ballesteros, según la cual:

> "Estrategia de seguridad nacional es el arte mediante el que la política general dirige, orienta y coordina todas las energías y fuerzas de la nación, para proteger los intereses nacionales contra riesgos, peligros, amenazas exteriores e interiores,

Ediciones Universidad de Salamanca | CC BY-NC-ND

> a la vez que permite al país cumplir con sus compromisos internacionales" (BALLESTEROS MARTÍN M. A., 2016, pág. 65).

En ella destacan los mismos elementos componentes que en la definición de Félix Arteaga: el interés nacional como fin último, la catalogación de los riesgos y amenazas tanto internos como externos que pueden afectarle, los fines de la estrategia, los modos de procurar la respuesta y los medios para llevarlos a cabo.

En esta línea, el DSN estima que la *estrategia de seguridad nacional* es el marco de referencia para la política de Seguridad Nacional, que parte de una concepción amplia de ésta, delimitando el marco conceptual en el que dar cabida a las distintas estrategias de seguridad españolas que, desde el año 2011, se han ido sucediendo a partir de la identificación de la necesidad de disponer de una estrategia capaz de hacer frente a la amenaza asimétrica que, a partir de los atentados terroristas del 11-S, se presenta como un nuevo factor estresante del equilibrio internacional que demuestra que:

> "[…] un actor no estatal sin apenas medios, podría llegar a causar miles de víctimas en una sola acción, convirtiéndose en la principal amenaza, pero una amenaza sin territorio, sin capacidades conocidas y sobre todo difícil de disuadir mediante represalias" (BALLESTEROS MARTÍN M. A., 2016, pág. 216).

Por ello, la *estrategia de seguridad nacional* debe ser un documento que aglutine las distintas visiones políticas de la realidad del país, que cohesione a la sociedad, que favorezca la solidaridad territorial y que, sobre la base de los valores y principios democráticos que conforman el núcleo del acuerdo de convivencia que garantiza la Constitución, represente la vía estipulada para alcanzar los intereses nacionales.

Es durante la IX legislatura cuando nuestro país redacta su primera estrategia de seguridad nacional, la cual surge del compromiso manifestado por José Luis Rodríguez Zapatero en la sesión de investidura como Presidente del Gobierno, el 8 de abril de 2008, al apuntar que:

> "[…] en esta línea de mejora de nuestra seguridad el Gobierno propondrá una Estrategia Nacional de Seguridad, que remitiremos a esta Cámara, para definir objetivos, señalar prioridades, cuantificar dotaciones, asegurar colaboración y planificar los esfuerzos organizativos y presupuestarios"[755].

A partir de este compromiso se le encomienda a Javier Solana, que viene de presentar al Consejo Europeo el Informe sobre la Aplicación de la Estrategia Europea de Seguridad como AR/VP de la UE, la dirección y coordinación de la Comisión y el grupo de trabajo responsable de la redacción de la primera estrategia de seguridad nacional española,

[755] Discurso de don José Luis Rodríguez Zapatero en la sesión de investidura como Presidente del Gobierno, el 8 de abril de 2008. Disponible en: https://www.lamoncloa.gob.es/presidente/intervenciones/Paginas/2008/prsp20080408.aspx (29/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

que será aprobada por el Consejo de Ministros el 24 de junio de 2011 con el título de *Estrategia Española de Seguridad: una responsabilidad de todos*[756].

4.4.1. Estrategia Española de Seguridad: una responsabilidad de todos (2011)

"Garantizar la seguridad de España y de sus habitantes y ciudadanos es responsabilidad esencial del Gobierno y del conjunto de las Administraciones Públicas. También de la sociedad. La seguridad es hoy responsabilidad de todos"[757]. Con este párrafo inicia la Estrategia Española de Seguridad de 2011 (EES 2011) centrando su objetivo y, al mismo tiempo, señalando responsables para poder alcanzarlo, mostrando ya ese novedoso enfoque integral y multidisciplinar de la seguridad nacional que impregna todo el documento. Por otro lado, es evidente el influjo europeísta de Javier Solana en su redacción, que marca una clara sintonía con la primera Estrategia Europea de Seguridad de 2003, de la que también fue su director.

La estructura que la vertebra es similar a la elegida por otros países occidentales para sus estrategias coetáneas y avanza a través de un resumen ejecutivo y cinco capítulos dedicados, respectivamente, a los conceptos básicos que definen la política de seguridad nacional, el contexto geoestratégico del momento, los potenciadores de riesgo, el análisis de las amenazas y las líneas de respuesta para cada una de ellas, para finalizar con el modelo institucional propuesto para articular la efectiva aplicación de este modelo de seguridad.

Partiendo de esta presentación, el primer capítulo de la EES 2011 titulado *una estrategia necesaria*, expone la relación entre la política de seguridad y la defensa de los intereses y valores de nuestro modelo de Estado, introduciendo los seis conceptos básicos que conforman el corazón de la seguridad española: su enfoque integral, la coordinación y cooperación a todos los niveles, la eficiencia en el empleo de los recursos disponibles, el enfoque anticipativo y preventivo frente a la amenaza, la resiliencia institucional y social, y la interdependencia con respecto a nuestros socios y aliados. Es de interés resaltar el dato de que, siendo ésta la primera Estrategia española, ya se refiere a la *resiliencia* como la capacidad de resistencia y recuperación para hacer frente a los "retos, amenazas y desafíos hoy imprevisibles"[758]. Por el contrario, se echa en falta una definición de lo que se entiende por *seguridad nacional*.

En el segundo capítulo, *la seguridad de España en el mundo*, se define su contexto geopolítico partiendo de algunas constataciones básicas que giran en torno a una idea central que comparte su hermanastra la Estrategia Europea de Seguridad 2003: las amenazas lejanas son tan a considerar como las cercanas, por lo que la seguridad

[756] Nota de prensa de La Moncloa sobre la aprobación de la Estrategia Española de Seguridad 2011. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/paginas/enlaces/24062011enlace2.aspx (29/12/2023).
[757] Estrategia Española de Seguridad 2011. Resumen ejecutivo, página 9. Gobierno de España, Madrid, 2011. Disponible en: https://www.lamoncloa.gob.es/documents/9BED-CF7A-estrategiaespanoladeseguridad.pdf (29/12/2023).
[758] IBIDEM, página 17.

Ediciones Universidad de Salamanca | CC BY-NC-ND

nacional atañe tanto a la actividad interior como a la acción exterior del Estado. A partir de ella se presentan los principales ámbitos geográficos de interés para nuestro país, comenzando lógicamente por la UE como principal núcleo de identidad e influencia, para continuar con EE.UU. en su papel de aliado prioritario, con Rusia en cuanto apuesta de futuro que debe consolidarse, con Iberoamérica por su profunda vinculación histórica, cultural y política que la convierten en oportunidad estratégica, con el Magreb y Oriente Próximo como regiones primordiales para nuestra seguridad y la de Europa, con África en cuanto centro de atención para promover su desarrollo como forma de desactivar la alta conflictividad criminal en zonas como el Sahel o el Cuerno de África, y finalmente con Asia en cuanto nuevo eje de atención internacional con actores cada vez más relevantes como China o India.

El tercero de los capítulos de la EES 2011, *potenciadores del riesgo*, se dedica íntegramente a estos en cuanto productos secretados por la globalización "que propician la propagación o transformación de las amenazas y riesgos que afrontamos e incrementan nuestra vulnerabilidad"[759] otorgándoles una preeminencia que, a nuestro modo de ver, no les corresponde como fenómenos subordinados a la auténtica razón de ser de un documento que debe reflejar una visión amplia e interdisciplinar de la seguridad, guía para la consecución de los intereses nacionales: la amenaza. Dicho esto, se enumeran en la EES 2011 como potenciadores del riesgo la globalización -auténtico origen de todos los demás-, los desequilibrios demográficos, la pobreza y la desigualdad, el cambio climático y la escasez de recursos, los peligros tecnológicos y las ideologías radicales y no democráticas.

A continuación, el capítulo cuarto, *amenazas, riesgos y respuestas*, entra ya a describir los riesgos y amenazas que se estima que pueden afectar a la seguridad nacional española, ligando a cada una de ellas las propuestas de acción de respuesta, de carácter bastante heterogéneo y que, conforme a la naturaleza estratégica del documento, no concretan las capacidades a emplear, confiando su desarrollo a posteriores estrategias de segundo y tercer nivel que lo lleven a efecto. No obstante, a nuestro parecer algunas de estas líneas de acción adolecen de un cierto talante propagandista al presentar como medidas puestas en marcha *ad hoc* a órganos y estructuras creadas años atrás a nivel táctico u operativo para responder a la realidad delincuencial del momento, como por ejemplo el Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior[760] o la Unidad de Delincuencia Económica y Fiscal[761]. En cuanto a los riesgos y amenazas, la EES 2011 refiere los que en ese momento pueden considerarse principales desafíos a

[759] IBIDEM, página 33.

[760] El Centro Nacional de Coordinación Antiterrorista de la Secretaría de Estado de Seguridad del Ministerio del Interior, fue creado por Acuerdo del Consejo de Ministros del 28 de Mayo de 2004. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2004/c2805040.aspx#CNCoordAntiterrorista (30/12/2023).

[761] La Unidad Central de Delincuencia Económica y Fiscal de la Comisaria General de Policía Judicial de la Policía Nacional se crea por Orden INT/2103/2005, de 1 de julio, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía. Disponible en: https://www.boe.es/boe/dias/2005/07/02/pdfs/A23672-23682.pdf (30/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la seguridad de cualquier democracia occidental, siendo estos los conflictos armados y las crisis regionales asociadas, el terrorismo autóctono y el de carácter internacional, el crimen organizado con su gran variedad de tentáculos, la inseguridad económica y financiera como potencial elemento desestabilizador, la vulnerabilidad energética y sus efectos en el funcionamiento de la economía y de la sociedad, la proliferación de armas de destrucción masiva y su vinculación con la criminalidad, las ciberamenazas como grave riesgo emergente, los flujos migratorios irregulares y las emergencias y catástrofes de todo tipo. En una especie de limbo, dentro de este capítulo pero con tratamiento aparte y diferenciado, se alude a las infraestructuras, suministros y servicios críticos como elementos sustanciales para salvaguardar el actual modo de vida de nuestra sociedad, su bienestar y su economía, que pueden verse afectados por algunas de las amenazas ya descritas generando graves problemas de seguridad por sus efectos en cascada en este tipo de sistemas altamente interdependientes. En este caso la EES 2011 se muestra particularmente ágil para dar cobijo, aunque sea en tierra de nadie, a una de las sensibilidades más novedosas del momento, la cual acaba de alcanzar su marco normativo con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su desarrollo mediante Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Finalmente, el capítulo quinto de la EES 2011, *un modelo institucional integrado*, representa el aspecto más innovador por cuanto:

> "[…] pone en marcha un cambio de modelo de seguridad en el que la responsabilidad de las decisiones importantes para la seguridad nacional se concentra en el Presidente del Gobierno; en el que se va a pasar de un modelo de gestión basado en la coordinación interministerial a otro basado en la integración supraministerial; y con el que se pretende pasar de reaccionar ante los problemas a anticiparse a ellos y de improvisar las respuestas a planificarlas" (ARTEAGA MARTÍN, 2011).

Efectivamente, se trata de impulsar cambios orgánicos de alto nivel en la estructura de Gobierno que hagan posible la efectiva aplicación de esta concepción integrada de la seguridad, mediante su gestión y seguimiento a través de un modelo encabezado por el Presidente del Gobierno que es asesorado por el *Consejo Español de Seguridad*, órgano político superior responsable de articular la respuesta coordinada de todos los Ministerios y liderar la gestión de asistencia al Presidente con la ayuda de una Unidad multidisciplinar, apoyado a su vez por un nivel técnico representado por las Comisiones Interministeriales creadas para cometidos precisos en áreas concretas de trabajo. Además, haciendo honor al lema de *la seguridad es hoy responsabilidad de todos*, determina la creación de un *foro social* como órgano consultivo de amplia participación, en el que tienen cabida expertos de cualesquiera materias que puedan ser de interés, académicos, investigadores, representantes de las diferentes Administraciones Públicas, empresas y otros actores que pueda aportar capacidades y conocimiento a esta concepción integradora de la seguridad nacional. Todo ello con el complemento normativo necesario y las consiguientes estrategias de segundo nivel para su desarrollo.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Podemos así concluir que la EES 2011 es un documento de marcado contenido doctrinal -característica que comparte con su hermanastra europea- enfocado claramente al impulso de la cultura de seguridad y la sensibilización social frente a la amenaza, valiente en cuanto primer acercamiento a la plasmación fundamentada de una *estrategia de seguridad nacional* y, en este sentido, innovadora por el modelo que sugiere, en el que se da carta de naturaleza a la resiliencia como concepto básico, pero que padece de falta de pragmatismo a la hora de definir cómo poner en marcha esos medios que permitan alcanzar los intereses nacionales que define, los cuales deberían haber tenido el mayor respaldo político posible para que la EES 2011 hubiese funcionado como un mecanismo de unidad y solidaridad entre territorios, cuestión que no llegó a producirse:

> "[…] debido, fundamentalmente, a que era un documento elaborado sin un mínimo consenso político y que se aprobó pocos meses antes de que se produjera un cambio de partido político en el Gobierno. Así, la «adaptación orgánica y normativa de las Administraciones Públicas para responder a las exigencias de esta Estrategia» no llegó a realizarse" (BALLESTEROS MARTÍN M. A., 2016, pág. 251).

4.4.2. Estrategia de Seguridad Nacional: un proyecto compartido (2013)

La Estrategia de Seguridad Nacional 2013 (ESN 2013) es una revisión continuista de la EES 2011 que busca el consenso político no alcanzado por su predecesora a la par de un enfoque menos conceptual y más práctico que, reduciendo incluso su extensión, se acompaña del desarrollo orgánico del sistema institucional que respalda su puesta en marcha. La estructura del documento es básicamente la misma, comenzando con un resumen ejecutivo que firma el Presidente del Gobierno para, posteriormente, desarrollar cinco capítulos en los que se abordan, respectivamente, las definiciones y los principios básicos de la estrategia de seguridad, los focos de interés geopolítico para España, los riesgos, amenazas y factores potenciadores que pueden afectar a sus intereses, las líneas de acción estratégicas y, finalmente, la enunciación de la *Ley Orgánica de Seguridad Nacional* y la concreción del *Sistema de Seguridad Nacional*.

La nueva ESN 2013, a diferencia de la de 2011, nace del acuerdo entre los dos principales grupos parlamentarios -PP y PSOE- para asegurar el consenso en los objetivos y líneas de acción estratégicas que, como corresponde a una Política de Estado, transcienden el marco temporal de un solo Gobierno y que buscan la adhesión de todas las fuerzas políticas y del conjunto de los ciudadanos "desde el convencimiento de que la seguridad nacional es -y así reza el mismo título de la estrategia- un proyecto compartido"[762].

El capítulo primero, *una visión integral de la Seguridad Nacional*, la presenta como el complemento necesario que sustenta, por un lado, la estabilidad y continuidad del Estado y, por otro, la vida, la libertad y el bienestar de los ciudadanos desde el respeto

[762] Comparecencia del señor director del gabinete del presidente del Gobierno (Moragas Sánchez), para presentar la estrategia de seguridad nacional 2013. A propuesta del Gobierno. (Número de expediente 212/001017). Diario de Sesiones del Congreso de los Diputados, Comisión Constitucional, sesión núm. 16 (extraordinaria), celebrada el martes 9 de julio de 2013, página 2. Disponible en: https://www.congreso.es/public_oficiales/L10/CONG/DS/CO/DSCD-10-CO-372.PDF (03/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

a la Constitución y el Estado de Derecho, resolviendo que "las sociedades que se hacen responsables de su seguridad son sociedades más libres"[763]. Desde este enfoque se define la *seguridad nacional* como:

> "[…] la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos"[764].

Posteriormente, y desde la premisa de que la *seguridad nacional* requiere el consenso y la responsabilidad política y social de todos y a todos los niveles, se define la *estrategia de seguridad nacional* como "la articulación fundamental de la Seguridad Nacional como Política de Estado"[765]. La delimitación del marco conceptual de este primer capítulo finaliza con la presentación de los cuatro principios informadores de la ESN:

1. La unidad de acción de los actores institucionales junto con la colaboración público privada y el apoyo ciudadano.
2. La anticipación y la prevención
3. La eficiencia y sostenibilidad en el uso de los recursos.
4. Y la resiliencia, concebida aquí como "la aptitud de los recursos humanos y materiales para afrontar con flexibilidad y fortaleza las situaciones de crisis y sobreponerse a ellas minimizando y absorbiendo sus consecuencias negativas"[766].

La seguridad de España en el mundo es el título del capítulo segundo que, esencialmente, hace un recorrido por los mismos escenarios de interés geoestratégico para España a los que atendía el capítulo segundo de la EES 2011, compartiendo las consideraciones de política exterior y el enfoque sobre los desafíos que se derivan de los conflictos no resueltos en nuestro entorno, de la reordenación geopolítica mundial, de las alianzas y relaciones de vecindad consecuentes a ser un país europeo clave en las relaciones con Latinoamérica y primordial en la política de estabilidad en la ribera sur del Mediterráneo.

El capítulo tercero se refiere a *los riesgos y amenazas para la Seguridad Nacional* que, a diferencia de la EES 2011, incluye también los factores potenciadores que, en aquella, tenían un tratamiento en capítulo diferenciado. El problema sigue siendo, sin embargo, que la nueva Estrategia no distingue entre *riesgo* y *amenaza* ofreciendo un tratamiento conjunto que, de nuevo, reproduce los de la anterior del 2011 con tres excepciones:

1. Introduce el *espionaje* como amenaza para la seguridad nacional de primer orden por su vinculación con actores estatales o no estatales, guiados por

[763] Estrategia de Seguridad Nacional 2013. Capítulo 1, página 5. Presidencia del Gobierno, Madrid, 2013. Disponible en: https://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf (03/01/2024).
[764] IBIDEM, página 7.
Esta definición prácticamente se calca en el artículo 3 de la Ley de Seguridad Nacional, que únicamente añade a la protección de la libertad y el bienestar de sus ciudadanos el de sus derechos.
[765] IBIDEM, página 8.
[766] IBIDEM, página 2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

intereses ideológicos o estratégicos para la obtención de información que les procure cualquier tipo de ventaja.

2. Se incluye también como factor de riesgo la *vulnerabilidad del espacio marítimo* por su alto valor estratégico en cuanto nuevo medio de acopio de recursos energéticos, vía preferente de comunicación e intercambio comercial, clave en el transporte de gas y petróleo, y custodio del patrimonio arqueológico submarino.
3. Y la tercera novedad es que también se da entrada como factor de riesgo a la *vulnerabilidad de las infraestructuras críticas y los servicios esenciales* -que en la anterior Estrategia quedaban en tierra de nadie- por el alto impacto que, sobre la seguridad nacional, tendría un incidente o ataque que causara la caída de estos sistemas complejos, interrelacionados, muy tecnificados y con escasas soluciones alternativas que dan soporte al normal funcionamiento de los sectores de producción y servicios, y de la sociedad en general.

El capítulo cuarto, *líneas de acción estratégicas*, supone un paso adelante respecto a la EES 2011 por cuanto cada uno de los doce riesgos y amenazas previamente identificados genera un ámbito de actuación para el que, específicamente, se define un objetivo a alcanzar y se marcan unas líneas de acción a través de las que articular la respuesta integral que permita alcanzarlo. Con estas variables se define una matriz con la que se trata de operativizar el concepto multidisciplinar y multidimensional de la seguridad "donde los asuntos militares comparten responsabilidad con los políticos, los económicos, los sociales, los medioambientales y los individuales" (JIMÉNEZ OLMOS, 2013).

Finalmente, el capítulo quinto recoge la aportación más novedosa de la ESN 2013: *un nuevo Sistema de Seguridad Nacional*, cuyo objetivo es preservar la seguridad nacional "a través del funcionamiento óptimo, integrado y flexible de todos los recursos disponibles a tal fin"[767], y sustentado en ocho principios: el liderazgo del Presidente del Gobierno, el funcionamiento integrado y coordinado de las Administraciones Públicas, la optimización y el uso eficaz de los recursos, la modernización de las estructuras y los procedimientos de actuación relativos a la seguridad nacional en las Administraciones Públicas, la implicación de la sociedad civil y el fomento de la cultura de seguridad, la colaboración público-privada, la gestión de la información y el conocimiento, y la transparencia. La estructura que se define del Sistema de Seguridad Nacional es la que se mantiene vigente, con el Consejo de Seguridad Nacional y los Comités Especializados como principales elementos característicos. También es relevante el compromiso que el Gobierno asume en la propia Estrategia con la redacción de una Ley Orgánica que dé soporte a la reforma institucional propuesta y a los instrumentos de gestión de crisis planteados, que se perfecciona meses después con la aprobación en trámite parlamentario de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Cabe concluir que la ESN 2013 cumple con acierto su objetivo de revisar la EES 2011 y, al mismo tiempo, se dota de un apoyo consensuado que su predecesora no tenía, pero debido a la coyuntura especialmente convulsa en la que se gesta, nace prácticamente

[767] Estrategia de Seguridad Nacional 2013. Capítulo 5, página 53. Presidencia del Gobierno, Madrid, 2013.

Ediciones Universidad de Salamanca | CC BY-NC-ND

condenada a una corta existencia derivada, paradójicamente, de la necesidad de mantenerse acorde con la realidad de los desafíos de seguridad a los que debe dar respuesta.

4.4.3. Estrategia de Seguridad Nacional: un proyecto compartido de todos y para todos (2017)

Guiada por los mismos principios de unidad de acción, anticipación, eficiencia y resiliencia[768] comienza la ESN 2017, hasta ahora la más extensa de todas con sus ciento veinticuatro páginas distribuidas en resumen ejecutivo, introducción y seis capítulos, explicando las razones que la justifican en base a los sustanciales cambios acaecidos en el panorama geoestratégico mundial desde la aprobación de la anterior ESN 2013, de acuerdo con lo estipulado al respecto[769] por la *Ley de Seguridad Nacional*, sobre cuyo marco conceptual se construye al presentar los *componentes fundamentales* de la Seguridad Nacional[770] y los *ámbitos de especial interés*[771] como la ciberseguridad o la seguridad energética, para los que no solo se requiere la actuación de aquellos "sino del conjunto de las administraciones y de la sociedad en general"[772] puesto que, al fin y al cabo, como reza su enunciado, se trata de *un proyecto compartido de todos y para todos*.

El capítulo primero de la ESN 2017, titulado *una Seguridad Nacional para la España de hoy*, señala los elementos que definen el perfil de país -Estado social y democrático de Derecho- y sus valores superiores -libertad, justicia, igualdad y pluralidad política- que condicionan tanto la misión como la visión de la Estrategia. Desde estos presupuestos se afrontan las amenazas y desafíos que pueden socavar su seguridad, conformando la *respuesta de carácter integral* que se necesita a partir de, por un lado, la vocación global de España, puente entre países y culturas consolidado sobre su fuertes pilares europeos, mediterráneos y atlánticos, y por otro, el firme compromiso de todos los actores nacionales sobre la base de la *cultura de seguridad nacional*.

Por su parte el capítulo segundo, *dinámicas de transformación de la Seguridad Nacional*, analiza los profundos cambios que, desde el 2013, se han producido en el entorno de

[768] Estos cuatro *principios rectores* ya son recogidos en la ESN 2013 bajo la denominación de *principios informadores*, pareciendo más adecuada y clarificadora la nueva denominación por cuanto estos constituyen la línea directriz que gobierna todo el desarrollo argumental de la Estrategia.

[769] El artículo 4.3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, estipula que la Estrategia de Seguridad Nacional "se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico".

[770] El artículo 9.1 de la LSN 2015 señala que "Se consideran componentes fundamentales de la Seguridad Nacional a los efectos de esta ley la Defensa Nacional, la Seguridad Pública y la Acción Exterior, que se regulan por su normativa específica".

[771] El artículo 10 de la LSN 2015 señala que "Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente".

[772] Estrategia de Seguridad Nacional 2017. Introducción, página 14. Presidencia del Gobierno, Madrid, 2017. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2017 (08/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

seguridad global y que confirman la necesidad de revisar la Estrategia con la que poder entenderlos para, en línea con lo establecido por sus principios rectores, poder afrontarlos con garantía de éxito. No es otro el problema que la incertidumbre que brota de la pérdida de referencias antes claramente instituidas, siendo que ahora, en el nuevo contexto mundial de feroz competición sistémica sin hegemonías incuestionables, se difuminan los límites entre *estabilidad* y *crisis*, entre *paz* y *conflicto*, entre *aliados* y *enemigos*, dando lugar a la insustancialidad del retorno a inoperantes técnicas proteccionistas y antiguas ideas revisionistas que, nutridas por la eclosión de las redes sociales y la vertiginosa evolución tecnológica, dan alas a la polarización social, a la radicalización y a la desnaturalización de la política como punto de encuentro para la diversidad de opiniones, esencia del sistema democrático. De ahí que el reto consista en gestionar la incertidumbre y anticiparse a sus consecuencias.

El capítulo tercero, *España en el mundo: un país con vocación global*, analiza los retos y desafíos provenientes de las principales zonas geopolíticas que pueden repercutir en la seguridad nacional española, siendo estas Europa, Norte de África y Oriente Medio, África Subsahariana, América Latina, EE.UU. y Asia-Pacífico. Se trata de una delimitación geográfica más acorde con el contexto estratégico español y que, en el ámbito europeo, que pasa en esos momentos por una complicada coyuntura política a raíz del Brexit, los movimientos nacionalistas y los efectos de la crisis económica, propone impulsar un mayor compromiso de los EEMM con la Unión mediante el desarrollo de una verdadera PCSD en *entente cordiale* con la Alianza transatlántica, la mejora del marco colaborativo en la seguridad interior y la búsqueda de soluciones conjuntas con Rusia para superar los retos que su política exterior está planteando para la seguridad europea, con acciones como la anexión ilegal de la península de Crimea.

El capítulo cuarto, *amenazas y desafíos para la Seguridad Nacional*, los clasifica y evalúa para graduar el nivel de la respuesta que merece cada uno de ellos, partiendo de su alto nivel de interconexión y su dimensión transfronteriza. Llama la atención la nomenclatura de referencia donde se cambian los *riesgos* por *desafíos*, definidos como aquellos "que sin tener de por sí entidad de amenaza, incrementan la vulnerabilidad, provocan situaciones de inestabilidad o pueden propiciar el surgimiento de otras amenazas, agravarlas o acelerar su materialización"[773]. Tanto la EES 2011 como la ESN 2013 contemplaban los *riesgos* y las *amenazas* sin distinción entre ellos, mientras que la ESN 2017 establece cinco tipos de *amenazas* que comprometen o puede socavar la seguridad nacional[774], tres *amenazas y desafíos que se desarrollan en espacios comunes globales*[775], la *amenaza sobe las infraestructuras críticas* que soportan los servicios

[773] Estrategia de Seguridad Nacional 2017. Capítulo 4, página 56. Presidencia del Gobierno, Madrid, 2017.
[774] Las cinco amenazas que señala la ESN 2017 en su capítulo 4 son los conflictos armados, el terrorismo, el crimen organizado, la proliferación de armas de destrucción masiva y el espionaje.
[775] La ESN 2017 entiende que el desafío que suponen los espacios comunes globales viene determinado por su ausencia de fronteras físicas, la débil jurisdicción y regulación que existe sobre ellos, su facilidad de acceso y la dificultad de atribución de acciones. A partir de ello, identifica como amenazas la vulnerabilidad del ciberespacio, del espacio marítimo y del espacio aéreo y ultraterrestre.

Ediciones Universidad de Salamanca | CC BY-NC-ND

esenciales necesarios para el desarrollo de las actividades sociales y económicas básicas[776] y, finalmente, seis *desafíos*[777].

El capítulo quinto, *objetivos generales y líneas de acción de la Seguridad Nacional*, presenta aquellos como un mandato a alcanzar, señalando en primer lugar el desarrollo de un *modelo integral de gestión de crisis* que parta del enfoque preventivo y anticipatorio, articule una respuesta que involucre a todos los sectores -públicos y privados- y a la sociedad civil, y potencie la resiliencia como mecanismo de superación y vuelta a la normalidad. Junto a ello, en segundo lugar, dispone la promoción de la *cultura de seguridad nacional* como la eterna tarea pendiente. Continúa indicando la necesidad de favorecer el buen uso de los espacios comunes globales en lo que, a nuestro entender, parece más una ingenua declaración que un objetivo que realmente se pueda conseguir dada la dimensión y la naturaleza de dichos entornos y la obviedad de que "cualquier acción contraria al buen uso de estos espacios resulta crítica, dada la dificultad de vigilancia, monitorización y respuesta ante cualquier acto ilícito y el impacto significativo de diversas formas de desconexión funcional e informativa"[778]. En cuarto lugar, estipula el impulso de la dimensión de seguridad en el desarrollo de las tecnologías, que se imbrica con las anteriores por cuanto forma parte del *modelo integral de seguridad* propuesto y, lógicamente, necesita del compromiso de una amplia parte del sector industrial y productivo del país, fruto a su vez de la concienciación sobre la relevancia de la seguridad y el alcance de los desafíos que comporta. Y en quinto y último lugar, señala como objetivo general el fortalecimiento de la proyección internacional de España como clave para proteger sus intereses desde la perspectiva integral de la seguridad nacional, atendiendo tanto a su dimensión interior como a la exterior.

A continuación, se despliegan los quince ámbitos de actuación que la ESN 2017 identifica como *críticos* para la seguridad nacional española. En el ámbito de la defensa nacional se marca como objetivo "asegurar la defensa de la soberanía e integridad de España y la protección de la población y el territorio frente a cualquier conflicto o amenaza proveniente del ámbito exterior, de forma autónoma o junto a socios y aliados"[779] en un claro ejemplo de identificación de la amenaza y adaptación concreta de la respuesta, proponiendo como líneas de acción la capacidad de disuasión efectiva de las Fuerzas Armadas, el relanzamiento de la PCSD y el mantenimiento del compromiso con la OTAN, entre otras.

En el ámbito de la lucha contra el terrorismo su objetivo no es otro que neutralizar dicha amenaza a través de la estrategia de *las tres P* que ya presentó la anterior ESN 2013: 1) prevención; 2) protección; 3) persecución y preparación de la respuesta.

[776] Estas infraestructuras estratégicas hacen referencia a las Administraciones Públicas, el sector de la alimentación, el agua, la energía, el espacio, la industria química y nuclear, las instalaciones de investigación, el sistema de salud y el financiero, el sector TIC y las infraestructuras de transportes.
[777] Los desafíos que recoge la ESN 2017 son la inestabilidad económica y financiera, la vulnerabilidad energética, los flujos migratorios irregulares, las emergencias y catástrofes, las epidemias y pandemias y, en último lugar, los efectos derivados del cambio climático.
[778] Estrategia de Seguridad Nacional 2017. Capítulo 5, página 84. Presidencia del Gobierno, Madrid, 2017.
[779] IBIDEM, página 88.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En el ámbito de la lucha contra el crimen organizado, el objetivo es igualmente la neutralización de la amenaza, a través de tres líneas de acción muy concretas:

1. La formación continua en las tácticas y procedimientos utilizados por las organizaciones criminales.
2. Potenciar el intercambio de información entre los actores involucrados.
3. Mejorar la cooperación internacional frente a esta lacra delincuencial, cuyos efectos para la estabilidad de las estructuras de gobierno son altamente desestabilizadores y peligrosos[780].

En el ámbito de la *no proliferación de armas de destrucción masiva* el objetivo es combatirla e impedir su acceso por actores no estatales y organizaciones terroristas, para lo que se establecen como líneas de acción, entre otras, potenciar el multilateralismo eficaz y promover el cumplimiento del ordenamiento jurídico internacional, reforzar los mecanismos de control del comercio internacional de materiales de doble uso que pudieran ser utilizados con fines ilícitos, y profundizar en la investigación de los flujos de capitales relacionados con este tipo de actividades.

En el ámbito de la contrainteligencia el objetivo es el mismo que el de la ESN 2013, incorporando como línea de acción la intensificación de las labores de contrainteligencia en el ciberespacio.

En el ámbito de la *ciberseguridad*, el objetivo es garantizar la seguridad de los sistemas y fomentar el uso seguro y confiable del ciberespacio, con líneas de acción referidas al reforzamiento de capacidades frente a la ciberamenaza, la promoción de un marco normativo adecuado en consonancia con medidas y planes de protección y fomento de buenas prácticas en el entorno digital, y la cooperación multinivel tanto a nivel nacional como internacional. Por su parte, la *desinformación* aún no es tratada singularmente "sino como parte de los riesgos tecnológicos asociados al ciberespacio y sin proponer objetivos ni líneas de acción específicas" (BADILLO & ARTEAGA, 2024, pág. 15).

En el ámbito de la seguridad marítima el objetivo es garantizarla desde un enfoque integral, colaborativo y cooperativo que contemple, además, la ciberseguridad en esta dimensión.

En el ámbito de la seguridad del espacio aéreo y ultraterrestre, novedad respecto a la ESN 2013, el objetivo es garantizar su seguridad previniendo las amenazas y neutralizando sus consecuencias, para lo que se definen líneas de acción como la actuación coordinada de todas las Administraciones Públicas concernidas y el impulso del desarrollo de un marco normativo para el uso civil de los UAS[781].

[780] Un claro ejemplo de los perniciosos efectos del crimen organizado para cualquier tipo de Estado es la situación generada en enero de 2023 en Ecuador, con acciones de alta violencia simultáneas y perfectamente coordinadas como el asalto al canal TC Televisión, algaradas callejeras, secuestro de policías y motines con rehenes en prisiones, que llevan al Presidente Daniel Noboa a decretar un conflicto armado interno en el país. Disponible en: https://cnnespanol.cnn.com/2024/01/10/que-es-conflicto-armado-interno-noboa-ecuador-orix/ https://www.rtve.es/noticias/20240111/ecuador-crimen-organizado/2470865.shtml (11/01/2024).

[781] Unmanned Aircraft System, término referido a cualquier sistema de aeronave no tripulada pilotada remotamente, o programada para realizar un patrón de vuelo predefinido.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En el ámbito de la protección de infraestructuras críticas, el objetivo es asegurar la provisión de los servicios esenciales y potenciar su resiliencia, destacando las líneas de acción referidas a la innovación en seguridad aplicada a los sistemas y componentes de dichas infraestructuras, apostando por el desarrollo I+D+i español, y la coordinación para su seguridad entre los actores responsables de la lucha contraterrorista y contra las ciberamenazas.

En el ámbito de la seguridad económica y financiera el objetivo es promover un crecimiento económico equilibrado a través de medidas como el desarrollo de órganos y procedimientos de control económico y financiero, la protección de los intereses nacionales a través del manejo de información y la aplicación de la inteligencia generada, la cooperación internacional o el avance en la Unión Económica y Monetaria.

En el ámbito de la seguridad energética, el objetivo es el mismo que el de la ESN 2013, referido a diversificar las fuentes de energía y garantizar su transporte y abastecimiento, destacando entre las líneas de acción la diversificación del mix energético nacional.

En el ámbito de la ordenación de flujos migratorios se marca como objetivo su prevención, control y ordenación, destacando la expresa mención al componente humano de esta realidad, que no se recogía en la ESN 2013, con líneas de acción entre las que destacamos el impulso de una política migratoria y de asilo común en la UE, así como la colaboración entre las Administraciones Públicas y el resto de actores del sector privado y no gubernamental para prevenir los riesgos asociados a la inmigración irregular.

En el ámbito de la protección ante emergencias y catástrofes, el objetivo es consolidar el Sistema Nacional de Protección Civil como instrumento integrador de la respuesta ante este tipo de crisis, con líneas de acción concretas como elaborar, aprobar e implantar de forma cooperativa en todas las Administraciones competentes la Estrategia del Sistema Nacional de Protección Civil, tras su aprobación por el Consejo de Seguridad Nacional, cuestión que tomaría forma con la publicación de la Estrategia Nacional de Protección Civil en 2019[782], reformada posteriormente en diciembre de 2024[783].

En el ámbito de la seguridad frente a pandemias y epidemias, que no aparece como tal en la anterior Estrategia, la ESN 2017 se muestra plenamente acertada al definir como objetivo "adoptar planes de preparación y respuesta ante riesgos sanitarios, tanto genéricos como específicos, bajo el principio de coordinación entre la Administración general del Estado y las Administraciones Autonómicas y con organismos

[782] Orden PCI/488/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Protección Civil, aprobada por el Consejo de Seguridad Nacional. BOE núm. 103, martes 30 de abril de 2019. Disponible en: https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6348.pdf (07/01/2024).

[783] Orden PJC/1430/2024, de 16 de diciembre, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 15 de octubre de 2024, por el que se aprueba la Estrategia Nacional de Protección Civil. BOE núm. 304, de 18 de diciembre de 2024. Disponible en: https://www.boe.es/eli/es/o/2024/12/16/pjc1430 (12/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

internacionales..."[784], destacando entre las líneas de acción la de adaptar servicios de salud pública, tanto del Estado como de Comunidades Autónomas, para asegurar la capacidad de respuesta a nivel nacional, y la revisión y actualización periódica de los planes preventivos y de respuesta ante crisis de este tipo.

En el ámbito de la preservación del medio ambiente, también novedoso, el objetivo es conservar un medio ambiente de calidad y la protección del patrimonio natural, con líneas de acción concretas en el marco de los incendios forestales, la contaminación atmosférica y del medio marino, el uso de energías alternativas o la gestión de la escasez hídrica.

Finalmente, el capítulo sexto se dedica al *Sistema de Seguridad Nacional*, donde se establecen iniciativas para su reforzamiento y consolidación estructural, como la aprobación de un Plan Integral de Cultura de Seguridad Nacional, definir la posición estratégica de España frente al uso de los espacios comunes globales, la declaración del CSN como punto de contacto único en el marco de la seguridad de redes y sistemas con las autoridades competentes europeas y de los EEMM, o la revisión de las estrategias de Seguridad Marítima, de Ciberseguridad y de Seguridad Energética, y la redacción de una nueva Estrategia de Seguridad Aeroespacial.

Podemos así concluir señalando que la ESN 2017 nace como consecuencia de los relevantes cambios en el panorama estratégico mundial que, lógicamente, tienen eco en el ámbito de la seguridad nacional española, revisando y actualizando la ESN 2013 a través de un documento más detallado y mejor estructurado que comienza poniendo en valor los elementos fundamentales que conforman nuestro Estado social y democrático de Derecho, y sus principios fundamentales de libertad, justicia, igualdad y pluralidad política, que justifican el carácter vertebrador y de cohesión que tiene la seguridad. Esta Estrategia plantea el reto de los *espacios comunes globales*, y los describe a través de la ausencia de fronteras definidas, la débil jurisdicción y regulación normativa que sobre ellos rige, la facilidad de acceso y la dificultad de atribución de acciones en su ámbito, frente a los que no muestra claridad de objetivos prácticos, quedándose a nuestro entender en el etéreo mundo de los deseos. Convenimos con el General Ballesteros que "el éxito de la ESN 2017 no reside tanto en lo que dice como en la capacidad de movilización de los niveles inferiores para que estos aborden todas y cada una de las líneas de acción establecidas para los quince ámbitos que recoge la ESN 2017" (BALLESTEROS MARTÍN M. Á., 2017, pág. 18).

4.4.4. Estrategia de Seguridad Nacional: un proyecto compartido (2021)

El CSN aprueba en octubre de 2020 el procedimiento para la elaboración de la ESN 2021[785] en el contexto de la pandemia del COVID-19, "primera gran crisis desde la Segunda Guerra Mundial, que se ha visto exacerbada por el uso perverso de la

[784] Estrategia de Seguridad Nacional 2017. Capítulo 5, página 114. Presidencia del Gobierno, Madrid, 2017
[785] Orden PCM/1028/2020, de 30 de octubre, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se aprueba el procedimiento para la elaboración de la Estrategia de Seguridad Nacional 2021. BOE núm. 292, de 05/11/2020. Disponible en: https://www.boe.es/buscar/pdf/2020/BOE-A-2020-13661-consolidado.pdf (08/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

desinformación por parte de actores tanto estatales como no estatales, con objeto de minar nuestras instituciones y alentar la polarización social, haciendo necesaria la puesta en marcha de mecanismos de lucha contra esta amenaza"[786] y, por consiguiente, la revisión de la estrategia de seguridad nacional como un ejercicio de responsabilidad compartida bajo un *enfoque multinivel y diferenciado* que, bajo la coordinación del CSN, da entrada a las Comunidades Autónomas, Ceuta y Melilla a través de la Conferencia Sectorial para Asuntos de la Seguridad Nacional[787] y, desde los grupos de trabajo liderados por el DSN, a las aportaciones de los especialistas institucionales y de la sociedad civil con conocimiento en la materia[788]. Se trata con ello de dar entrada a todos los actores interesados para, por un lado, como procede con la inteligencia estratégica, "no duplicar recursos y dejar que organismos como universidades, centros de pensamiento y centros de análisis, de cálculo y fuentes abiertas se ocupen de parte del proceso de reflexión sobre las nuevas amenazas" (DÍAZ FERNÁNDEZ A. M., 2013, pág. 63) y, por otro, buscar el "mayor consenso posible"[789] de cara a la aprobación de la estrategia, clave en la definición de la Política de Seguridad Nacional.

Como documento programático, la ESN 2021[790] se estructura en resumen ejecutivo, introducción y cinco capítulos a través de los que se actualiza la visión de los retos que debe afrontar la seguridad nacional española en relación con el nuevo contexto internacional y, al igual que su predecesora de 2017, nace prematura empujada por la naturaleza global de la amenaza, la velocidad del cambio y la incertidumbre que genera, en esta ocasión auspiciada tanto por las consecuencias de la pandemia del COVID-19 como por el incremento en el uso de las estrategias híbridas contra las democracias, vulnerables por su propio dinamismo y permeabilidad a la incorporación de tecnologías que contribuyan a mejorar la interacción entre personas e ideas (RUBIO NUÑEZ, FRANCO ALVIM, & DE ANDRADE MONTEIRO, 2024, pág. 61). Tal es el alcance de estos riesgos sobre la seguridad nacional que se adelanta un año su redacción para, a partir de ella, concretar objetivos tan relevantes como "disponer de un Sistema de Seguridad Nacional digitalizado, capaz de proporcionar datos para la toma de decisiones en tiempo oportuno"[791], destacando así la importancia estratégica de la *propiedad del dato* y de su protección en una sociedad global e hiperconectada, o la elaboración de una *Estrategia Nacional de Lucha contra las campañas de desinformación* que, junto con la *injerencia*

[786] Exposición de Motivos de la Orden PCM/1028/2020 por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se aprueba el procedimiento para la elaboración de la Estrategia de Seguridad Nacional 2021.

[787] Orden PCM/1028/2020, apartado quinto, que dispone "La participación de las Comunidades Autónomas, Ceuta y Melilla en el proceso de elaboración de la Estrategia de Seguridad Nacional" que, a su vez, remite al artículo 6 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional en lo relativo a la articulación de esta colaboración a través de la Conferencia Sectorial para asuntos de la Seguridad Nacional.

[788] Orden PCM/1028/2020, apartados tercero, "Grupo de Trabajo de la Comisión de Alto Nivel", y cuarto, "Comité asesor".

[789] Orden PCM/1028/2020, Exposición de Motivos.

[790] Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. BOE núm. 314, de 31 de diciembre de 2021 (referencia BOE-A-2021-21884). Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884 (08/01/2024).

[791] Estrategia de Seguridad Nacional 2021: un proyecto compartido. Introducción, página 19. Presidencia del Gobierno, Madrid, 2021. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 (08/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de actores externos, suponen un importante elemento de innovación en la consideración de la amenaza para la seguridad nacional española, por cuanto ya se les da un tratamiento específico, no como en la anterior ESN 2017, donde venían vinculadas al espectro de riesgo generado en torno a la ciberamenaza.

Partiendo de que la ESN 2021 presenta una *visión integral de la seguridad* como condición necesaria para la evolución económica y la cohesión social de España, siempre desde la perspectiva de Estado europeo, mediterráneo y atlántico, llama la atención el *desiderátum* de acción multilateral y coordinada que, en el capítulo introductorio, se lanza a la Unión Europea (UE) la cual "debe efectuar acciones conjuntas militares que contribuyan a reforzar el vínculo trasatlántico y que favorezcan la gestión de crisis transfronterizas y su autonomía estratégica" y, en particular, "asumir un mayor papel a la hora de gestionar desafíos, como las pandemias, el terrorismo internacional, los ciberataques o las campañas de desinformación, que requieren respuestas colectivas y la integración de capacidades"[792]. No obstante, hay que señalar al respecto que, para asegurar su efectividad, ambas cuestiones demandan acciones coordinadas dentro de Europa, por lo que, si de verdad se quiere integrar competencias y capacidades de los distintos EEMM, el compromiso y el impulso político desde el Consejo y el Parlamento Europeo son condición *sine qua non* para conseguir, realmente, que prospere una política de defensa europea acorde a este deseo español.

El capítulo primero, *seguridad global y vectores de transformación*, describe el nuevo entorno de relaciones internacionales y sus implicaciones para la seguridad través de cuatro vectores de cambio, siendo el primero de ellos el contexto geopolítico en el que se deteriora el multilateralismo y crece la rivalidad competitiva entre la vieja y egocéntrica zona euroatlántica, representada por EE.UU., y la joven y descarada zona del Indopacífico que, representada por China, quiere para sí la llave del futuro. Una de las principales amenazas que se nutre de esta tensión es la cada vez más probable brecha digital que puede acabar fracturando la Pangea de las tres *www* que hoy día permite el intercambio de ideas a nivel global, y que generaría dos bloques sin contacto y con desarrollos paralelos que, a través de su afectación a las cadenas de suministro y la economía mundial, tendría un efecto en cascada sobre el resto de objetivos de desarrollo comercial, financiero, tecnológico, cultural o diplomático, entre otros.

Dicha tensión de bloques tiene también representación en el incremento del "uso de las estrategias híbridas que, mediante acciones coordinadas y multidimensionales, tratan de explotar las vulnerabilidades de los Estados y sus instituciones con un objetivo de desestabilización o coerción política, social o económica. Estas estrategias se caracterizan por la dificultad de atribuir su autoría y por emplear medios que pueden incluir, además de acciones convencionales, otras como campañas de desinformación, ciberataques, espionaje, subversión social, sabotaje, coacción económica o el uso asimétrico de medios militares"[793].

El segundo factor de cambio es el entorno socio-económico, en el que destaca la fragilidad de la *cadena de suministros*, altamente dependiente de la seguridad en el

[792] IBIDEM, página 19.
[793] Estrategia de Seguridad Nacional 2021. Capítulo 1, página 26. Presidencia del Gobierno, Madrid, 2021.

Ediciones Universidad de Salamanca | CC BY-NC-ND

dominio marítimo, particularmente sensible a actividades ilícitas como las acciones de piratería que vienen ocurriendo desde hace años en el Mar Rojo y el golfo de Adén, cuyo bloqueo al tráfico mercante puede ocasionar pérdidas económicas millonarias a las navieras y graves problemas de suministro a nivel global por cuanto la región aglutina el doce por ciento del comercio mundial[794] o, simplemente, colapsar con un evento tan puntual y localizado como puede ser la avería de un barco de transporte de contenedores en uno de los grandes canales de paso en las rutas marítimas del mundo[795].

El tercer vector de cambio global, que se interrelaciona con los anteriores, se refiere a la *transformación digital* y la amplia vulnerabilidad de los sistemas y redes informáticas de soporte por la ampliación de la superficie de exposición a ciberataques, derivada de la hiperconectividad social y la alteración de los patrones de comportamiento que ello ha supuesto, junto con la permanente aparición de tecnologías disruptivas que obligan a una reconsideración del *dato* como activo estratégico de primer orden y de la *soberanía digital* como política de seguridad nacional.

El cuarto elemento de cambio es el referido a la transición ecológica y sus implicaciones de seguridad, vinculadas con el cambio de paradigma energético y la rivalidad por el control de las materias primas y las tecnologías asociadas a las renovables.

El segundo capítulo, *una España segura y resiliente*, comienza con una declaración de principios y valores democráticos que definen el perfil de país y que, fiel a los postulados de la LSN 2015, abogan por una seguridad centrada en el ciudadano, la cual también debe funcionar como elemento de cohesión territorial. A continuación, se repasan los puntos geográficos de especial interés para España, siendo idénticos a los fijados por la ESN 2017.

El primero de ellos es la UE, a la que se insta al impulso en el desarrollo de la PESC y, en concreto, de la PCSD para posteriormente incluir, por primera vez, una visión de Rusia como rival estratégico frente al que la Unión debe continuar dialogando, al mismo tiempo que debe mantener una postura de firmeza sobre el respeto al Derecho Internacional y la defensa de la soberanía e integridad territorial del resto de Estados.

En cuanto al Magreb y Oriente Próximo, la ESN 2021 se refiere explícitamente a Marruecos y Argelia para destacar su relación "de buena amistad, desde la premisa de

[794] En diciembre de 2023 la compañía Maersk cancela sus rutas por el Mar Rojo a consecuencia de los ataques de los Hutíes. Disponible en: https://cincodias.elpais.com/economia/2023-12-15/maersk-paraliza-todo-su-trafico-de-contenedores-a-traves-del-mar-rojo-ante-la-escalada-de-ataques.html https://blog.hispamicro.com/la-situacion-del-mar-rojo-y-el-golfo-de-aden-y-su-impacto-en-el-comercio-maritimo/ (08/01/2024).

[795] En marzo de 2021 el buque portacontenedores Ever Given se quedó atascado durante casi una semana en el Canal de Suez, cortando el paso al transporte marítimo mundial que transita por esa ruta y generando con ello pérdidas millonarias. Disponible en: https://www.nytimes.com/es/2021/07/19/espanol/canal-suez-evergiven.html https://www.lavanguardia.com/internacional/20210329/6615967/canal-suez-buque-barco-encallado-ultimas-noticias-en-directo.html (08/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

la cooperación leal y el respeto a las fronteras mutuas"[796], haciendo una interpretación timorata de la compleja realidad de las relaciones con estos socios estratégicos que, a nuestro entender, desvirtúa la situación actual y la hace más difícil de entender de lo que ya de por sí es por las complejas relaciones históricas que la condicionan[797].

A continuación, la zona del África Subsahariana por sus delicadas situaciones de inestabilidad y conflicto vinculadas al Sahel, el Golfo de Guinea y el Cuerno de África, focos de máximo interés[798] para "avanzar hacia la paz y seguridad en el Continente –especialmente en la región del Sahel- como condición ineludible para, de forma simultánea, contribuir al desarrollo y la gobernanza de los africanos y, por ende, de los propios europeos" (DIEZ ALCALDE, 2024, pág. 26).

En cuarto lugar, América del Norte y el vínculo transatlántico, apostando por la cooperación UE-OTAN "como eje central de la seguridad colectiva frente a los grandes desafíos globales"[799]. En quinto lugar América Latina y, finalmente, Asia-Pacífico como

[796] Estrategia de Seguridad Nacional 2021. Capítulo 2, página 44. Presidencia del Gobierno, Madrid, 2021.

[797] La relación de España con Marruecos tiene sus peculiaridades como, por ejemplo, la cuestión de la soberanía sobre las ciudades españolas de Ceuta y Melilla: https://en.hespress.com/51054-morocco-has-no-land-borders-with-spain-says-government-assuring-enclaves-are-occupied.html ; la rivalidad en capacidades ofensivas de sus Fuerzas Armadas: https://fr.hespress.com/336631-le-maroc-domine-dans-le-domaine-des-blindes-face-a-lespagne.html y https://www.eldebate.com/espana/defensa/20240113/espana-mantiene-contundente-supremacia-militar-sobre-marruecos_166686.html ; la cuestión del Sáhara: https://aroapress.com/2023/12/22/43166/ ; desencuentros respecto a los límites de las aguas territoriales: https://www.lavanguardia.com/politica/20211124/7886445/espana-protesta-piscifactoria-marroqui.html o la conflictividad en la valla fronteriza de ambas ciudades, entre otras: https://fr.hespress.com/323865-melilla-bruits-de-bottes-pres-de-la-frontiere-marocaine.html (13/01/2024).
Respecto a Argelia, a principios de septiembre de 2024 se une al Nuevo Banco de Desarrollo (NBD) de los BRICS, institución creada para ofrecer una alternativa a los mecanismos financieros internacionales existentes. Esta decisión parece formar parte de una estrategia argelina más amplia para diversificar sus asociaciones económicas y tratar de fortalecer su papel en el escenario global, tras el varapalo que supuso el reconocimiento francés a las tesis marroquíes sobre el Sáhara occidental, y que se sumó a la posición mantenida por EE.UU. y España. Disponible en: https://www.barrons.com/articles/argelia-se-une-al-nuevo-banco-de-desarrollo-de-los-brics-e20f6b6b
https://www.lanacion.com.ar/agencias/argelia-se-une-al-nuevo-banco-de-desarrollo-de-los-brics-nid01092024/
https://www.swissinfo.ch/spa/aprobada-la-membres%C3%ADa-de-argelia-en-el-banco-de-los-brics-un-a%C3%B1o-despu%C3%A9s-de-su-solicitud/87472961 (12/09/2024).

[798] En 2006 se aprobó el Plan África para luchar contra la inmigración irregular, reforzar la presencia institucional española y luchar contra la pobreza como forma de afianzar la paz y la seguridad en el Continente. En 2019 se aprobó el III Plan África y, en 2021, el Foco África 2023 como programa de acción para tratar de dar respuesta al grave deterioro de la situación en el Sahel, con la proliferación de conflictos armados en la zona, el asentamiento de estructuras de crimen organizado que capitalizan los flujos de inmigración irregular y la trata de seres humanos, y el apoyo al terrorismo internacional de carácter yihadista. Disponible en: https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/Africa/III-Plan-%c3%81frica.aspx
https://www.exteriores.gob.es/es/Comunicacion/Noticias/Paginas/Noticias/MICROSITE-FOCO-AFRICA.aspx (12/01/2024).

[799] Estrategia de Seguridad Nacional 2021. Capítulo 2, página 46. Presidencia del Gobierno, Madrid, 2021.

Ediciones Universidad de Salamanca | CC BY-NC-ND

evidente zona de interés para España por "el progresivo desplazamiento del centro de gravedad económico y estratégico mundial"[800] hacia dicha área.

Los *riesgos y amenazas* conforman el tercer capítulo de la ESN 2021, que retorna a la nomenclatura de las dos primeras estrategias, desapareciendo el término *desafíos* que utilizaba la de 2017. Se llama la atención sobre la mayor complejidad técnica de las amenazas que actualmente repercuten en la seguridad nacional y, sobre todo, se resalta el componente híbrido y alto nivel de interrelación que existe entre ellas. Partiendo de estas premisas, destaca como novedad la inclusión por primera vez, como amenaza específica, de las *campañas de desinformación* que, operando desde el ámbito cognitivo, "pretenden distorsionar la realidad mediante contenido manipulado"[801] para generar confusión, minar la cohesión social y tratar de polarizar a la ciudadanía manipulando su opinión, ya sea para guiar su criterio hacia fines interesados o para socavar la credibilidad de las instituciones y afectar a los procesos democráticos.

Tal es la relevancia de esta nueva amenaza desinformativa para la seguridad nacional que, para hacerla frente, se propone una línea de acción -la número 13- relativa a la elaboración de una *Estrategia de segundo nivel específica* desde la que definir el procedimiento de detección, alerta temprana y coordinación de la respuesta, en la que se integre el marco de colaboración público-privada y la estrategia comunicativa orientada a la sensibilización de los ciudadanos ante la gravedad de los posibles efectos que pueden conllevar las campañas de desinformación[802]. Sin embargo, esta propuesta no fraguará hasta tres años después, con la aprobación en enero de 2025 por el CSN del *Acuerdo de elaboración de la Estrategia nacional contra las campañas de desinformación*[803] que, desde una perspectiva integral, aborde los diferentes aspectos de la seguridad nacional que pueden verse afectados por el uso de estrategias híbridas y desinformativas, junto con los riesgos asociados a las últimas tecnologías disruptivas, como la IA generativa.

Íntimamente vinculada a la anterior, la ESN 2021 se refiere también de manera innovadora a las *injerencias desde el exterior* como riesgo con alto componente tecnológico e híbrido como manera de alcanzar objetivos de variada naturaleza que, en conjunto, comparten el interés por la obtención de información sensible, activo estratégico para la seguridad nacional que como tal debe ser protegido.

En este mismo sentido, otra cuestión novedosa que presenta el mapa de riesgos de la ESN 2021 es la consideración del *dato* y de la *seguridad de la información* como nuevos ámbitos de poder e influencia con elevada capacidad de impacto en la seguridad nacional a través, y esta es la cuestión clave, *de su afectación al ciudadano y su esfera de privacidad personal*. Por ello, al analizar la vulnerabilidad del ciberespacio se establece que "la regulación, protección y garantía del uso adecuado de los datos y las

[800] IBIDEM, página 48.
[801] IBIDEM, página 60.
[802] IBIDEM, páginas 81 a 83.
[803] Nota de prensa del DSN sobre el acuerdo del CSN para la elaboración de la Estrategia Nacional contra las Campañas de Desinformación. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-de-prensa/aprobado-procedimiento-elaboracion-estrategia-nacional-campanas-desinfo (31/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

redes por las que transitan es un aspecto clave de la Seguridad Nacional, con impacto directo sobre la privacidad personal"[804].

En relación con las amenazas a las infraestructuras críticas, también muy conectadas con el componente híbrido y tecnológico, merece ser enfatizada la específica referencia que se hace a la "potencial pérdida de control sobre la capacidad de decisión estratégica a raíz de inversiones por actores, estatales o no estatales, con intereses no necesariamente alineados con la Seguridad Nacional", en clara alusión al uso de maniobras híbridas en el plano financiero por actores que, formando parte de estrategias más amplias, buscan posicionarse en sectores clave como medio para alcanzar sus propios objetivos[805].

Finalmente, también merece nuestra atención la ampliación de concepto que supone la referencia que la ESN 2021 hace a la *tensión estratégica y regional* como riesgo de elevado componente híbrido y alta capacidad de impacto en los intereses españoles, superando la mención que todas sus antecesoras hacían a los meros conflictos armados, para dar de esta forma cabida a realidades tan dispares, pero a la vez tan interconectadas, como el repliegue del multilateralismo en favor de la asertividad de los BRICS[806], la feroz rivalidad sistémica entre pretendidos líderes internacionales, los conflictos congelados y aquellos otros de carácter interno no resueltos definitivamente, y la aparición de nuevos dominios de confrontación que están cambiando la tradicional escena de guerra. El resto de los riesgos presentados en la Estrategia son una actualización de los ya analizados en la ESN 2017[807].

Una vez identificados los riesgos y amenazas, en el capítulo cuarto, *un Planeamiento Estratégico Integrado*, la ESN presenta tres objetivos principales que, a su vez, se articulan conforme a *tres ejes estratégicos*:

---

[804] IBIDEM, página 61.

[805] En diciembre de 2023, el Gobierno español aprueba en Consejo de Ministros la adquisición por el Estado de un 10% del capital de Telefónica, como respuesta a la agresiva operación de compra de Saudi Telecom Company que, en septiembre del mismo año, se hizo inicialmente con el 4,9 %, como primer paso para una segunda operación que podría convertirla en el primer accionista de la multinacional española. Disponible en: https://elpais.com/economia/2023-12-19/el-gobierno-aprueba-que-la-sepi-compre-hasta-un-10-de-telefonica.html
https://www.rtve.es/noticias/20230907/stc-compra-acciones-telefonica-planeado-durante-meses/2455402.shtml
https://theobjective.com/economia/2023-09-05/principal-operador-arabia-saudi-telefonica/
(11/01/2024).

[806] Los BRICS representan un foro político y económico que desafía al poder tradicional representado por el G7, y está conformado inicialmente por los cinco países emergentes con mayor potencial, Brasil, Rusia, India, China y Sudáfrica. Además coincide con ser los países más grandes y más poblados del mundo, y con enormes recursos naturales. Disponible en: https://datosmacro.expansion.com/paises/grupos/brics (11/01/2024).

[807] El mapa de riesgos de la ESN 2021 lo conforman los siguientes: 1) tensión estratégica y regional; 2) terrorismo y radicalización violenta; 3) epidemias y pandemias; 4) amenazas a infraestructuras críticas; 5) emergencias y catástrofes; 6) espionaje e injerencias desde el exterior; 7) campañas de desinformación; 8) vulnerabilidad del ciberespacio; 9) vulnerabilidad del espacio marítimo; 10) vulnerabilidad aeroespacial; 11) inestabilidad económica y financiera; 12) crimen organizado y delincuencia grave; 13) flujos migratorios irregulares; 14) vulnerabilidad energética; 15) proliferación de armas de destrucción masiva; 16) efectos del cambio climático y de la degradación del medio natural.

Ediciones Universidad de Salamanca | CC BY-NC-ND

1. La definición de un *modelo de gestión de crisis*, caracterizado por la visión preventiva y la alerta temprana que permitan una gestión anticipativa de la amenaza, para lo cual se apuesta, en el ámbito interno, por la gobernanza en corresponsabilidad con las Comunidades Autónomas y, en el plano supranacional, por la cooperación y la puesta en común de bases de datos de información relevante para poder llevar a cabo la valoración de riesgos de acuerdo a parámetros estandarizados en el marco de la UE. En este mismo sentido, se busca fomentar la colaboración con los proveedores de servicios de tecnología clave, enfocada a tratar de identificar e interrumpir la acción de los ciberdelincuentes antes de que comprometan la seguridad de las redes y los sistemas críticos. Merece destacada mención en este apartado la consideración del dato como base de la protección y de la gestión de la información para generar inteligencia con posterior aprovechamiento operativo.
2. *Incorporar la dimensión de seguridad al desarrollo tecnológico*, apoyando la adaptación tanto de las instituciones públicas como de la industria y la empresa privada nacional a través del fomento de la I+D+i, generando sinergias con el legislador para dar cobertura a la innovación aplicada a la seguridad que, en conjunto, coadyuve a la recuperación de la soberanía digital de España y, por ende, de Europa. Es esta una importante novedad respecto a anteriores estrategias, por cuanto considera la amenaza como un factor dinámico e interrelacionado con múltiples facetas entre las que se incluye la tecnología y todo su proceso de I+D+i como proceso enmarcado en la esencia de la defensa de un Estado, que no es otra que su soberanía.
3. El desarrollo de capacidades de prevención, disuasión, detección y respuesta frente a las *estrategias híbridas* que, independientemente de su origen estatal o no estatal, buscan las grietas y el enfrentamiento ideológico subyacente en el discurso social para, mediante acciones coordinadas y multidimensionales que pueden incluir campañas de desinformación, ciberataques, espionaje, subversión social, sabotaje, coacción económica o el uso asimétrico de medios militares entre otros, desestabilizar a las democracias o desacreditar sus instituciones.

Posteriormente, las *líneas de acción* de la Política de Seguridad Nacional se organizan en torno a tres grandes ejes -proteger, promover, participar- que, no por casualidad, se complementan con el enfoque amplio de la libertad que forma parte del concepto integral de la *seguridad humana*. El primero de ellos es el que garantiza la libertad para vivir sin miedo y con dignidad a través de la *protección de la vida, los derechos y libertades de las personas y del orden constitucional*. A continuación, la perspectiva económica de la seguridad que "consiste en la prevención y evitación de todas las situaciones que pueden interrumpir la vida tanto de empresas como del Estado" (DÍAZ FERNÁNDEZ A. M., 2013, pág. 58) y que se presenta a través del compromiso para *promover la prosperidad y el bienestar de los ciudadanos* como valedores de la libertad frente a la pobreza, lo cual contribuye a sostener el poder del Estado. Finalmente, la voluntad de *participar en la preservación de un orden internacional de paz y buen gobierno* como único marco de actuación en el que hacer viable este planeamiento estratégico integrado que no pierde de vista su vocación europeísta y global.

Ediciones Universidad de Salamanca | CC BY-NC-ND

El quinto y último capítulo, *el Sistema de Seguridad Nacional y la gestión de crisis*, presenta la estructura de funcionamiento del SSN y define un modelo de gestión integral de crisis basado en el compromiso de todas las administraciones junto con la sociedad civil, y en la *resiliencia* como una de sus claves de garantía de resistencia, transformación y recuperación ante una crisis. Para ello propone cinco iniciativas: la elaboración de un catálogo dinámico de recursos estratégicos del Estado y las Comunidades Autónomas a disposición del Gobierno –que en 2025 aún no se ha llevado a efecto-, la elaboración de planes de contingencia para actuar conforme a los informes de riesgo, la activación de un Sistema de Alerta Temprana como apoyo a la toma de decisiones en base a indicadores y datos objetivos, la integración de la información en un sistema de inteligencia avanzado que permita el análisis de grandes volúmenes de datos, el desarrollo de una red securizada de comunicaciones especiales de la Presidencia del Gobierno y la integración de las Comunidades y Ciudades Autónomas en el mismo.

Conforme a todo lo analizado, podemos concluir que la ESN 2021 trata de ofrecer una respuesta proactiva y solidaria ante los riesgos y amenazas provenientes de un entorno global altamente cambiante, tecnificado e hiperconectado donde la defensa de los valores democráticos, el respeto innegociable de los derechos humanos y la consecución de la paz internacional constituyen un objetivo principal que trasciende fronteras. Sin duda, el valor de esta Estrategia es el aporte de un enfoque novedoso en lo relacionado con el análisis de las amenazas, más completo que el de sus antecesoras, por la incorporación de tres variables en su tratamiento: la interconexión entre ellas, la influencia de la tecnología y el predominio de las estrategias híbridas.

Con todo, el incierto y cambiante contexto mundial hace que esta Estrategia, como la de cualquier otro Estado democrático occidental, se vea afectada y requiera, más pronto que tarde, una revisión para readaptarse a la dinámica propia de esta tercera década del siglo XXI. La invasión rusa de Ucrania y la consiguiente reactivación de la estrategia de defensa común europea, el inesperado giro en la política exterior de EE.UU. a partir de la reelección de Donald Trump como Presidente decidido a cambiar el planteamiento de sus alianzas, la escalada nuclear de países como Corea e Irán, el conflicto israelí palestino y la inestabilidad en el Golfo de Adén, o los efectos en cascada tras la pandemia del COVID 19 sobre el comercio mundial, son algunos ejemplos de esa incertidumbre generada por los acontecimientos que, íntimamente conectados, desafían día a día al orden internacional y al multilateralismo que, durante décadas, lo ha soportado. El tiempo determinará el nivel de acierto de la visión proyectada por la ESN 2021 que, en cualquier caso, deberá ser revisada próximamente por la rapidez y profundo calado de estos cambios.

4.5. Los ámbitos de interés de la Seguridad Nacional y su desarrollo normativo de segundo nivel

Una vez estudiada la vigente ESN 2021 debemos avanzar en el camino hacia la ratificación de nuestra hipótesis de trabajo, en la que la *desinformación* se muestra como una grave amenaza a la seguridad nacional, y para ello debemos comenzar a descender hacia niveles tácticos y operacionales que son los que, en definitiva, representan la materialización de los objetivos definidos en el marco estratégico. En este

Ediciones Universidad de Salamanca | CC BY-NC-ND

sentido, por ejemplo, es clarificadora la distinción que el profesor Colom Piella hace entre las *estrategias de seguridad nacional* y las *directivas de defensa nacional*, advirtiendo que:

> "[…] mientras las primeras fijan un marco general de la seguridad nacional que el Ministerio de Defensa debería transformar en una hipotética Estrategia de Defensa Nacional que informara el planeamiento futuro, las segundas establecen prioridades para el corto plazo que condicionan la presupuestación, pero no informan el desarrollo de capacidades en el largo" (COLOM PIELLA, 2021, pág. 8).

De esta forma, para construir de manera coherente el marco de respuesta integral ante los riesgos y amenazas, "la ESN facilita el desarrollo de las estrategias de segundo y tercer nivel alineándolas para que persigan los mismos objetivos estratégicos de modo que se aprovechen las sinergias" (BALLESTEROS MARTÍN M. A., 2016, pág. 18), constituyendo todas ellas el marco político-estratégico de referencia inmediata en cada uno de los *ámbitos de especial interé*s definidos para la seguridad nacional, a través de los que se desarrollan los objetivos a alcanzar y las líneas de acción desde las que construir la adecuada respuesta frente a los riesgos y amenazas concretas identificadas.

Así, actualmente existen siete estrategias de segundo nivel incardinadas en el marco de los *ámbitos de especial interés* del artículo 10 LSN 2015, los cuales "requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales"[808]. Conforme a ello, en las ESN 2017 y 2021, estos *ámbitos de especial interés* son fijados como objetivos para cuya consecución se establecen *líneas de acción* que han de ser desarrolladas por las *estrategias de segundo nivel*, correspondientes con los tres espacios comunes globales –marítimo, aeroespacial y ciberespacio-, el sector energético, el crimen organizado y la delincuencia grave, la protección civil y el terrorismo.

A estas siete estrategias de segundo nivel se une en enero de 2025 la apertura del procedimiento de elaboración de la *Estrategia nacional contra las Campañas de Desinformación*, por acuerdo del CSN[809] conforme a lo establecido en la ESN 2021, en su línea de acción número 13, y la propuesta recogida en el *Plan de Acción por la Democracia*[810], de septiembre de 2024, para establecer treinta y una medidas de mejora de la transparencia y la rendición de cuentas del *Gobierno*, de los *medios de comunicación* y del *poder legislativo*, entre las que dos de ellas corresponden expresamente al ámbito de la amenaza desinformativa: la aprobación de una Estrategia

[808] Artículo 10 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

[809] Orden PJC/248/2025, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 28 de enero de 2025, por el que se aprueba el procedimiento para la elaboración de la Estrategia Nacional contra las Campañas de Desinformación. BOE núm. 64, de 15 de marzo de 2025. BOE-A-2025-5151. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151 (17/03/2025).

[810] Esta propuesta del *Plan de Acción por la Democracia*, presentada oficialmente el 17 de septiembre de 2024, se analiza específicamente en el Capítulo 8, apartado 8.1.4. Disponible en: https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (04/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Nacional de lucha contra las campañas de desinformación, y la creación de una nueva comisión en el Congreso de los Diputados sobre desinformación.



Gráfico 4.2.
Pirámide normativa
Fuente: propia

Como puede verse en el gráfico 4.2., por ejemplo para el caso del ciberespacio, la pirámide normativa que da soporte legal a la respuesta de seguridad tendría en la estructura de la UE el primer nivel en el que se definen los grandes desafíos comunes en ese ámbito de interés, en este caso la Estrategia Europea de Ciberseguridad para la Década Digital[811], cuyas líneas de acción serán adaptadas por cada EEMM en sus estrategias nacionales, en el ejemplo la Estrategia Nacional de Ciberseguridad[812], que adquiere concreción a través de actuaciones específicas de los órganos de gobierno afectados, como el Plan Estratégico contra la Cibercriminalidad de la Secretaría de Estado de Seguridad del Ministerio del Interior[813] que, finalmente, se ejecuta mediante el Plan Operativo contra la Cibercriminalidad de la Policía Nacional.

Todas estas normas de segundo nivel ponen de manifiesto la relevancia de los *ámbitos de especial interés* que señala la LSN 2015 y dan consistencia a la estructura de respuesta y capacidad de resiliencia frente a los desafíos que conllevan, vertebrada en torno al SSN que, a través de sus Comités Especializados, logra la capilaridad que le permite llegar a cada uno de ellos con líneas de actuación específicas, actualizadas y adaptadas a la amenaza concreta que cada uno de ellos atiende.

[811] Estrategia Europea de Ciberseguridad para la Década Digital. Comisión Europea y Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 16 de diciembre de 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (17/01/2024).

[812] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

[813] No disponible en fuentes abiertas. Puede consultarse la nota de prensa de La Moncloa sobre la Instrucción 1/2021, del Secretario de Estado de Seguridad, por la que se aprueba el Plan Estratégico contra la Cibercriminalidad.

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.5.1. La Estrategia de Seguridad Marítima Nacional

La primera de estas normas de segundo nivel es la Estrategia de Seguridad Marítima Nacional (ESMN), aprobada en 2013[814] para desarrollar las previsiones de la ESN de ese mismo año y adaptarlas a las singularidades del ámbito marítimo y sus implicaciones para la seguridad, que posteriormente es relevada por la Estrategia Nacional de Seguridad Marítima 2024[815].

La ESMN 2013 contemplaba las ciberamenazas en el ámbito marítimo por cuanto la propia evolución de las TIC las había convertido en elemento transversal y de interconexión multidimensional que, al mismo tiempo, había servido para potenciar el alcance y el volumen de los ciberataques, con especial incidencia contra estructuras esenciales para el normal desenvolvimiento de la actividad propia de este medio –sistemas de vigilancia y control, infraestructuras marítimas críticas, sistemas de comunicación y navegación-[816]. Por ello, se definía una línea de acción orientada a la mejora de la ciberseguridad desde un enfoque integral con el objetivo de contribuir "a la mejora de los estándares de seguridad marítima nacional"[817]. Como principal novedad se incluía la creación del Comité Especializado de Seguridad Marítima que, en 2018, pasó a denominarse Consejo Nacional de Seguridad Marítima[818].

En junio de 2022 el CSN adopta un Acuerdo en el que se aprueba el procedimiento para elaborar una nueva ESMN[819] ante la necesidad de adaptarla a los cambios producidos en el contexto estratégico global, como son la mayor incertidumbre en la seguridad de las rutas marítimas, la creciente importancia y vulnerabilidad de las infraestructuras críticas marinas, la fragilidad de la cadena de custodia global, y la transformación digital aplicada a las comunicaciones y sistemas marinos, así como para adaptarla a la nueva Estrategia de Seguridad Marítima de la UE de 2023[820] que, alineada con la Brújula Estratégica para la Seguridad y la Defensa, pretende convertir a la UE "en un proveedor de seguridad marítima a nivel global" (ROMERO JUNQUERA, 2023, pág. 3). Finalmente,

---

[814] Estrategia de Seguridad Marítima Nacional 2013. Resumen Ejecutivo, página 4. Presidencia del Gobierno, Madrid, 2013. Disponible en: https://www.dsn.gob.es/en/node/23415 (14/01/2024).

[815] Orden PJC/501/2024, de 27 de mayo, por la que se publica la Estrategia Nacional de Seguridad Marítima 2024, aprobada por el Consejo de Seguridad Nacional. BOE número 130, de 29 de mayo de 2024 (BOE-A-2024-10762). Disponible en: https://www.boe.es/eli/es/o/2024/05/27/pjc501 (24/01/2025).

[816] IBIDEM, página 28.

[817] IBIDEM, página 40.

[818] Orden PRA/34/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Seguridad Marítima. BOE número 20, de fecha 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-800.pdf (26/12/2023).

[819] Orden PCM/720/2022, de 23 de julio, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 21 de junio de 2022, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia de Seguridad Marítima Nacional. BOE núm. 180, de 28 de julio de 2022. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-12627 (14/01/2024).

[820] Comunicación Conjunta al Parlamento Europeo y al Consejo relativa a la actualización de la Estrategia de Seguridad Marítima de la UE y su Plan de Acción «Una Estrategia de Seguridad Marítima de la UE reforzada para hacer frente a unas amenazas marítimas cambiantes». Bruselas 10/03/2023. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:9e3d4557-bf39-11ed-8912-01aa75ed71a1.0006.02/DOC_1&format=PDF (14/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

el 19 de marzo de 2024, el CSN aprueba la Estrategia Nacional de Seguridad Marítima 2024, que muestra a España como país de condición marítima y a este dominio como espacio común global de importancia estratégica.

Asimismo, define la seguridad marítima como "la combinación de medidas preventivas y de respuesta orientadas tanto a proteger el entorno marítimo de amenazas y actos ilegales intencionados, como a limitar los efectos de peligros naturales, de accidentes y daños al medio ambiente, las actividades económicas y a las personas"[821], con una visión proactiva hacia la mar que, por un lado, pone en valor la fuerte vinculación de la economía del país con este dominio en aspectos claves como el turismo, la pesca o la industria naval, y por otro, se muestra conocedora de que se trata de un área propicia para la materialización de gran parte de las amenazas reflejadas en la ESN 2021. En este contexto de alta competición geoestratégica se define como pieza determinante la mejora de la *resiliencia* de los puertos, las infraestructuras marítimas y energéticas, así como de las actividades económicas que de ellas dependen[822].

En ese mismo sentido, se distingue el componente de seguridad vinculado a las amenazas —"actos deliberados o de naturaleza ilícita que pueda poner en peligro la seguridad"[823]— y el de protección, relacionado con los riesgos –"aquellos incidentes no intencionados, como consecuencia de accidentes o de los efectos de la naturaleza"[824]-.

Dentro del apartado dedicado a las amenazas contra los intereses nacionales en el ámbito marítimo adquieren especial relevancia las estrategias híbridas que, en relación con el alto nivel tecnológico implicado en este dominio, se materializan en ejemplos como los actos de sabotaje a gasoductos o infraestructuras de cables submarinos, determinadas acciones asertivas por parte de flotas mercantes y de pesca de determinados países, sabotajes y ciberataques contra buques o su toma de control remota y, también, en el posible uso hostil de la migración irregular contra España por parte de terceros Estados interesados, ya sea de manera directa o por delegación a través de estructuras criminales interpuestas.

Finalmente, concluir señalando que este complejo panorama de amenazas y riesgos hace que la Estrategia Nacional de Seguridad Marítima se marque tres objetivos principales: 1) la protección de España "en" y "desde" la mar; 2) la mejora de sus capacidades en este entorno; 3) y la contribución a un océano más seguro[825] en el marco

[821] Estrategia Nacional de Seguridad Marítima 2024, Op. Cit. Página 61923.
[822] IBIDEM, página 61933.
[823] IBIDEM, página 61929.
[824] IBIDEM, página 61929.
[825] IBIDEM, página 61922.

Ediciones Universidad de Salamanca | CC BY-NC-ND

del Tratado de Alta Mar de NNUU, firmado por la UE en septiembre de 2023[826], y la Convención de las NNUU sobre el Derecho del Mar, de 1982[827].

4.5.2. La Estrategia de Seguridad Energética Nacional

En segundo lugar, por orden cronológico, hay que citar la Estrategia de Seguridad Energética Nacional (ESEN) de 2015, actualmente en vigor, que desarrolla las líneas de actuación marcadas por la ESN 2013 por las que "la energía es un componente fundamental de la prosperidad, el crecimiento económico y bienestar de la sociedad, así como de la propia soberanía y continuidad del Estado"[828], cuya seguridad pasa por garantizar el suministro a través del abastecimiento exterior y la generación de recursos propios, resultando vital para ello que la sociedad esté concienciada de la importancia de preservar y proteger las fuentes de energía que mantienen activo al país.

En la ESEN 2015 ya se menciona a Rusia como productor de hidrocarburos de relevancia estratégica y se destaca el hecho de que "la seguridad energética de España sólo se puede entender en el marco de la Unión Europea"[829], referenciándose cuatro vectores clave -el suministro, el abastecimiento, la sostenibilidad económica y la sostenibilidad medioambiental- orientados al objetivo final que pasa por "la diversificación de las fuentes de energía, la garantía de la seguridad del transporte y abastecimiento y el impulso de la sostenibilidad energética"[830], así como por la resiliencia de las infraestructuras TIC que dan soporte al sector energético, para garantizar la continuidad al suministro de energía[831].

Tratándose de un marco como el de la energía, la ESEN 2015 necesita una renovación urgente no solo por su falta de alineación con la ESN 2021 sino, también, por la evidente separación que existe entre sus postulados de origen y el actual panorama geoestratégico, que ha evolucionado grandemente no solo por las derivadas de conflictos como el de Ucrania, que ha obligado a reconsiderar la política energética de toda la UE, sino por la propia evolución tecnológica, que diez años después permite nuevas perspectivas en la estrategia de los suministros esenciales.

Con todo, la ESEN 2015 nació adelantada a su tiempo y ya contempla la amenaza desde la doble dimensión -física y ciber- con la que puede aprovecharse de la vulnerabilidad

---

[826] Decisión (UE) 2023/1974 del Consejo de 18 de septiembre de 2023 relativa a la firma, en nombre de la Unión Europea, del Acuerdo en el marco de la Convención de las Naciones Unidas sobre el Derecho del Mar relativo a la conservación y el uso sostenible de la diversidad biológica marina de las zonas situadas fuera de la jurisdicción nacional. DOUE núm. 235, de 25 de septiembre de 2023, páginas 1 a 3. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81321 (20/03/2024).

[827] Convención de las NNUU sobre el Derecho del Mar, de 1982. Disponible en: https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf (20/03/2024).

[828] Estrategia de Seguridad Energética Nacional 2015. Presentación, página II. Presidencia del Gobierno, Madrid, 2015. Disponible en: https://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20seguridad%20energetica%20nacional.pdf (14/01/2024).

[829] IBIDEM, página 2.

[830] IBIDEM, página 3.

[831] IBIDEM, página 41.

Ediciones Universidad de Salamanca | CC BY-NC-ND

de las infraestructuras críticas para causar ataques que provoquen "la pérdida de control sobre dichos sistemas o la emisión de mensajes erróneos en la operación, que, a su vez, pueden ocasionar fallos o accidentes técnicos"[832]. Un ataque de este tipo podría ser considerado catastrófico por su impacto directo en las redes de servicios críticos - sistema de salud y atención sanitaria, telecomunicaciones, acceso a Internet, gestión del agua potable y residual, acceso a combustibles, etc.- que conllevan una interrupción grave y generalizada de la provisión de servicios públicos con los consiguientes efectos para el desarrollo económico del país, el normal desempeño de las actividades industriales y el mantenimiento de la calidad de vida de los ciudadanos.

Finalmente, en cuanto a estructura, la ESEN introduce la figura del Comité Especializado de Seguridad Energética[833] incardinado dentro del marco colaborativo del SSN.

4.5.3. La Estrategia de Seguridad Aeroespacial Nacional

En cuanto a la Estrategia de Seguridad Aeroespacial Nacional (ESAN) de 2019[834], desarrolla las consideraciones vinculadas con la seguridad nacional de la ESN 2017 en el ámbito del espacio aéreo y ultraterrestre, de evidente relevancia para la sociedad moderna altamente tecnificada e interconectada que no concibe el actual modelo de vida sin el soporte de este sector vertebrador de la economía, la industria, la ciencia, la tecnología y el poder militar de un Estado.

Es éste un ámbito en el que las amenazas se desarrollan a gran velocidad, con facilidad de expansión por la ausencia de fronteras geográficas y disponen de un contexto tecnológico multiplicador que determinan tiempos de reacción muy cortos y la necesidad de contar con el apoyo de sistemas de mando y control de altas capacidades para gestionar la información y poder tomar decisiones acertadas. Los servicios que tienen su base en las comunicaciones por satélite son parte de la infraestructura esencial del país[835], de forma que un ciberataque a cualquiera de ellas supone una grave amenaza, como por ejemplo los servicios de posicionamiento, navegación y temporización, elementos clave para las telecomunicaciones, la navegación, el

[832] IBIDEM, página 33.

[833] Órgano de apoyo al CSN regulado por Acuerdo de 1 de diciembre de 2017 y publicado por la Orden PRA/30/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se crea y regula el Comité Especializado de Seguridad Energética. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-796.pdf (27/12/2023).

[834] Orden PCI/489/2019, de 26 de abril por la que se publica la Estrategia de Seguridad Aeroespacial Nacional, aprobada por el Consejo de Seguridad Nacional. Disponible en: https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Aeroespacial%202019%20Interactiva.pdf (15/01/2024).

[835] Baste citar como ejemplo la construcción y lanzamiento en 2025 de los satélites de nueva generación SpainSat NG I y II, para dotar de comunicaciones seguras a las Fuerzas Armadas españolas y sus aliados mediante el apoyo a la cadena de mando en sus operativos de defensa. Al tratarse de tecnología de doble uso, también dará servicio al ámbito civil. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5082017/despegue-satelite-comunicaciones-spainsat-ng-i-llevara-cabo-entre-enero-febrero-2025
https://www.europapress.es/nacional/noticia-satelite-militar-spainsat-pasa-ultimas-pruebas-cara-ponerse-orbita-principios-2025-20241124110003.html (24/11/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

transporte y la disposición de unidades de tiempo precisas. Pero la ESAN 2019 no solo se refiere a la amenaza proveniente del ciberespacio sino, también, a la que deriva de los propios conflictos armados, del terrorismo, del crimen organizado, de la proliferación de armas de destrucción masiva o del espionaje, y de los desafíos consustanciales a las emergencias y catástrofes, las epidemias y pandemias o la contaminación atmosférica.

Todas estas facetas le confieren al dominio ultraterrestre un carácter estratégico, por cuanto un ataque a las infraestructuras que soporta tendría un efecto inmediato y generalizado en el resto de dominios físicos y virtuales. Por ello:

> "El sector aeroespacial está altamente tecnificado e intrínsecamente vinculado al dominio cibernético y constituye un objetivo de alto valor estratégico. Cuenta con un gran componente tecnológico de avanzados sistemas de información y telecomunicaciones aislados o integrados en redes, que se distribuyen globalmente y dan servicio a un complejo entramado de centros de seguimiento y control, radares, comunicaciones digitales de voz y datos, aeronaves y sus sistemas a bordo, y diversas instalaciones aeroportuarias. El componente espacial de este ámbito contiene infraestructuras como estaciones de control y seguimiento de satélites, centros de operaciones para vigilancia espacial, centros de comunicaciones y de procesado de datos espaciales, con un elevadísimo grado de interconexión cibernética"[836].

Desde el espacio se da soporte a múltiples servicios que forman parte de la infraestructura crítica del país, desde las comunicaciones por satélite hasta la tecnología utilizada para el seguimiento y pronóstico del tiempo, pasando por los sistemas de geoposicionamiento y navegación global. Es así que los ciberataques con afectación a estas infraestructuras aeroespaciales se consideren de *máxima rentabilidad*, por cuanto sus objetivos son muy diversos y de diferente alcance: modificación o exfiltración de la información de bases de datos sensibles, alteración del tráfico aéreo, ataques disruptivos contra los sistemas embarcados o de control de tierra, accesos no autorizados a infraestructuras de comunicaciones espaciales, sistemas de medición exacta del tiempo, entre otros.

En consonancia con este alto valor estratégico de la seguridad aeroespacial, la ESAN 2019 señala expresamente que le son plenamente aplicables los cuatro principios rectores definidos en la ESN 2017 -unidad de acción, anticipación, eficiencia y resiliencia- a partir de los cuales asegurar la disponibilidad de los elementos esenciales para la seguridad de la nación, tanto en su dimensión interna como en la exterior, como dominio clave en la coordinación para arbitrar una respuesta efectiva con sus aliados[837].

Para concluir, indicar que la estructura de seguridad en este dominio se incardina en el SSN a través del Consejo Nacional de Seguridad Aeroespacial, regulado por Acuerdo de 4 de marzo de 2020[838].

---

[836] Estrategia de Seguridad Aeroespacial Nacional, Op. Cit. Página 49.

[837] IBIDEM, páginas 59 y 60.

[838] Publicado por la Orden PCM/218/2020, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se crea y regula el Consejo Nacional de Seguridad Aeroespacial, para dar cumplimiento a lo establecido en el Capítulo 4 de la Estrategia de Seguridad Aeroespacial Nacional de

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.5.4. La Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave

En cuarto lugar, la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023 (ENCODG)[839] que, en el marco de las líneas definidas por la ESN 2017, actualiza la anterior Estrategia Nacional contra el Crimen Organizado 2011-2014 por los cambios sucedidos en el perfil delictivo ligados al uso de la tecnología, la transnacionalidad de las estructuras criminales y la interacción con otros fenómenos "como los conflictos armados, el terrorismo, la proliferación de armas de destrucción masiva, el espionaje, los ciberdelitos y las amenazas sobre las infraestructuras críticas"[840], que se retroalimentan como factores potenciadores de la amenaza que ya de por sí suponen y aumentan la vulnerabilidad del entorno en que se desenvuelven.

En este línea, la ESN 2017 califica como amenaza a la seguridad nacional la vulnerabilidad del ciberespacio por cuanto los índices de ciberdelincuencia definen una gráfica ascendente año tras año "generando una inseguridad social difícil de minimizar en términos de amenaza a largo plazo"[841] que determinan la necesidad de definir líneas de acción específicas para combatir esta cibercriminalidad como el control de los criptoactivos como medios de pago y el favorecimiento de las investigaciones financieras, la potenciación de la formación de especialistas en los Cuerpos Policiales para aumentar la eficacia de las investigaciones en este campo, mejorar la colaboración de las unidades especializadas contra el crimen organizado con especial atención a las investigaciones transfronterizas, o mejorar la calidad de la información y la inteligencia generada para focalizar la actividad policial en los ciberdelitos con mayor impacto –fraudes y estafas en Internet, pornografía infantil, extorsiones, comercio ilícito de datos personales, entre otros-. Llama en este sentido la atención cómo la ENCODG vincula la inteligencia, eje troncal de la prevención y anticipación contra la amenaza, con la resiliencia desde un punto de vista de facilitador *ex post facto*, en caso de que no haya funcionado su dimensión preventiva[842].

Se trata con todo ello de mejorar la cooperación policial, fomentar la creación de redes de intercambio de información y aumentar la oferta formativa para las Unidades operativas. Destaca que, en el marco colaborativo del SSN, se asigna al Ministerio del Interior la responsabilidad de mantener actualizada la ENCODG, así como de "la superior

2019, que dispone la creación de un Consejo Nacional de Seguridad Aeroespacial para dar apoyo al CSN en su labor de asistencia al Presidente del Gobierno en lo que en dicho ámbito afecte a la Política de Seguridad Nacional.

[839] Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. BOE núm. 46, de 22 de febrero de 2019. Disponible en: https://www.boe.es/boe/dias/2019/02/22/pdfs/BOE-A-2019-2442.pdf (16/01/2024).

[840] Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023. Resumen Ejecutivo, página 9. Presidencia del Gobierno, Madrid, 2019. Disponible en: https://www.dsn.gob.es/sites/dsn/files/ESTRATEGIA%20ESPA%C3%91OLA%20CRIMEN%20ORGANIZADO%20DG.pdf (16/01/2024).

[841] Estrategia de Seguridad Nacional 2017, Op. Cit., página 24.

[842] Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave, Op. Cit., página 17057.

Ediciones Universidad de Salamanca | CC BY-NC-ND

dirección, impulso y seguimiento de las medidas, los planes y las actuaciones previstas en esta Estrategia"[843].

En este sentido, el CITCO elaborará los informes anuales de Balance sobre Criminalidad Organizada y Delincuencia Grave, y las Direcciones Generales de la Policía y la Guardia Civil establecerán los correspondientes Planes de Acción Operativos con las actuaciones policiales concretas que se deben poner en marcha para alcanzar los objetivos, señalando plazo de ejecución y definiendo indicadores que permitan su seguimiento y evaluación de cumplimiento.

Debido a los profundos y relevantes cambios acaecidos en el contexto global de la criminalidad desde la aprobación de la ENCODG (2019-2023), el CSN acuerda en marzo de 2024 su revisión[844] con el objeto de adaptarla, por un lado, a la ESN 2021 alineada con las prioridades de la Unión en esta materia[845] y, por otro, a la propia evolución de la amenaza, influida por eventos tan perturbadores como la pandemia del COVID-19 y su influjo en la ciberdelincuencia, la invasión rusa de Ucrania y sus concomitancias en el tráfico de armas, la inestabilidad en Oriente Medio, el Magreb y el Sahel con el consiguiente auge de las formas de criminalidad ligadas al tráfico de seres humanos y de sustancias estupefacientes, sin olvidar el exponencial desarrollo de tecnologías con gran potencial disruptivo -IA, 5G, etc.- que siempre van a estar en el punto de mira de las organizaciones criminales para su aprovechamiento. Una muestra de la íntima conexión entre el contexto geopolítico, los conflictos zonales y la seguridad interior, en este caso española, se manifiesta con la operación policial llevada a cabo en noviembre de 2024 en Algeciras y Marbella que acaba con la red de "narcodrones" que operaba entre España y Marruecos[846], fruto de la aplicación a la actividad delincuencial de capacidades técnicas de última generación gestadas con el *know how* obtenido en el terreno del conflicto de Ucrania,, en este caso para el transporte de droga entre ambos países con estos dispositivos que facilitaban la impunidad de los hechos delictivos a través del Estrecho de Gibraltar.

[843] IBIDEM, página 17074.

[844] Orden PJC/327/2024, de 14 de abril, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba una nueva Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. BOE núm. 93, de martes 16 de abril de 2024. Disponible en: https://www.boe.es/boe/dias/2024/04/16/pdfs/BOE-A-2024-7482.pdf (23/04/2024).

[845] Interconexión de las distintas modalidades criminales de la delincuencia grave y organizada, incremento del uso de la violencia, el abuso de estructuras empresariales legales para el aprovechamiento económico del producto del delito y su enriquecimiento ilícito, la afectación institucional a través de la corrupción y la compra de voluntades, la adaptación a nuevos entornos delincuenciales como el ciberespacio, o el aprovechamiento de sus estructuras para multiplicidad de delitos (tráfico de seres humanos, tráfico de drogas, inmigración irregular, tráfico de armas…).

[846] Amplia repercusión en prensa de esta operación de la Policía Nacional. Disponible en: https://www.interior.gob.es/opencms/va/detalle/articulo/La-Policia-Nacional-desmantela-una-red-de-narcodrones-que-operaba-entre-Espana-y-Marruecos/
https://elpais.com/espana/2024-11-28/cae-una-banda-que-usaba-narcodrones-ucranios-para-transportar-hachis-por-el-estrecho.html
https://www.rtve.es/noticias/20241128/desmantelada-algeciras-red-narcodrones-fabricados-ucrania/16350551.shtml (14/12/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

El desarrollo de las TIC y la disrupción tecnológica, junto con las conexiones ventajistas con actores estatales hostiles, son elementos aprovechados por las estructuras de crimen organizado para el favorecimiento de sus actividades, con una repercusión inmediata en la desestabilización de los Estados democráticos. En España, por ejemplo, en diciembre de 2024 se lleva a cabo una operación policial simultánea en cinco países europeos y liderada por EUROPOL[847], que consigue desmantelar la infraestructura de una plataforma de mensajería encriptada -*Matrix*- utilizada por la Mocro Mafia para asegurar las comunicaciones vinculadas a sus actividades de narcotráfico, blanqueo de capitales y tráfico de armas, poniendo de manifiesto la potenciación de las capacidades de estos grupos criminales como desafío a la seguridad interior de los Estados.

4.5.5. La Estrategia Nacional de Protección Civil

La quinta estrategia de segundo nivel a la que debemos referirnos es la Estrategia Nacional de Protección Civil (ENPC) de diciembre de 2024[848], cuyo objetivo es dar respuesta y asegurar la protección de los ciudadanos ante los fenómenos meteorológicos extremos que, en un mundo cada vez más global, tecnológico e interconectado que genera un elevado nivel de interdependencia entre territorios y personas, convierte los riesgos en complejos procesos con consecuencias que superan fronteras. Para ello apuesta por reforzar el Sistema Nacional de Protección Civil, la cooperación y cooperación entre los distintos niveles de la Administración, la puesta en marcha del Mecanismo Nacional de Respuesta, la utilización de los avances de la tecnología y la formación permanente de sus integrantes.

Al igual que su antecesora de 2019, la actual ENPC lleva a cabo un análisis de "las principales amenazas y riesgos de origen natural, humano y tecnológico que pueden dar lugar a emergencias y/o catástrofes en nuestro país, así como las líneas de acción estratégicas para integrar, priorizar y coordinar todos los esfuerzos que permitan optimizar los recursos disponibles para su gestión"[849], en línea con lo establecido en la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil que, siendo parte integrante del SSN, ordena las políticas públicas referidas a las emergencias, con un enfoque vinculado a la *seguridad humana* donde el ciudadano es el elemento central de la acción y que incorpora como factores potenciadores del riesgo todos sus condicionantes sociales, económicos o personales que pueden llevarle a una situación de especial vulnerabilidad ante la amenaza proveniente de una emergencia o catástrofe.

---

[847] Esta operación ejecutada en España por la Policía Nacional tiene amplia repercusión en prensa. Disponible en: https://elpais.com/espana/2024-12-03/cae-matrix-un-servicio-de-comunicacion-encriptada-que-utilizaban-la-mocro-maffia-y-otras-organizaciones-criminales.html https://www.larazon.es/espana/policia-desmantela-sistema-mensajeria-encriptada-matrix-utilizado-delincuentes_20241203674f07c31258380001f2cbe1.html https://es.euronews.com/next/2024/12/05/europol-desmantela-matrix-un-servicio-de-mensajeria-encriptada-creado-por-y-para-el-crimen (14/12/2024).

[848] Orden PJC/1430/2024, de 16 de diciembre, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 15 de octubre de 2024, por el que se aprueba la Estrategia Nacional de Protección Civil. BOE núm. 304, de 18 de diciembre de 2024. Disponible en: https://www.boe.es/eli/es/o/2024/12/16/pjc1430 (12/01/2025).

[849] IBIDEM, página 173936.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Se diseña de esta manera un elemento integrador e integrado en el marco de la cultura de seguridad nacional, donde las conductas de autoprotección y de resiliencia de la sociedad adquieren carácter esencial[850], en sintonía con los Objetivos de resiliencia de la Unión ante catástrofes[851].

En este contexto, la emergencia provocada por la DANA que castigó la comarca de l'Horta Sud de Valencia la noche del 29 de octubre de 2024, no hace sino poner énfasis en el impacto que este tipo de catástrofes tiene en la vida y la seguridad de las personas. Por ello, esta ENPC 2024 avanza en la identificación de las inundaciones, los incendios forestales, las erupciones volcánicas, los terremotos y maremotos como algunos de los principales riesgos y amenazas para la seguridad nacional.

4.5.6. La Estrategia Nacional Contra el Terrorismo

La Estrategia Nacional Contra el Terrorismo (ENCOT) conforma el marco político-estratégico de la lucha contra el terrorismo y el extremismo violento dentro de la estructura del SSN.

La ENCOT 2023[852], aprobada por el CSN el 19 de marzo de 2024, actualiza la anterior ENCOT de 2019 para adecuarse al nuevo contexto de la amenaza, caracterizado por:

1. La propia evolución de las tácticas vinculadas a un terrorismo de carácter eminentemente yihadista[853], altamente tecnificado en sus procedimientos -operativos, de comunicación, captación y reclutamiento-, con una estructura cada vez más descentralizada y difusa que apuesta por los actores solitarios y la focalización hacia los denominados *objetivos blandos,* de fácil acceso y elevada potencialidad de víctimas –concentraciones de personas en vía pública, medios de transporte colectivo, celebraciones multitudinarias, lugares de culto-[854].
2. El empleo de la propaganda a través de las nuevas tecnologías como elemento clave de la estrategia terrorista para radicalizar a sus seguidores y lanzar un mensaje extremista que les induzca a pasar a la acción. Con este objetivo aprovechan nuevos desarrollos de encriptación que fortalecen la seguridad de sus comunicaciones, usan la IA para el diseño de su narrativa proselitista, y gestionan su imagen desde las redes sociales[855] para consolidar su presencia en el ciberespacio y amplificar su alcance a nivel global[856].

---

[850] IBIDEM, página 173937.

[851] Recomendación de la Comisión de 8 de febrero de 2023 sobre los objetivos de resiliencia de la Unión ante catástrofes. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-Z-2023-70010 (12/01/2025).

[852] Orden PJC/406/2024, de 7 de mayo, por la que se publica la Estrategia Nacional contra el Terrorismo 2023, aprobada por el Consejo de Seguridad Nacional. BOE núm. 112, de 8 de mayo de 2024. Referencia BOE-A-2024-9149. Disponible en: https://www.boe.es/eli/es/o/2024/05/07/pjc406 (20/03/2024).

[853] Esta amenaza terrorista de carácter yihadista proviene fundamentalmente de DAESH y Al Qaeda, tal y como señala la ENCOT 2023 al referirse al marco geoestratégico.

[854] IBIDEM, páginas 13, 14, 15 y 29.

[855] En este sentido se considera prioritaria la definición de una línea de actuación para contrarrestar la narrativa terrorista o radical en las redes sociales, junto con la retirada de sus contenidos en colaboración con las plataformas de servicios.

[856] Estrategia Nacional contra el Terrorismo 2023, Op. CIt. Página 51510.

Ediciones Universidad de Salamanca | CC BY-NC-ND

3. Los cambios acaecidos en el marco geoestratégico de España como país europeo, mediterráneo y atlántico, donde permanece vigente la intención de atentar de DAESH y Al Qaeda con el posible apoyo de Combatientes Terroristas Extranjeros retornados[857], al tiempo que se complica la situación en las zonas de influencia, principalmente el Sahel, el Cuerno de África y el Golfo de Guinea, donde las citadas organizaciones terroristas están asentándose aprovechando las posibilidades de recursos y de financiación que ofrecen, así como el apoyo brindado por estructuras de crimen organizado dedicadas al tráfico de personas, que pueden facilitarles la entrada a Europa[858].

Por todo ello, la ENCOT 2023 considera que "el terrorismo, en todas sus formas y manifestaciones, es una de las mayores amenazas para España y sus ciudadanos, dado su carácter asimétrico y transnacional"[859], por lo que representa un desafío multifacético que requiere una respuesta coordinada a todos los niveles en el ámbito interno, basada en la cooperación internacional como parte del enfoque global , y con una apuesta firme y decidida por el intercambio de información entre los actores intervinientes, la inversión en capacidades tecnológicas que permitan afrontar con garantías de éxito la amenaza, la actuación profunda en frentes como el penitenciario o el tratamiento psicosocial de determinadas franjas de población, el apoyo a las víctimas y, desde luego, el compromiso y la implicación de todo el espectro político y social para lograr la unidad de acción frente al terrorismo.

Este enfoque nacional está en consonancia con el Convenio Europeo para la Represión del Terrorismo[860] y su complemento, el Convenio del Consejo de Europa para la Prevención del Terrorismo[861], conforme a los cuales los delitos terroristas no pueden considerarse delitos políticos o inspirados por motivos políticos[862].

[857] Estos terroristas suponen una clara amenaza para la seguridad nacional por cuanto su estancia en zonas de conflicto les ha dotado de una experiencia operativa y de una serie de conocimientos sobre armas, explosivos y otro tipo de facilitadores que les convierte en verdaderos ejes vertebradores de las capacidades de DAESH y Al Qaeda tanto para la consecución de atentados complejos como para el reclutamiento y liderazgo de grupos radicalizados.

[858] Estrategia Nacional contra el Terrorismo 2023, Op. CIt. Página 51513.

[859] Esta referencia es prácticamente una copia literal del punto 10 del Concepto Estratégico de la OTAN, aprobado en Madrid en junio de 2022. Estrategia Nacional contra el Terrorismo 2023, Op. CIt. Página 51509.

[860] El Convenio Europeo para la Represión del Terrorismo, de fecha 27 de enero de 1977, fue ratificado por España el 9 de mayo de 1980, publicado en BOE 242, de 8 de octubre de 1980, páginas 22357 a 22360. Disponible en: https://www.boe.es/eli/es/ai/1977/01/27/(2) (22/03/2024).

[861] Convenio del Consejo de Europa para la Prevención del Terrorismo, de 16 de mayo de 2005. Diario Oficial de la Unión Europea 22.6.2018, L 159/3. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22018A0622(01)&from=ES (22/03/2024).

[862] El 28 de febrero de 2023, el Presidente de la Federación de Rusia firmó una ley federal por la cual Rusia terminaba su membresía en el Consejo de Europa a partir del día 16 de marzo de 2023. Con ello, se ven afectados diferentes tratados internacionales, entre los que destaca el Convenio Europeo para la Represión del Terrorismo, de 27 de enero de 1977, cuyo cese de vigencia respecto a Rusia puede tener efectos negativos para la efectiva articulación de extradiciones por este tipo de delitos, al abrirse la vía para su consideración como políticos o inspirados por motivos políticos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por otra parte, la ENCOT se alinea con la Estrategia de la UE para una Unión de la Seguridad 2020-2025[863] por cuanto ésta considera al terrorismo[864] y la radicalización[865] como una de sus cuatro prioridades estratégicas[866], frente a la que hay que actuar de manera integral dando cabida a las acciones que dificulten el uso del ciberespacio como uno de los comunes globales más idóneos para "la captación, el adoctrinamiento, el reclutamiento y la difusión de su propaganda"[867] y la promoción del compromiso internacional y de la coordinación entre operadores públicos y privados para contrarrestar el ciberterrorismo.

En esta idea se definen los cuatro pilares de actuación -prevenir, proteger, perseguir y preparar la respuesta-[868] entre los que merece especial atención el de *prevención*, donde se recoge expresamente una línea estratégica referida al aumento de las capacidades en la lucha contra la desinformación que, en su desarrollo, entronca directamente con el objetivo de nuestra hipótesis de trabajo, cual es la afectación que ésta tiene a la seguridad nacional:

> "Incrementar las capacidades de las Administraciones públicas y de las unidades de investigación de las FCS, frente a las campañas de desinformación que afecten a la seguridad nacional y tengan por objeto fines terroristas o de radicalización, ya sea mediante la difusión de falsas narrativas, el uso de la guerra cognitiva, estrategias híbridas, manipulación persistente u otras tácticas, técnicas y procedimientos"[869].

También dentro de este primer pilar se establece el desarrollo de normas de segundo nivel como el Plan Estratégico Nacional de Prevención y Lucha contra la Radicalización

[863] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE para una Unión de la Seguridad, Bruselas 24.07.2020, COM (2020) 605 Final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0605 (03/12/2023).

[864] La UE define su línea de acción contra el terrorismo en la Estrategia de la Unión Europea de Lucha contra el Terrorismo, del Consejo de la Unión Europea, 14469/4/05. Bruselas, 30 de noviembre de 2005. Disponible en: https://data.consilium.europa.eu/doc/document/ST%2014469%202005%20REV%204/ES/pdf (17/01/2024).

[865] La UE define su línea de acción contra la radicalización en la Estrategia revisada de la UE para luchar contra la radicalización y la captación de terroristas, del Consejo de la Unión Europea, 9956/14. Bruselas, 19 de mayo de 2014. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/es/pdf (17/01/2024).

[866] Las cuatro prioridades estratégicas que define la EEUS 2020-2025 son: 1) alcanzar un entorno de seguridad con garantías de futuro, con especial atención a la ciberseguridad; 2) afrontar las amenazas cambiantes como la ciberdelincuencia, la amenaza híbrida y la desinformación; 3) luchar contra el terrorismo, la radicalización y la delincuencia organizada; 4) construir un ecosistema de seguridad europeo sólido sobre el compromiso y la concienciación de la amenaza global de carácter multidimensional.

[867] Estrategia Nacional contra el Terrorismo 2023, Op. CIt. Página 51521.

[868] IBIDEM, página 51505.

[869] IBIDEM, página 51521.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Violenta (PENCRAV)[870], el Plan Integral de Cultura de Seguridad Nacional[871] y el Plan Estratégico Nacional contra la Financiación del Terrorismo (PENCFIT)[872].

En el segundo pilar, *proteger*, deben destacarse dos líneas de actuación: la referida al aumento de las capacidades y el impulso de herramientas de detección en el ámbito de la ciberseguridad, y la potenciación del intercambio de información y la asistencia recíproca a nivel nacional e internacional.

Dentro del tercer pilar, *perseguir*, nuevamente se define como estratégica la labor de inteligencia junto con la cooperación operativa, así como lucha contra las narrativas terroristas para contrarrestar la propaganda en Internet o por cualquier otro medio.

El cuarto pilar, *preparar la respuesta*, incide en promover una sociedad más resiliente, el apoyo a las víctimas del terrorismo y, como novedad, la implementación de un sistema de lecciones aprendidas de gestión de crisis, sobre la base de la evaluación crítica de todos los actores intervinientes. En relación con la resiliencia, definida por la ENCOT como la "capacidad de resistencia y recuperación ante la acción terrorista"[873], se recoge expresamente la gran capacidad que nuestra sociedad, a lo largo de la historia reciente, ha demostrado para sobreponerse al terrorismo y sus devastadores efectos, "bajo el principio de proteger la vida de las personas y sus derechos y libertades, así como el orden constitucional"[874].

Especial relevancia posee el Comité Especializado contra el Terrorismo, presidido por la persona que desempeñe la dirección de la Secretaría de Estado de Seguridad, en lo relativo a la continua tarea de actualización de estos Planes y de la coordinación de las Fuerzas y Cuerpos de Seguridad a través del CITCO, principalmente en lo referido a la consecución de objetivos marcados en sus Planes Operativos específicos, y la elaboración de propuestas como el Protocolo Interinstitucional de Respuesta ante Atentados Terroristas[875] para poner en común los instrumentos de coordinación y las capacidades de los distintos actores implicados en la respuesta a una posible acción terrorista de cualquier tipo, tanto dentro como fuera de territorio nacional o en los espacios comunes globales.

---

[870] PENCRAV, no disponible en fuentes abiertas por estar clasificado como "confidencial", fue aprobado en octubre de 2020. Tiene desarrollo operativo a través del Plan Operativo de Prevención de la Radicalización Violenta de la Policía Nacional, de diciembre de 2023. Disponible en: https://www.interior.gob.es/opencms/es/servicios-al-ciudadano/plan-estrategico-nacional-de-prevencion-y-lucha-contra-la-radicalizacion-violenta-pencrav/plan-estrategico-nacional/objetivos-mision-vision/ (17/01/2024).

[871] Orden PCM/575/2021, de 8 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 25 de mayo de 2021, por el que se aprueba el Plan Integral de Cultura de Seguridad Nacional. BOE núm. 138, de 10/06/2021. Referencia BOE-A-2021-9631. Disponible en: https://www.boe.es/eli/es/o/2021/06/08/pcm575 (20/03/2024).

[872] PENCIFT, no disponible en fuentes abiertas por estar clasificado como "confidencial" y, al igual que el PENCRAV, fue aprobado en octubre de 2020.

[873] Estrategia Nacional contra el Terrorismo 2023, Op. CIt. Página 51519.

[874] Estrategia Nacional contra el Terrorismo 2023, Op. CIt. Página 51515.

[875] La elaboración de este Protocolo fue acordada por el Comité Especializado Contra el Terrorismo en junio de 2021, tras la presentación del primer informe de evaluación de la Estrategia Nacional Contra el Terrorismo. No está disponible en fuentes abiertas por su carácter reservado.

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.5.7. La Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad (ENC) de 2019[876] es parte esencial de la Política de Seguridad Nacional que, mediante el desarrollo de las líneas de actuación presentadas por la ESN 2017 en el ámbito de la ciberseguridad, focaliza su atención en la amenaza que se beneficia de las ventajas de la transformación digital, con un elevado nivel de tecnificación y de impacto amplificado por la conectividad global de dispositivos, redes y sistemas, siendo por ello que "las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual"[877] y, consecuentemente, las TIC elementos transversales para todas las esferas de actividad de aquella.

Las vulnerabilidades del ciberespacio, lugar de encuentro común y global que puede ser utilizado tanto como medio para delinquir como ser el objetivo en sí mismo, representan un riesgo clave que ya la Estrategia de Ciberseguridad Nacional de 2013 supo identificar. Ese camino iniciado años antes beneficia a la ENC 2019 que, desde los principios rectores de la ESN 2017 -unidad de acción, anticipación, eficiencia y resiliencia-, construye el muro de contención frente a la ciberamenaza vertebrando el refuerzo de capacidades como las de las Fuerzas y Cuerpos de Seguridad para la "investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio"[878], impulsando el desarrollo de la industria española vinculada con la tecnología y la ciberseguridad, o llamando la atención sobre la gestión del talento nacional para tratar de generarlo desde las etapas más tempranas de la educación superior, motivarlo, aplicarlo con acierto y, sobre todo, retenerlo con expectativas apropiadas. En este sentido, es de máxima relevancia la relación de causalidad que aquí se establece entre la cibercriminalidad y la seguridad ciudadana, elemento clave para reforzar las capacidades frente a esta amenaza que, no por desenvolverse en el dominio del ciberespacio, deja de tener consecuencias físicas directas para la seguridad de los ciudadanos.

De igual forma se refiere la ENC 2019 a la *resiliencia* como característica fundamental de las infraestructuras críticas y servicios esenciales que el Estado, como garante último de la seguridad nacional, debe proteger contra las ciberamenazas[879] en el marco de la búsqueda de la autonomía estratégica europea que permita fortalecer las capacidades de prevención, detección, respuesta y recuperación de los activos estratégicos tanto del sector público como del privado[880].

Finalmente, debemos llamar la atención sobre la nueva perspectiva que sabe identificar la ENC 2019 al señalar la protección de los datos personales de los ciudadanos, el acceso a información veraz y su libertad de expresión en el ciberespacio, haciendo una acertada extrapolación del artículo 20 de la CE para la defensa de esos derechos fundamentales

[876] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. BOE núm. 103, de martes 30 de abril de 2019.
[877] Estrategia Nacional de Ciberseguridad. Resumen Ejecutivo, página 9. Presidencia del Gobierno, Madrid, 2019. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019 (18/01/2024).
[878] IBIDEM, página 10.
[879] IBIDEM, página 31.
[880] IBIDEM, página 39.

Ediciones Universidad de Salamanca | CC BY-NC-ND

que, de hecho, son la base para articular la defensa frente a la venta de datos exfiltrados, la desinformación, o las noticias falsas, entre otras, tal y como analizaremos en detalle posteriormente.

Un respaldo a este planteamiento de ciberseguridad nacional que se integra en el propio de la Unión Europea, por cuanto transpone la Directiva NIS 2[881], supone el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad[882], presentado el 14 de enero de 2025 de manera conjunta por los Ministerios de Interior, de Defensa y para la Transformación Digital y de la Función Pública[883], el cual propone una serie de obligaciones relacionadas con la actualización de la Estrategia Nacional de Ciberseguridad, la designación de autoridades de control y gestión de crisis apoyados por equipos de respuesta a incidentes de seguridad informática, el establecimiento de medidas para la gestión de riesgos de ciberseguridad, la notificación de ciberataques por parte de las entidades críticas y otras específicamente reguladas, y las normas de intercambio de información sobre ciberseguridad a diferentes niveles. Una de sus principales novedades es, sin duda, la creación del Centro Nacional de Ciberseguridad que, siguiendo el modelo de otros como el CITCO, se presenta como el responsable de la dirección, impulso y coordinación de los organismos competentes en la materia y, como tal, máxima autoridad para la gestión de crisis de ciberseguridad y punto único de contacto con la UE. A este respecto, merece destacarse la nueva dimensión transfronteriza que se concede a la *ciberresiliencia* para garantizar un elevado nivel común de ciberseguridad y asegurar la prestación de servicios entre los distintos Estados miembros.

4.5.8. La Estrategia Nacional contra las Campañas de Desinformación

Aunque en el momento de presentar esta tesis no ha hecho más que comenzar el proceso de redacción de la Estrategia Nacional contra las Campañas de Desinformación (ENCCD), consideramos necesario analizar las líneas que definen este mandato por su directa implicación con el objeto de nuestro estudio.

La Orden PJC/248/2025, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 28 de enero de 2025, por el que se aprueba el procedimiento para la elaboración de la Estrategia Nacional contra las Campañas de Desinformación[884]

---

[881] Directiva NIS 2 (UE) 2022/2555 del Parlamento Europeo y del Consejo, del 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148.

[882] Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad. Disponible en: https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf (18/01/2025).

[883] Disponible en: https://www.interior.gob.es/opencms/ca/detalle/articulo/El-Consejo-de-Ministros-aprueba-el-anteproyecto-de-Ley-de-Coordinacion-y-Gobernanza-de-la-Ciberseguridad/ https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/140125-rueda-de-prensa-ministos.aspx (18/01/2025).

[884] BOE núm. 64, de 15 de marzo de 2025. BOE-A-2025-5151. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151 (17/03/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

señala como garante de su preparación a la Comisión Permanente contra la Desinformación[885], en cuanto responsable de la coordinación interministerial y de la asistencia al CSN sobre aquellos aspectos que requieran la valoración técnica sobre posibles campañas desinformadoras.

Dicha Comisión será la encargada de crear un grupo de trabajo de carácter técnico en el que tendrán cabida las Comunidades y Ciudades Autónoma, así como aquellos expertos de la sociedad civil, el sector privado y académico que puedan contribuir al mejor resultado por su conocimiento en la materia. Con este diseño de *equipo multifacético*, el legislador se asegura la participación de todos los sectores interesados, tratando así de evitar errores pretéritos como el cometido con el *Procedimiento de actuación contra la desinformación*[886], donde la inadecuada gestión de comunicación estratégica de la iniciativa legislativa y la no inclusión de otros actores civiles y privados en el proceso de redacción, generaron un debate político y social que hubo de sofocarse con la instauración del Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional[887]. De la dirección del proyecto, la gestión de recursos y la tramitación de los acuerdos se responsabiliza el DSN, en su rol de Secretaría Técnica y órgano del CSN.

Las directrices que la referida Orden PJC/248/2025 marca para la elaboración de la ENCCD son claves para entender la naturaleza del producto que se espera:

1. La Estrategia debe contar con un análisis del contexto actual de la amenaza desinformativa, como punto de partida desde el que poder interpretar la situación real referida a narrativas, actores, objetivos y afectación a los intereses nacionales, con especial atención a la seguridad nacional.
2. De acuerdo con la amenaza y los riesgos identificados, la Estrategia debe ofrecer las líneas de prevención y articulación de la respuesta desde un enfoque amplio y transversal, debidamente alineado con la política de seguridad nacional.
3. Lógicamente, habrá de estar en consonancia con el esquema europeo de lucha contra la desinformación y la injerencia extranjera y, en particular, con el Plan de Acción para la Democracia Europea[888] como referencia de la respuesta democrática a esta amenaza desde la cooperación de los distintos actores implicados -públicos y privados-, el desarrollo y la implementación de herramientas específicas, el ejercicio de la autoridad legal y reguladora frente a las grandes plataformas y prestadores de servicios en línea, y el fomento de la alfabetización mediática y de gestión de la información para impulsar las competencias digitales de los ciudadanos.
4. Igualmente, la ENCCD ha de nacer alineada con las consideraciones de la comunidad internacional en lo relativo a la protección del acervo de derechos y

[885] La Comisión Permanente contra la Desinformación se crea en marzo de 2019 por el CSN, de acuerdo a los establecido en el marco de la UE por el Plan de Acción contra la Desinformación. Está integrada por el DSN, el CNI, la Secretaría de Estado de Seguridad, la Secretaría de Estado de Transformación Digital e Inteligencia Artificial y la Dirección General de Comunicación, Diplomacia Pública y Redes.
[886] Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. BOE número 292, de 5 de noviembre de 2020. Disponible en: https://www.boe.es/eli/es/o/2020/10/30/pcm1030 (07/12/2024).
[887] Ver Capítulo 8, apartado 8.1.2.
[888] Ver Capítulo 7, apartado 7.2.2.2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

libertades que deben prevalecer en un espacio de información plural, pacífico y sostenible. A este respecto, se menciona expresamente los Principios Globales de las Naciones Unidas para la Integridad de la Información, marco de acción integral de carácter internacional para la consecución de un ecosistema de la información más seguro y respetuoso con los derechos humanos.

5. Para conseguir un mejor resultado a través del entendimiento profundo de la amenaza, la Estrategia debe tener un componente de colaboración público-privada donde tenga entrada la sociedad civil, a través de iniciativas como la que representa el Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional, y las investigaciones académicas en los diferentes ámbitos de actuación del desafío desinformador.
6. Finalmente, se hace referencia a dos cuestiones esenciales para el buen fin de la propuesta: que la misma sea producto del mayor consenso posible entre sus partícipes, y que sea presentada a la ciudadanía a través de una adecuada estrategia de comunicación y divulgación formativa.

Se inicia de esta manera un apasionante proceso de redacción para el que, en nuestra opinión, España cuenta actualmente con la experiencia, la motivación y el respaldo social como elementos determinantes para poder llevar a buen término una Estrategia europeista y alineada con el derecho Internacional que, como ya se ha hecho en anteriores ocasiones, sea innovadora en sus propuestas, garantista de libertades y firme frente a la amenaza desinformativa que, como veremos en capítulos posteriores, puede afectar a la propia seguridad interna del Estado a través de la negativa repercusión en la conformación de la opinión pública libre y plural que ampara la Constitución, generando una sociedad incapaz "de ponerse de acuerdo sobre hechos básicos, lo que impide construir una democracia funcional, al tiempo que polariza las opiniones" (SERRA CRISTÓBAL, 2023, pág. 30).

4.6. El Modelo de Seguridad 2030 en España

Una vez analizado el poliédrico enfoque del concepto de *seguridad* en la Constitución española, estudiada la estructura sobre la que se construye el Sistema de Seguridad Nacional y examinado el desarrollo de las sucesivas *estrategias de seguridad* como base de la respuesta frente a la continua caracterización de la amenaza a lo largo del tiempo, debemos avanzar en el análisis de la aplicación de este concepto como elemento esencial para el disfrute de la libertad y el progreso propios de un Estado del bienestar, en consonancia con la interpretación actual de los derechos humanos.

4.6.1. La ampliación del concepto de seguridad en el marco normativo español

En el trámite parlamentario de aprobación de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional[889] (LSN), la representante del Gobierno debatía las enmiendas presentadas al proyecto de ley manifestando que:

[889] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. BOE-A-2015-10389. Disponible en: https://www.boe.es/eli/es/l/2015/09/28/36/con (27/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] la seguridad es de hecho un bien público, un derecho de los ciudadanos y, en consecuencia, un deber del Estado, si me apuran, el primero. Es la base sobre la que sustentamos el ejercicio de nuestras libertades y la efectividad de nuestros derechos. La seguridad nos permite generar confianza y construir certidumbres; es una condición indispensable para que las personas puedan desarrollar sus proyectos de vida y las sociedades logren avanzar en su propio progreso, en suma, ejercer la libertad"[890].

Con esta misma visión amplia, multidisciplinar y adaptativa de la seguridad comienza el Preámbulo de la citada Ley, cuando señala que "la seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones".

La interrelación de los ámbitos de seguridad, el desempeño vital en libertad para conseguir prosperidad y la garantía de una buena gestión de gobierno, claves de la Agenda 2030, se filtran en la norma española consciente el legislador de que en el actual escenario interconectado y dinámico, global, la seguridad debe ser concebida como un modelo integral capaz de ofrecer respuestas ágiles y adaptadas que cuenten con el compromiso de todos los actores involucrados, tanto en el ámbito público como en el privado.

Por ello, merece la pena llamar la atención sobre el común denominador que comparten la Agenda 2030, como pacto global para el desarrollo, y la Ley de Seguridad Nacional, como espacio de acuerdo para conformar la nueva visión de la seguridad, que no es otro que "la denominada regla de la triple C, cooperación, coordinación y complementariedad, en aras de garantizar una capacidad de reacción eficaz"[891], para posteriormente entrar a analizar la forma en que todo este marco conceptual se adapta a la estrategia de seguridad interior española.

Desde estos planteamientos, la LSN 2015 en su título preliminar establece definiciones y principios generales necesarios para entender la dimensión del *superior interés nacional* que en ella subyace. A partir de aquí, en su artículo 3, se define por vez primera en nuestro ordenamiento jurídico ese concepto no constitucionalizado que es la *seguridad nacional*, entendiéndose como una *Política de Estado* que se lleva a cabo para proteger los *derechos, las libertades y el bienestar de los ciudadanos*, en un modelo de convivencia y de valores propios de una sociedad democrática avanzada que, a su vez, garantiza la *defensa de España y de la seguridad internacional* a través de los compromisos asumidos con socios y aliados a nivel global[892].

[890] Diario de Sesiones del Congreso de los Diputados, sesión plenaria núm. 278 (extraordinaria), de 8 de julio de 2015, p. 29.
[891] Diario de Sesiones del Congreso de los Diputados, sesión plenaria núm. 278 (extraordinaria), de 8 de julio de 2015, p. 31.
[892] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, artículo 3: "A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos".

Ediciones Universidad de Salamanca | CC BY-NC-ND

Este es el primer paso que se da para, desde la responsabilidad compartida en el marco funcional y competencial de cada uno de los actores, involucrar en la política de seguridad nacional a los tres niveles de la Administración Pública -estatal, autonómica y local-, al sector privado y a la sociedad civil. De esta forma, salvando las distancias, parece que se extrapola a la seguridad nacional el modelo de compromiso multinivel que rige en el marco de acción de la seguridad pública, buscando ese encaje legitimador de toda política de Estado en una Constitución que, lógicamente, no puede contemplar algunos de los conceptos y riesgos actuales que, sencillamente, no existían cuando vio la luz en 1978.

A continuación, se define la *Política de Seguridad Nacional* como aquella política pública que, bajo la responsabilidad del Gobierno, es participada por todas las Administraciones Públicas y por la sociedad en su conjunto para responder a las necesidades de ella derivadas. El siguiente concepto necesario para la construcción del modelo es el de la *Estrategia de Seguridad Nacional*[893], donde se concreta la amenaza a la que hay que dar respuesta, se definen las líneas de acción estratégicas y se organiza la contribución de recursos necesarios para ser empleados de manera optimizada en la situación de interés para la seguridad nacional que lo requiera. La LSN 2015, en este sentido, hunde sus raíces en la ESN 2013 pero, necesariamente, mira hacia adelante obligada por el contexto de interdependencia y globalización que rige el momento, marcando de esta manera su carácter avanzado, inclusivo, transversal y proactivo que queda reflejado en la organización del Consejo de Seguridad Nacional y sus Comités Especializados, equiparándonos con ello «a los países más avanzados en materia de seguridad» (CASTELLÓN MORENO, 2015, pág. 33)

Es así que dos años más tarde, en 2017, en este escenario determinado por la tecnología como palanca transversal de efecto multiplicador de oportunidades pero, también, de amenazas como el terrorismo y la cibercriminalidad, nace la tercera strategia de Seguridad Nacional española[894], con el subtítulo *un proyecto compartido de todos y para todos*, sin agotar el periodo de cinco años que la Ley prevé para su revisión y, además, bajo el mandato del mismo Presidente del Gobierno, Mariano Rajoy. Las razones para adelantar la revisión de la ESN 2013 no solo son las derivadas de la necesaria adaptación a los cambios surgidos al amparo del citado panorama geopolítico internacional que afectan a España como país europeo, mediterráneo y atlántico, miembro de la UE y la OTAN, sino también a las propias de la necesidad de dar entrada a la participación de los distintos actores públicos y privados en el funcionamiento del Sistema de Seguridad Nacional que prevé la LSN del 2015. Conforme a ello se definen cinco objetivos generales que orientan la acción del Estado en esta materia como son: 1) desarrollar un modelo

[893] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, artículo 4.3: "La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley".

[894] En 2011 se publica la primera Estrategia Española de Seguridad, bajo el lema *una responsabilidad de todos*. En 2013 se presenta la Estrategia de Seguridad Nacional, con el subtítulo *un proyecto compartido*.

Ediciones Universidad de Salamanca | CC BY-NC-ND

integral de gestión de crisis; 2) promover una *cultura de seguridad nacional*; 3) favorecer el buen uso de los espacios comunes globales; 4) impulsar la dimensión de seguridad en el desarrollo tecnológico; 5) y fortalecer la proyección internacional de España.

Por su parte, la ESN 2017 avanza en estos objetivos alineada con la concepción integral de la seguridad, considerando los retos que plantean la seguridad económica, el cambio climático, los recursos energéticos, los avances tecnológicos, el desarrollo del ciberespacio, los problemas de la demografía y los flujos migratorios, la seguridad frente a las epidemias y pandemias o la protección frente a catástrofes, entre otros, como *ámbitos de especial interés para la seguridad nacional* de un país como España "abierto al mundo, que respeta el Estado de Derecho, el valor del consenso constitucional, defensor de los Derechos Humanos, de la legalidad internacional y del multilateralismo, que son señas de identidad de la Unión Europea" (BALLESTEROS MARTÍN M. Á., 2017, pág. 6).

La ESN 2013 ya partía de una concepción amplia de la seguridad, pero es la de 2017 la que definitivamente consolida la ubicación del ser humano en el centro de la política de seguridad para abordar las amenazas y los desafíos[895] derivados de ámbitos como la ordenación de los flujos migratorios, incluyendo la línea de acción de cooperar con los países de origen y tránsito migratorio para favorecer su desarrollo, fomentar vías de inmigración legal, prevenir en origen la inmigración irregular y luchar contra las redes de inmigración y el tráfico ilícito de personas, o la seguridad frente a pandemias y epidemias, con líneas de acción como la de adaptar servicios de salud pública del Estado y Comunidades Autónomas para asegurar una adecuada capacidad de respuesta operativa y desarrollar los Equipos Técnicos Españoles de Ayuda y Respuesta en Emergencias (START) y favorecer su participación en misiones internacionales, o la preservación del medio ambiente mediante la profundización en el seno de la UE en el cumplimiento de los compromisos asumidos para la preservación del medio ambiente, la biodiversidad, la prevención de la inseguridad hídrica y, muy especialmente, la lucha contra el cambio climático avanzando en la cooperación internacional. En este marco definido por la ESN 2017[896] se encuadra el *Modelo de Seguridad 2030* del Ministerio del Interior, sobre el que posteriormente las Fuerzas y Cuerpos de Seguridad del Estado definen sus correspondientes *Planes Estratégicos*[897].

[895] La ESN 2017 define los desafíos como retos que, sin tener la entidad de amenaza, suscitan vulnerabilidad, provocan situaciones de inestabilidad o pueden propiciar el surgimiento de nuevas amenazas.

[896] Este marco definido por la ESN 2017 se ve superado por lo que la siguiente ESN 2021 señala en su capítulo introductorio, al señalar que "en condiciones normales, la revisión de la Estrategia de Seguridad Nacional 2017 se hubiese llevado a cabo pasados cinco años. Sin embargo, el impacto de la pandemia de la COVID-19 y el incremento en el empleo de estrategias híbridas han aconsejado una revisión estratégica que permita enfrentar los riesgos y las amenazas en un renovado contexto de globalización, condicionado por una mayor incertidumbre y un cambio acelerado". Esta situación no hace sino afianzar las líneas maestras que marca la Agenda 2030 y que se trasladan a la normativa española, como por ejemplo el Plan Estratégico de la Policía Nacional 2017-2021 y el posterior 2022-2025.

[897] En el caso de la Policía Nacional, su Plan Estratégico es posteriormente desarrollado por los *Planes Operativos Funcionales* para abordar problemáticas concretas, los *Planes Territoriales* elaborados por las Jefaturas Superiores para dar respuesta a las contingencias específicas y prioritarias de cada demarcación y, finalmente, los *Planes Globales* que los Servicios Centrales diseñan en su área funcional, encargados todos ellos de atomizar las líneas marcadas por los ejes generales definidos por el Ministerio del Interior

Ediciones Universidad de Salamanca | CC BY-NC-ND

4.6.2. El Modelo de Seguridad 2030 del Ministerio del Interior

El Ministro del Interior Grande-Marlaska presenta el *Modelo de Seguridad 2030* a la Comisión de Interior del Congreso de los Diputados en la comparecencia de inicio de la XIV Legislatura, el 17 de febrero de 2020, iniciando con una referencia al ODS 16.6 como inspirador de su Gobierno "que tiene en la transparencia y en la rendición de cuentas uno de sus ejes principales de trabajo"[898], para continuar plenamente alineado con la Agenda 2030 revelando un planteamiento conceptual de la seguridad humana como respuesta de su departamento para enfrentar tanto las amenazas tradicionales vinculadas con la reducción de la violencia en cualquiera de sus formas, como los nuevos retos de seguridad que se conectan e interrelacionan de manera indivisible con los riesgos derivados de la sostenibilidad ambiental, la transformación digital, el odio o la violencia de género.

El Modelo de Seguridad 2030 refleja la materialización efectiva del concepto de *seguridad humana* en la política del Ministerio del Interior, enfocándolo como un bien público, con vocación vertebradora del Estado y con una doble naturaleza, *preventiva y adaptativa* en cuanto a las nuevas amenazas transversales que debe afrontar, y reactiva y flexible para coordinar la respuesta que permita aprovechar todas las capacidades disponibles en el plano nacional, fruto de la cooperación vertical entre administraciones y de la horizontal con el ámbito privado y la sociedad civil, y en el plano supranacional como Estado miembro de la UE y con focos de interés en el Atlántico, América del Sur o África.

El Modelo se construye sobre tres *áreas de actuación*, que se definen como entornos a proteger para garantizar la seguridad, y nueve *ejes estratégicos* a través de los cuáles se articulan las cuarenta y cinco *medidas de actuación* concretas para operativizarlos.

La primera de estas áreas de actuación se denomina *entorno seguro* y es la premisa inicial del Modelo de Seguridad 2030, puesto que parte de la consideración de que la garantía efectiva de los derechos fundamentales y las libertades públicas requiere de un entorno seguro, en una acepción amplia, que abarca una dimensión territorial, una digital, una medioambiental y una vial.

La protección del entorno desde el punto de vista *territorial* es el primer eje estratégico y se refiere al control de fronteras y a la política migratoria, para los que se proponen medidas basadas en la modernización de la tecnología aplicada a la vigilancia física, el reforzamiento de la cooperación con los países de origen y tránsito para luchar contra las graves lacras del tráfico de seres humanos y la trata de personas para fines de explotación sexual y laboral, y la colaboración con el resto de Estados miembros de la

para que lleguen a dar respuesta integral y efectiva a las necesidades de los ciudadanos en el espacio de convivencia actual.

[898] Diario de Sesiones del Congreso de los Diputados, Comisión Interior, XIV Legislatura, sesión núm. 2, de 17 de febrero de 2020, p. 4.

Ediciones Universidad de Salamanca | CC BY-NC-ND

UE en la implementación de las medidas necesarias para llevar a cabo la Política Común de Fronteras de la Unión[899].

La *dimensión digital* del aseguramiento del entorno implica una apuesta por la transformación digital de la Administración y de la sociedad en general, con especial atención a la cultura de seguridad para dar respuesta al incremento de las estadísticas de cibercriminalidad, fruto del aumento de la superficie de exposición vinculada a la hiperconectividad y la dependencia de las tecnologías propias del modo de vida actual, con especial referencia al elemento disruptivo que ha supuesto el teletrabajo como forma de compaginar la jornada laboral presencial y a distancia.



Gráfico 4.3.
Evolución anual de la cibercriminalidad 2019-2023
Fuente: Ministerio del Interior

Como señala la profesora Álvarez Robles, estas políticas de seguridad digital centran su objetivo en:

> "[…] concienciar a los ciudadanos sobre diversos temas que abarcan desde los peligros asociados a publicar determinados datos consciente o inconscientemente en una red social, o de admitir a personas que no conocemos en las redes sociales y que podrían ser utilizados en un spear phishing, hasta señalar los riesgos a los que nos exponemos al no instalar un buen antivirus, al no realizar copias de seguridad o al conectarnos a las redes wifi-abiertas" (ÁLVAREZ ROBLES, 2024, pág. 281).

El tercer eje es el vinculado al *entorno medioambiental*, que se pretende consolidar mediante la modernización del sistema de protección civil con el objetivo de mejorar la

[899] Conforme a lo establecido en el Capítulo 2 del Tratado de Funcionamiento de la UE, artículos 77 a 80, las políticas sobre controles en las fronteras, asilo e inmigración son comunes para los Estados miembros y se regirán por el principio de solidaridad y de reparto equitativo de la responsabilidad entre ellos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

prevención, la respuesta y la resiliencia frente a las catástrofes naturales que, de manera cada vez más frecuente y vinculadas al cambio climático, castigan a la población civil en sus personas y propiedades.

Por último, el cuarto eje es el relativo al aseguramiento del *entorno vial*, como "uno de los primeros derechos del día a día"[900] de los ciudadanos, partiendo de la base de la Agenda 2030 y el reforzamiento de la cultura de seguridad para lograr un cambio del modelo de movilidad más activo y saludable.

La segunda área de actuación es la de *garantizar la convivencia*, elemento diferencial de toda democracia como requisito básico para hacer efectivo el bienestar económico y social y el ejercicio de los derechos y libertades ciudadanas, y se articula sobre tres ejes de protección: la erradicación del odio y la dominación, la lucha contra el terrorismo y el crimen organizado y la actuación sobre la política penitenciaria.

En cuanto a la *erradicación del odio y la dominación en la sociedad* como quinto eje estratégico, remite a la numerosa normativa desarrollada *ad hoc* y que tienen sus referencias principales, en cuanto a los delitos de odio e intolerancia, en el Plan de Acción de Lucha contra los Delitos de Odio[901] y, en lo que respecta a la violencia de género, en la Ley y en el Pacto de Estado contra la Violencia de Género[902], con su acomodo informático a través del Sistema VioGén[903].

[900] Así lo expresa el Ministro del Interior D. Fernando Grande-Marlaska Gómez en su intervención en la Comisión de Interior del Congreso de los Diputados, tal y como lo recoge su Diario de Sesiones, sesión núm. 2, de 17 de febrero de 2020, p. 42.

[901] El primer Plan de Acción de Lucha contra los Delitos de Odio de la Secretaría de Estado de Seguridad del Ministerio del Interior se firmó en enero de 2019, con el objetivo de luchar contra este tipo de delitos de prejuicio que no solo atacan a la víctima sino que, también, generan sentimientos de miedo e inseguridad que afectan a la seguridad y la convivencia de la sociedad en general, que tiene como uno de sus pilares básicos el respeto mutuo entre las personas que la conforman. Posteriormente, se aprobó el II Plan de Acción de Lucha contra los Delitos de Odio 2022-2024. Actualmente está se encuentra en vigor el III Plan de Acción (2025-2028) para luchas contra los delitos de odio, que prioriza la asistencia a las víctimas, la prevención y la persecución de este tipo de delitos, reforzando la colaboración internacional y el uso de la tecnología para afrontar el odio en la red. Estos planes tienen desarrollo a través del Protocolo de actuación de las FCS para los delitos de odio y conductas que vulneran las normas legales sobre discriminación, y el Protocolo para combatir el discurso de odio ilegal en línea.

[902] Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, y Real Decreto-ley 9/2018, de 3 de agosto, de medidas urgentes para el desarrollo del Pacto de Estado contra la violencia de género.

[903] El Sistema de Seguimiento Integral de los Casos de Violencia de Género (Sistema VioGén) es la aplicación informática del Ministerio del Interior para la valoración policial del riesgo en los casos de violencia de género, el seguimiento y la gestión de dicha evaluación a través de la actuación de las FCS. Es administrado por la actual Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad (SES) y se comenzó a usar en el año 2007, siendo que actualmente, además de las FCS del Estado y autonómicas, hay incorporados a VioGén más de 700 Cuerpos de Policía Local de toda España. Desde entonces ha ido actualizándose con la implementación de nuevas versiones que incluyen formularios adaptados a la realidad del problema conforme va evolucionando día a día para dar un tratamiento integral de la violencia de género. En este sentido, citar las Instrucciones de la Secretaría de Estado de Seguridad (ISES) 4/2019, por la que se establece un nuevo protocolo para la valoración policial del nivel de riesgo de violencia de género y de gestión de la seguridad de las víctimas; la ISES 2/2021 sobre reforzamiento de las actuaciones policiales en materia de valoración de riesgo en los casos de violencia de género y de gestión de la seguridad de las víctima; la ISES 5/2021, por la que se establece el protocolo

Ediciones Universidad de Salamanca | CC BY-NC-ND

El sexto eje se refiere a la *lucha contra el terrorismo y el crimen organizado*, auténticos ataques al corazón de cualquier sociedad democrática que España, desafortunadamente, ha sufrido a lo largo de su historia reciente. Ambos son problemas complejos que exigen un enfoque alineado y la responsabilidad compartida por parte de todos los estratos sociales, políticos e institucionales pues se trata de dos de las principales prioridades de la política de seguridad pública por los graves riesgos asociados que comportan para la convivencia pacífica y en libertad. Con idea de potenciar la prevención y mejorar, igualmente, la capacidad de reacción para combatir y contrarrestar la amenaza que suponen este tipo de delitos violentos, se publica en 2019 la primera Estrategia Nacional contra el Terrorismo[904] que, expresamente, refiere en su resumen ejecutivo el acceso a la tecnología por los grupos terroristas como elemento incentivador de su capacidad de financiación, reclutamiento, adiestramiento y propaganda. Este documento se alinea con la Estrategia Contra el Terrorismo de la UE y la de NNUU utilizando como base los mismos cuatro pilares –prevenir, proteger, perseguir y preparar la respuesta-. Se aprueba también la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023[905] para adaptarse igualmente al nuevo paradigma tecnológico de la delincuencia, fijando líneas de actuación concretas para puntos conflictivos a través de Planes Especiales como el del Campo de Gibraltar[906], con el objetivo de reforzar las capacidades operativas y de inteligencia de las FCSE y reducir el impacto en la seguridad, la vida social y el desarrollo económico de la zona. Especialmente relevante para dar respuesta a estas dos formas de delincuencia extrema resulta la utilización de los datos del Registro de Nombres de Pasajeros (PNR)[907] para, en orden a garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos europeos, poder acceder a las listas de pasajeros de los vuelos internacionales que tengan origen, destino o tránsito en España, tanto de carácter comercial como privados, y poder tratarlos para generar inteligencia a través de la Unidad Nacional de Información sobre Pasajeros española (UNIP), incardinada en la estructura del Centro de Inteligencia

de primer contacto policial con víctimas de violencia de género en situación de desprotección (Protocolo Cero); la ISES 8/2021, por la que se establecen medidas para prevenir la violencia de género ocasionada por agresores persistentes; o la reciente ISES 1/2023, por la que se desarrolla la obligación de comunicación a la víctima de los antecedentes del agresor en los denominados casos de "agresores persistentes" y otras medidas de protección y seguridad en los casos de violencia de género. En enero de 2025, el Ministerio del Interior junto con el de Igualdad presentan el nuevo Sistema VioGén 2, consistente en una nueva plataforma digital más evolucionada que da respuesta a las modificaciones normativas surgidas en la materia desde 2018.

[904] Orden PCI/179/2019, de 22 de febrero, por la que se publica la Estrategia Nacional contra el Terrorismo 2019, aprobado por el Consejo de Seguridad Nacional.

[905] Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave, que actualiza la anterior Estrategia Española contra el Crimen Organizado 2011-2014.

[906] Este Plan se ha ido prorrogando y actualmente ya va por la tercera vez que se dota de presupuesto, ampliando su ámbito territorial de aplicación por la necesidad de atender a nuevos enclaves de las organizaciones criminales de la zona.

[907] El PNR, acrónimo del nombre en inglés *Passenger Name Record*, se regula en la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, que traspone al ordenamiento interno español la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Ediciones Universidad de Salamanca | CC BY-NC-ND

contra el Terrorismo y el Crimen Organizado (CITCO) dependiente de la Secretaría de Estado de Seguridad.

El séptimo eje se centra en la *política penitenciaria*, con el objetivo de avanzar en la encomienda que la Constitución hace respecto a la finalidad resocializadora del sistema penal, para lo cual se plantean medidas de inversión y mejora de medios y capacidades, y de modernización del marco normativo para la mejora de la eficacia restaurativa del modelo.

La tercera y última área de actuación del Modelo de Seguridad 2030 es la de *generar valor público* a través del compromiso con el servicio prestado a la sociedad, de acuerdo con los desafíos y retos que la efectividad de los derechos y libertades de los ciudadanos exige.

Por su parte, el octavo eje estratégico es el de la mejora del marco de *seguridad ciudadana*, a través de líneas de acción que pretenden reforzar a nivel policial la cooperación internacional canalizada por las Oficinas Nacionales respectivas[908] y la coordinación nacional de los distintos Cuerpos –estatales, autonómicos y locales- coadyuvando a la unificación de procedimientos de respuesta a través de la integración en el Servicio 112.

El último eje es el del fomento del *empleo público* para tratar de recuperar el número de efectivos de las FCSE que decrecieron paulatinamente a lo largo de los años anteriores y, también, de incorporar la dimensión demográfica al modelo de seguridad en el entorno rural.

Esta es la política de seguridad con la que el Ministerio del Interior español trata de hacer suyo el espíritu de la Agenda 2030 y la *visión 360º* del ODS 16 orientado a la paz, la justicia y las instituciones sólidas. Para ello se apoya en el desarrollo de estrategias y planes de segundo nivel para, desde los diferentes niveles de actuación referidos a las FCS, conseguir accionar las líneas de implantación del Modelo de Seguridad 2030. A nuestro juicio, el resultado es desigual en cuanto a los objetivos conseguidos porque, sobre todo en lo referido al ámbito normativo, el marco temporal que marca la propia dinámica política no permite avanzar en algunas de las propuestas formuladas[909]. De

[908] Las Oficinas Centrales Nacionales (OCN) son tres –Interpol, Europol y SIRENE- y se incardinan dentro de la División de Cooperación Internacional de la Policía Nacional, a la que corresponde tal competencia conforme al artículo 12.1.A) de la LOFCS 2/1986. La OCN Interpol es el punto nacional de contacto para la gestión y coordinación de las órdenes internacionales de detención y el intercambio de información policial internacional, entre otras. La Unidad Nacional de Europol se encarga de la colaboración policial sobre la base de la confianza en el marco de la UE y se apoya en las oficinas de enlace nacionales en la sede de La Haya, conformando un nodo de comunicaciones rápidas y directas que favorecen la respuesta coordinada frente a la criminalidad transnacional. Finalmente, la Oficina SIRENE es la encargada de canalizar el intercambio de información en el marco del espacio Schengen, y de gestionar la estructura de Centros de Cooperación Policial y Aduanera con los países con los que compartimos frontera.

[909] Por ejemplo, una de las propuestas del Eje Seguridad Ciudadana era la derogar la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y sustituirla por una nueva que, finalmente, no se llevó a cabo en la XIV Legislatura con el equipo de Gobierno que planteó el Modelo de Seguridad 2030. Es más, dicha Ley fue objeto de Recurso de Inconstitucionalidad 2896/2015 planteado por 97 diputados y diputadas y, sin embargo, el Tribunal Constitucional avaló su constitucionalidad en la STC (Pleno)

Ediciones Universidad de Salamanca | CC BY-NC-ND

igual manera, para ejecutar cualquier proyecto de esta envergadura se necesita un respaldo presupuestario que, muchas veces, no es lo suficientemente amplio para dar cobertura a todas las necesidades derivadas de su implementación. Y, finalmente, algunas inercias que vienen de tiempo atrás son muy difíciles de transformar, por ejemplo, la cada vez mayor proporción de miembros de las FCS en las grandes ciudades en detrimento de los puestos rurales de la *España vaciada* donde, sin ningún género de duda, la presencia policial es igualmente necesaria para mantener esta propuesta de servicio de seguridad integral para todos los ciudadanos, independientemente de su lugar de residencia.

4.7. Reflexiones sobre la seguridad española: la integración de la ciberamenaza como nuevo horizonte de riesgo

Resulta adecuado en este punto hacer un receso en la evolución del discurso para extraer unas conclusiones de la visión española de la seguridad por su diversidad y riqueza de matices, entroncadas con momentos históricos pretéritos que marcaron lo que hoy entendemos por entorno seguro y bienestar ciudadano. En este sentido, nos atrevemos a decir que el estudio de la historia de la seguridad española es un recorrido parejo por la historia de los derechos fundamentales de la persona, cuestión que no hace sino poner en valor la voluntad de sus gobiernos, con la excepción de la dictadura franquista, de respetar la libertad y derechos de sus ciudadanos, así como de protegerlos frente a terceros de cualquier orden o naturaleza.

No significa esto que la evolución de los tiempos y, con ellos, de las normas y estructuras de Estado, hayan salido indemnes de males endémicos como el partidismo, bien liberal como conservadurista, o de ajadas visiones autárquicas del modelo de gobierno que han tenido sus consecuencias en la manera de entender la seguridad y, lógicamente, en las instituciones públicas que, como la Policía, deben servir a los ciudadanos.

Sin embargo, España se convierte con su Constitución de 1978 en un caso de éxito gracias a la construcción de vías de encuentro entre las distintas sensibilidades políticas y al firme compromiso de la sociedad en su conjunto con el modelo de democracia planteado. A ello se suma la responsabilidad de todas las instituciones y organismos del Estado que, todos a una, contribuyen a la estabilidad y al impulso exitoso de la convivencia pacífica y segura que busca la transición española.

Esto es lo que permite que, ya en ese momento, los Cuerpos de Seguridad del Estado asuman en un contexto de normalidad la misión de defender la Constitución, proteger el libre ejercicio de los derechos y libertades de los ciudadanos y garantizar su seguridad, desde unos principios y valores que propugnan, entre otros, el servicio permanente y la dedicación exclusiva a tal elevada misión, siendo en este sentido España uno de los marcos constitucionales más avanzados de la Europa contemporánea.

172/2020, de 19 de noviembre de 2020. No solo no se derogó dicha Ley sino que, al contrario, resultó fortalecida por superar el recurso de inconstitucionalidad planteado.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Y este consenso político y social tiene un reflejo inmediato y evidente en la consideración de la seguridad que, por ejemplo, sustituye el tradicional concepto de orden público por el de seguridad ciudadana, que comprende una visión proactiva y flexible del deber de asistencia y servicio a las personas, fruto de lo cual la seguridad pasa a tener la más alta catalogación posible, que no es otra que la de derecho fundamental.

En este sentido, la Constitución española, como hemos visto, contempla la acepción de seguridad desde diferentes puntos de vista y aplicada a ámbitos tan dispares como la protección de las relaciones de trabajo o de la sanidad, que no dejan de ser sino partes del todo que supone la seguridad de las personas.

Además, la seguridad española evoluciona al ritmo y en la línea marcada por la comunidad internacional, haciendo suyos conceptos como el de la *seguridad humana* que, a través de sus siete facetas -económica, alimentaria, sanitaria, ambiental, personal, comunitaria y política- representa el modelo integral de la seguridad que sustenta retos mundiales como los ODS, claves en la interpretación de la forma de vida en democracia.

Todo ello es lo que explica que España acuerde una norma tan avanzada como la LSN 2015, como respuesta de adaptación de su política de seguridad frente a los nuevos desafíos que presenta un panorama internacional globalizado, interdependiente y altamente tecnologizado, en el que entran con fuerza la ciberseguridad y las amenazas híbridas. Desde esta perspectiva innovadora y apropiada al contexto geopolítico del momento se define con acierto la esencia tripartita de la seguridad nacional: la seguridad individual de las personas, la colectiva del Estado y la global de la comunidad internacional. Es este enfoque novedoso el que posibilita, por ejemplo, la consideración de amenaza para la seguridad nacional de aquellos ciberataques que, aunque no afecten a un sector estratégico o esencial, tengan por sujeto pasivo a personas físicas determinadas, en atención a la gravedad de la agresión, la transversalidad de sus efectos, la dimensión de su perjuicio y la urgencia generada para la reparación del quebrando producido, variables en las que también se analiza la motivación del ataque como indicador de esa posible afectación a la seguridad nacional.

Sobre esta premisa se construye la estructura del SSN y se vincula, a su vez, con la cultura de seguridad nacional, en la convicción de que la sociedad en su conjunto es corresponsable de su propia seguridad y de la preservación del modelo de democracia y libertad en la que se desarrolla su vida y su actividad económica, en la que debe implicarse activamente puesto que, este marco de seguridad, lejos de ser estable, puede verse comprometido por multitud de actores de diversa naturaleza y complejas motivaciones, que actúan tanto en el plano físico como en el virtual.

De acuerdo a esta visión integral de la seguridad nacional, la ciberamenaza es considerada desde la primera ESN 2011 que, en consonancia con la por entonces recién nacida Ley 8/2011 de protección de las infraestructuras críticas, ya la señala como factor de riesgo emergente por las graves consecuencias que puede tener sobre la prestación de servicios esenciales. En este mismo sentido, la ESN 2013 cifra uno de sus objetivos en

Ediciones Universidad de Salamanca | CC BY-NC-ND

garantizar el uso seguro de las redes y los sistemas de información a través del fortalecimiento de las capacidades frente a los ciberataques que, por su transversalidad, pueden tener un alto impacto en la seguridad nacional. Por ello se comienza a trabajar en la línea de la cultura de ciberseguridad, donde la concienciación de ciudadanos, profesionales y empresas en el uso responsable de la tecnología y los servicios asociados es la pieza clave de la política de prevención. Esta misma línea es seguida por la ESN 2017, que presenta el modelo integral de gestión de crisis en el que la respuesta involucra a todos los sectores, públicos y privados, y a la sociedad civil, puesto que el objetivo de un ciberespacio seguro y fiable, como común global, requiere de un compromiso de todos los ciudadanos con el uso responsable de las tecnologías y los servicios ofrecidos en la red, al tiempo que un compromiso con la UE y la comunidad internacional, fomentando la cooperación y el cumplimiento del Derecho Internacional.

Por su parte, la actualmente en vigor ESN 2021, ante la realidad conformada por elementos como la trasformación digital, la hiperconectividad de la sociedad y la eclosión de las tecnologías disruptivas, se mantiene fiel a la consideración de la ciberseguridad como línea de acción estratégica para la seguridad nacional e introduce como novedad *las campañas de desinformación y las injerencias externas* como riesgos de alto componente híbrido que, mediante la explotación de las vulnerabilidades y grietas estructurales democráticas, pueden socavar la estabilidad del Estado o actuar como herramientas de coerción política y polarización social. Fruto de esta apreciación de la gravedad de los efectos de la amenaza desinformativa para la seguridad nacional, en enero de 2025 se abre el proceso de elaboración de una nueva Estrategia de segundo nivel específica *contra las campañas de desinformación*, mediante la cual el CSN inicia la materialización práctica de la medida propuesta en la línea de acción número 13 de la ESN 2021, con la que posteriormente, en septiembre de 2024, se enlaza la misma propuesta recogida en el *Plan de Acción por la Democracia* para proteger e incentivar los valores democráticos ante la erosión y el desgaste que muestran para los ciudadanos.

Ante esta ciberamenaza que germina en un contexto global donde el dato y la información constituyen nuevos ámbitos de poder e influencia, se presenta la soberanía digital como principio rector de la política de seguridad nacional a través de la cuál incorporar la dimensión de seguridad a ámbitos tan dispares pero vinculados entre sí como el del desarrollo industrial, el de la innovación, la tecnología aplicada a la defensa o, incluso, el ámbito académico como centro del conocimiento y el talento.

También es muy relevante la importancia que en la ESN 2021 se le otorga al dato y a la información estratégica como activos a salvaguardar para garantizar la estabilidad política, social y democrática del país y, sobre todo, la visión que se proyecta de la defensa de la seguridad nacional a través de su vinculación con la protección de los datos personales de los ciudadanos. Este planteamiento es el que permite, en el marco del artículo 23 de la LSN[910], determinar el verdadero alcance de la situación de interés para

[910] El artículo 23.2 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional establece que "La situación de interés para la Seguridad Nacional es aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la

Ediciones Universidad de Salamanca | CC BY-NC-ND

la Seguridad Nacional, trascendiendo de la mera naturaleza esencial o crítica del sujeto atacado lo cual, por ejemplo, ha permitido llevar a cabo operaciones policiales judicializadas en la Audiencia Nacional contra ciberataques que han supuesto la exposición de millones de datos de ciudadanos españoles de bases gubernamentales tan críticas como el Punto Neutro Judicial, la Agencia Estatal de Administración Tributaria o la Dirección General de Tráfico, entre otras[911].

Finalmente, en esta integración de la ciberamenaza como factor de riesgo para la seguridad española desempeña papel protagónico la Estrategia Nacional de Ciberseguridad de 2019 que, sobre la base que le dio su antecesora de 2013, presenta una nueva concepción del ciberespacio:

> "Es una dimensión fundamental para la estabilidad el preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad.
> El buen entendimiento de este planteamiento, exige trabajar con un enfoque multidisciplinar que abarque aspectos más allá de los puramente técnicos, bajo el principio de dirección centralizada y ejecución coordinada, con la afectación de la ciberseguridad a la Seguridad Nacional como competencia del Estado."[912].

Consciente de esta cada vez mayor vulnerabilidad del ciberespacio, el Informe Anual de Seguridad Nacional refleja, desde 2019, una permanente escalada de los parámetros de impacto y probabilidad que la determinan, llegando en 2023 a posicionarse como la principal fuente de amenaza para la seguridad nacional, tal y como refleja la siguiente imagen.

---

dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles, en los términos previstos en esta ley".

[911] La Policía Nacional detuvo en marzo de 2023 en Madrid a un conocido ciberdelincuente conocido como Alcasec que, a través de la vulneración de credenciales de acceso, fue escalando privilegios en los sistemas informáticos de diferentes instituciones públicas hasta acceder a datos confidenciales y restringidos, entre otros del Punto Neutro Judicial del Consejo General del Poder Judicial. Con los datos exfiltrados desarrolló una plataforma de consulta –Udyat- a través de la que monetizaba el fruto de sus delitos, que ocultaba a través de una compleja estructura de mixers de criptomonedas. Lo relevantes del caso es la clasificación de estos ciberataques, por primera vez en España, como amenaza grave a la Seguridad Nacional por su magnitud, alcance y afectación a millones de datos personales de ciudadanos españoles. Disponible en: https://elpais.com/espana/2023-04-03/detenido-el-joven-hacker-alcasec-en-la-causa-sobre-el-ciberataque-al-poder-judicial.html
https://www.abc.es/espana/alcasec-detenido-hackeo-punto-neutro-judicial-20230403113056-nt.html
https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=15523#
https://www.larazon.es/espana/audiencia-nacional-luz-verde-procesamiento-dos-hackers-que-atacaron-punto-neutro-judicial_202401046596af29cf86730001c74a71.html (12/01/2024).

[912] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. BOE núm. 103, de martes 30 de abril de 2019. Página 43441.

Ediciones Universidad de Salamanca | CC BY-NC-ND

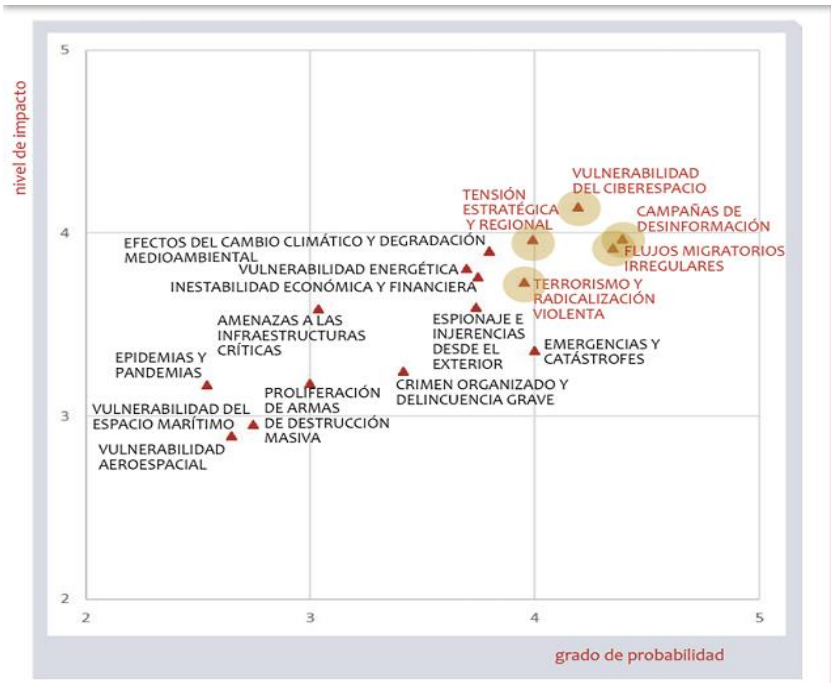


Gráfico 4.4.
Mapa de riesgos para la Seguridad Nacional 2023
Fuente: Informe Anual de Seguridad Nacional 2023. Presidencia del Gobierno

Queda de esta manera evidenciada la íntima relación entre la ciberamenaza y la seguridad nacional, así como el compromiso de España con la estrategia de ciberseguridad que la UE viene definiendo como marco de acción conjunta para facilitar un mundo físico y digital más seguro, marcado por un ritmo de cambio acelerado en el que la tecnología y la transformación digital son los exponentes de las nuevas oportunidades y, también, de las nuevas amenazas a la seguridad.

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 5. EVOLUCIÓN DE LAS AMENAZAS A LA SEGURIDAD Y SU VINCULACIÓN CON LA SINGULARIDAD DEL CIBERESPACIO

Una vez estudiados los conceptos de soberanía y seguridad y analizada su vinculación con el poder político, parece más natural avenirse a la idea de que, desde el momento en que la humanidad supera la fase de la economía de subsistencia y comienza a acumular riqueza y poder, no es posible comprenderla sin la realidad de la guerra, contexto de lucha para alcanzar la superioridad convertida en una constante en la evolución de las sociedades y que, con ellas, se ha ido transformando de acuerdo a sus principios, valores, estructura, forma política y tejido económico. Desde la Antigüedad Clásica hasta la época moderna la guerra era señal de poder e, incluso, de prestigio asimilado a la nobleza y la defensa de los más elevados valores a través de las armas, como el mismo don Quijote manifiesta en su *curioso discurso de las armas y de las letras* donde "todo en él rezuma alabanza, sobrepujo y hasta exageración magnificadora" para ensalzar a las primeras (CAZORLA PRIETO, 2018, pág. 25).

Sin embargo, es a partir de las dos Guerras Mundiales del pasado siglo, caracterizadas por la afectación total a civiles y combatientes, y la potencia destructora inusitada que la bomba atómica desvela en Hiroshima y Nagasaki cuando, al tiempo que germina en la sociedad el miedo por lo que puede pasar en la partida de bloques de la Guerra Fría, comienza a arraigar en ella la percepción negativa de la guerra y, de su mano, un cambio cultural que conlleva su rechazo, el cual se instrumentaliza y subyace como *leitmotiv* en nuevas tendencias ideológicas[913] que se suman a la *doctrina de las cero bajas*[914] (BAQUÉS QUESADA, 2021, págs. 83-86), porque no están dispuestas a asumir los costes que comporta cualquier conflicto bélico, aunque el Derecho Internacional lo considere un modo legítimo para que los Estados diriman sus controversias.

El fin del equilibrio del miedo que supone la caída del muro de Berlín y el posterior desmoronamiento de la URSS abre, principalmente en Occidente, una senda de amplias expectativas de paz que, desafortunadamente, choca con la realidad que ha acompañado desde su nacimiento al siglo XXI, con conflictos que han evolucionado mediatizados por el escenario internacional, ahora multipolar y de geometría variable, que genera novedosas formas de enfrentamiento muy alejadas de la clásica concepción de la guerra, no en tanto a su naturaleza como en su morfología. El progresivo y desigual aumento demográfico mundial, los consiguientes movimientos migratorios desde los países menos desarrollados a los más prósperos, el terrorismo internacional y la delincuencia organizada transnacional, los estados fallidos y su afectación al orden internacional, la aparición de nuevas enfermedades y pandemias de carácter global, el calentamiento de la tierra y la degradación del medio ambiente, y la consolidación del ciberespacio como nuevo dominio de confrontación entre Estados son algunas de las variables que conforman el contexto político, social y de seguridad del siglo XXI, lo que

[913] Pacifismo, desobediencia civil, objeción de conciencia y otros movimientos que vinculan la protección del medio ambiente, los derechos humanos y la paz como ideario opuesto a la guerra.
[914] La guerra sin bajas propias.

Ediciones Universidad de Salamanca | CC BY-NC-ND

nos lleva indefectiblemente a una panorámica de las nuevas amenazas que acompañan a esta era digital y de la información.

Así, posicionados desde el realismo al que nos obliga la evidencia de los tiempos, podemos decir que el progreso, los conflictos y las relaciones humanas son inseparables, tal y como sentencia el aforismo clásico *ubi societas, ibi bellum*[915]. Partiendo de esta premisa que nos permite aseverar que la amenaza evoluciona conforme lo hace la sociedad a la que afecta, nos centraremos en los tres principales retos de seguridad del siglo XXI, siguiendo como criterio de análisis el orden de prelación temporal conforme a su aparición en la sociedad a la que desafían: la guerra, el terrorismo y las ciberoperaciones.

5.1. La guerra: evolución desde el entorno físico al virtual

El viejo brocardo latino *si vis pacem para bellum*[916] consagra la evidencia de que la guerra constituye, por antonomasia, un acto político que evoluciona en paralelo al hombre, de forma que la consumación de violencia que comporta alcanza hasta donde acierta a señalar cada momento histórico. De esta forma, si el desarrollo humano llega hasta el manejo de la pólvora, también la guerra lo hará; y si alcanza a dominar una nueva dimensión virtual o, incluso, al control del espacio ultraterrestre, allí, sin duda, la guerra de igual forma habrá de llegar. Un claro ejemplo de ello lo tenemos con la modernización del nombre del *Ejército del Aire* español por el de *Ejército del Aire y del Espacio*[917], que denota la preocupación del Estado por adelantar la defensa a esos nuevos entornos vitales para su soberanía y la organización de su propia seguridad en el revolucionario panorama tecnológico y digital del siglo XXI (COELLO DE PORTUGAL, 2023, págs. 203-204).

Tan asimilada al ámbito de las categorías básicas del comportamiento político y social del hombre se encuentra la guerra -y su antagónica, la paz- que, incluso, las propias normas supremas de cada nación la regulan.

En nuestro caso, es el artículo 63.3 CE el que, dejando patente la función del Rey como símbolo de la unidad de España y máximo representante en las relaciones internacionales que, en nuestro sistema parlamentario, *reina pero no gobierna*, establece que:

> "Al Rey corresponde, previa autorización de las Cortes Generales, declarar la guerra y hacer la paz".

De esta manera, complementando al anterior y de acuerdo al artículo 97 CE, habrá de ser el Gobierno, en el marco de sus funciones de dirección de la defensa del Estado, el

[915] "Donde hay sociedad, hay guerra".
[916] "Si quieres la paz, prepárate para la guerra".
[917] Real Decreto 524/2022, de 27 de junio, por el que se dispone el cambio de denominación del Ejército del Aire por la de Ejército del Aire y del Espacio. BOE núm. 155, de 29 de junio de 2022. BOE-A-2022-10787. Disponible en: https://www.boe.es/eli/es/rd/2022/06/27/524

Ediciones Universidad de Salamanca | CC BY-NC-ND

que dé inicio al procedimiento parlamentario que concluya con la declaración de guerra por el Rey [918].

En cualquier caso, como decimos, la guerra forma parte consustancial del modelo de relaciones políticas entre Estados y, como tal, se consagra en sus marcos normativos.

5.1.1. La guerra clásica o convencional

Conviene a nuestro análisis comenzar previniendo que la esencia moral de la guerra ofrece dos caras de una misma realidad: la primera referida al *ius ad bellum*[919], el derecho a la guerra, que remite a las razones por las que los Estados llegan al conflicto, resultando así la guerra justa o injusta en base a las estimaciones que hagamos sobre la agresión y la legítima defensa; la segunda, el *ius in bello*[920], el derecho en la guerra, que alude a los medios con los que se lleva a cabo, suponiendo así que la guerra se haya desarrollado justa o injustamente de acuerdo a que en el combate se hayan observado o no las reglas acordadas internacionalmente (WALZER, 2001, pág. 51), que tienen su principal reflejo normativo en el Derecho Internacional humanitario formulado en los Convenios de Ginebra de 1949 y sus Protocolos adicionales[921].

Dicho lo anterior, conviene igualmente precisar que el término *guerra* no ofrece un concepto neto y fijo que perdure a través del tiempo y de las sociedades a las que, siempre, afecta:

> "La guerra no es un concepto estático; sus límites, además, son imprecisos en la medida en que no los marca necesariamente la violencia. Definir la guerra supone navegar por la Escila de la vaguedad y el Caribdis de un purismo que

[918] Artículo 97 de la Constitución Española: "El Gobierno dirige la política interior y exterior, la Administración civil y militar y la defensa del Estado. Ejerce la función ejecutiva y la potestad reglamentaria de acuerdo con la Constitución y las leyes".

[919] El *ius ad bellum* está fundamentado en el Carta de las NNUU y en el Derecho Internacional consuetudinario. De esta forma, se prohíbe el recurso al uso de la fuerza en las relaciones entre Estados, salvo en unas señaladas excepciones que lo legitiman.

[920] El *ius in bello* se fundamenta en el Derecho Internacional humanitario, representado en los Convenios de Ginebra y sus Protocolos Adicionales, cuyo objetivo no es otro que imponer límites para proteger a las víctimas de los conflictos armados, cuya legalidad se vincula a que se produzcan en el marco de alguna de las excepciones amparadas por la Carta de las NNUU para el uso de la fuerza entre Estados.

[921] Los cuatro Convenios de Ginebra originales se firmaron el 12 de agosto de 1949. El I Convenio de Ginebra protege, durante la guerra, a los heridos y los enfermos de las FFAA en campaña. El II Convenio de Ginebra protege a los heridos, los enfermos y los náufragos de las FFAA en el mar. El III Convenio de Ginebra se refiere al trato debido a los prisioneros de guerra. El IV Convenio de Ginebra protege a las personas civiles en tiempo de guerra, distinguiendo entre la situación de los extranjeros en el territorio de una de las partes en conflicto y la de los civiles en territorios ocupados. En respuesta al aumento del número de conflictos armados no internacionales y de guerras de liberación nacional, el 8 de junio de 1977 se aprobaron dos Protocolos adicionales a los cuatro Convenios de Ginebra de 1949, el I para la protección de las víctimas de los conflictos armados internacionales, y el II para las víctimas de los conflictos no internacionales. El 8 de diciembre de 2005, se aprobó un tercer Protocolo adicional que establece el *cristal rojo* como signo distintivo con el mismo estatuto internacional que los emblemas de la *cruz roja* y la *media luna roja.* Los Convenios de Ginebra han sido ratificados por todos los Estados y son aplicables universalmente. Disponible en: https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/state-parties (29/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> permanentemente exige de definiciones, cuando además el concepto ha sufrido un proceso de evolución" (AZNAR FERNÁNDEZ-MONTESINOS, 2011, pág. 26).

Una vez puntualizada esta idea, debemos comenzar citando al general, filósofo y estratega chino Sun Tzu, autor del tratado de tácticas y estrategias castrenses del siglo V a.C. *El arte de la guerra*, para el que ésta es cuestión grave y como tal determina la política de un Estado:

> "La guerra es un asunto de importancia vital para un estado; constituye la base que determina la vida o la muerte; el camino hacia la supervivencia o hacia la aniquilación. Es por lo tanto indispensable conocerla y estudiarla" (SUN TZU, 2007, pág. 13).

Más ajustado al pensamiento occidental del siglo XVII entiende Hobbes en su *Leviathan* que todo modo de relación humana que no se estructure en torno a un poder absoluto deviene en guerra, por la propia naturaleza del hombre:

> "Durante el tiempo en que los hombres viven sin un poder común que los atemorice a todos, se hallan en la condición o estado que se denomina guerra; una guerra tal que es la de todos contra todos. Porque la guerra no consiste solamente en batallar, en el acto de luchar, sino que se da durante el lapso de tiempo en que la voluntad de luchar se manifiesta de modo suficiente. Por ello la noción del tiempo debe ser tenida en cuenta respeto a la naturaleza de la guerra, como respecto a la naturaleza del clima" (HOBBES, 2013, pág. 167).

Es ya en el primer cuarto del siglo XIX cuando se publica el principal tratado de ciencia militar, obra del general prusiano Carl von Clausewitz, *De la Guerra*, en la que se presenta la idea de que la guerra supone un acto de fuerza para imponer la voluntad propia al adversario:

> "La guerra no es otra cosa que un combate singular amplificado. Si queremos concebir como unidad la multitud de combates singulares que la constituyen, nada mejor que representarnos dos luchadores. Cada uno pretende, por medio de la fuerza física, someter al otro al cumplimiento de su voluntad; su fin inmediato es derribarlo e incapacitarlo para ulterior resistencia.
> La guerra es, pues, un acto de fuerza para obligar al contrario al cumplimiento de nuestra voluntad" (CLAUSEWITZ, 2021, pág. 21).

El filósofo alemán George W.F. Hegel, contemporáneo del general Clausewitz, en su obra *Filosofía del Derecho* sugiere que la guerra no es algo bueno en sí mismo pero puede ser aceptada en aras de un fin superior:

> "La paz perpetua con frecuencia se defiende como un ideal hacia el cual la humanidad ha de tender. Con este fin en perspectiva, Kant propuso una liga de monarcas que adecuasen las diferencias entre los estados, y la Sagrada Alianza se pretendió que fuera algo de este tipo. Pero el Estado es un individuo y la individualidad implica esencialmente negación. De aquí que si un número de estados se unen constituyendo una familia, este grupo como individuo ha de engendrar un agente opuesto y, por tanto, un enemigo. Como resultado de la guerra, las naciones se fortalecen y los pueblos envueltos en una guerra civil

Ediciones Universidad de Salamanca | CC BY-NC-ND

también logran la paz interna, haciendo las guerras fuera. Con toda seguridad las guerras producen inseguridad en la propiedad, pero esta inseguridad de cosas no es más que algo pasajero, además inevitable" (HEGEL, 1965, pág. 747).

También el Diccionario de la Real Academia Española define la guerra, presentando en sus tres primeras acepciones la perspectiva de la desavenencia, la lucha armada o la falta de paz entre potencias, naciones o facciones de ésta:

1. "Desavenencia y rompimiento de la paz entre dos o más potencias.
2. Lucha armada entre dos o más naciones o entre bandos de una misma nación.
3. Pugna (oposición o rivalidad)".

Por su parte, el profesor Díaz Fernández en su Diccionario de Inteligencia y Seguridad, la define como conflicto entre Estados donde rige la aplicación del Derecho de guerra, independientemente de que exista o no declaración como tal:

> "Tradicionalmente, en Derecho Internacional, lucha armada entre Estados destinada a imponer la voluntad de uno de los bandos en conflicto y cuyo desencadenamiento provoca la aplicación del Derecho de guerra consuetudinario y convencional, independientemente de que exista o no declaración de guerra" (DÍAZ FERNÁNDEZ, y otros, 2013, págs. 149-150).

Coinciden estas dos últimas enunciaciones en el componente fundamental de la guerra, entendida como lucha armada que tiene lugar entre Estados o naciones, por un enfrentamiento o desacuerdo que deviene en quebranto de la situación de paz previa entre ellos. La segunda acepción puntualiza aún más indicando que dicha acción está destinada a imponer al contrario la voluntad propia, siendo aplicable a la contienda el Derecho Internacional de guerra y humanitario.

Ambas acepciones conforman una aproximación al término que sigue la línea trazada por Clausewitz en su obra *De la Guerra*, en la que desarrolla un marco conceptual en el que se integran todos los elementos sustanciales del conflicto armado clásico: los Estados como únicos actores en escena que persiguen el objetivo concreto de destruir al enemigo mediante el enfrentamiento armado, bajo una dimensión humana controlada por cuanto sólo se enfrentan los ejércitos de ambas partes, regulares y simétricos en cuanto a capacidades, en un marco espacial concreto delimitado por el campo de batalla, con una motivación superior cifrada en la defensa del Estado y los intereses de la nación, y todo ello bajo las reglas que marca el *ius in bello*.

En cuanto a los intereses que pueden incitar y, en su caso, justificar el recurso a la guerra, el general prusiano aprecia que ésta se asocia íntimamente con la política, lo que implica que el propósito político -mayormente la lucha por el poder- sea el objetivo del conflicto y la guerra el medio para su consecución:

> "Así vemos, pues, que la guerra no es simplemente un acto político, sino un verdadero instrumento político, una continuación de las relaciones políticas, una gestión de las mismas con otros medios. Queda sólo como exclusivo de la guerra la peculiar naturaleza de sus medios" (CLAUSEWITZ, 2021, pág. 38).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Chomsky va más allá en la consideración de esta simbiosis al argumentar que los intereses políticos que determinan las guerras son complejos y multidimensionales, por lo que suelen diferir y prevalecer sobre los del pueblo ya que atienden a la formación de sus propias estrategias orientadas a ganar en la contienda:

> "Las guerras raramente son un asunto simple, en el que un antagonista (un estado-nación) se enfrenta a otro. Siempre tienen múltiples dimensiones" (CHOMSKY, 1994, pág. 108).

En este mismo sentido, Ottone aboga por intereses propiciatorios de la guerra entroncados con la misma naturaleza humana -poder, riquezas, conquista de territorio- que se disfrazan con falsos argumentos culturales, identitarios o religiosos, entre otros:

> "En verdad, los conflictos de ayer y de hoy, incluso aquellos que se revisten como portadores de reclamos identitarios o al contrario de una pretendida responsabilidad universalista, nunca tienen un carácter puramente civilizacional. Se mezclan siempre con razones menos elevadas, con cosas que suelen ser más concretas y terrenales como el poder, la conquista territorial o el dominio económico. El argumento civilizacional, cultural, identitario o religioso es muchas veces la cobertura emocional necesaria para la movilización bélica. En cierta medida le otorgan "sus cartas de nobleza" (OTTONE, 2017, págs. 55-56).

No obstante, volviendo al general prusiano, la política no es el único factor que determina la guerra, sino uno de los tres factores que conforman, según sus palabras, *una maravillosa trinidad*:

> "[…] constituye una maravillosa trinidad, compuesta del poder primordial de sus elementos, del odio y la enemistad que pueden mirarse como un ciego impulso de la naturaleza; de la caprichosa influencia de la probabilidad y el azar, que la convierten en una libre actividad del alma; y de la subordinada naturaleza de un instrumento político, por la que recae puramente en el campo del raciocinio.
> El primero de estos aspectos es más bien propio de los pueblos; el segundo de los generales y sus Ejércitos; y el tercero, de los Gobiernos. Las pasiones que se han de inflamar en la guerra es preciso que ya existan en los pueblos; el desarrollo que tome la acción del valor y del talento en el reino de las probabilidades del azar depende de las cualidades del general y del Ejército; los fines políticos, en cambio, pertenecen exclusivamente a los Gobiernos" (CLAUSEWITZ, 2021, pág. 40).

Se trata de un constructo conceptual de Clausewitz para conectar a gobernantes, gobernados y militares en un todo integrado y dinámico que permita afrontar con garantía de éxito la pugna:

1. El elemento *pasional*, el pueblo, que permanece al margen de la guerra pero la sostiene con su fuerza irracional e impulsiva.
2. El elemento *volitivo*, el ejército, que aporta su impulso, su valor y su destreza en el empleo de la fuerza.
3. El elemento *intelectual*, el Estado como estructura política, que dirige y determina el objetivo que ha de tener la guerra y que aplica la razón para que no se vuelva caótica e impredecible.

Ediciones Universidad de Salamanca | CC BY-NC-ND

A través de esta tríada, que posee un claro enfoque estatocéntrico, Clausewitz sustenta el convencimiento de que la guerra es un medio legítimo para defender los intereses del Estado –territorio, población, autoridad- cuya intensidad se gradúa conforme al fin buscado frente al contrario, y que dispone de una dimensión y alcance limitados por cuanto no afecta al global de la sociedad, únicamente a los ejércitos en liza y siempre bajo las reglas que dicta el Derecho Internacional. En este mismo sentido, los objetivos que deben alcanzar los militares son marcados por el poder político y aquellos deben confiar en que las victorias conseguidas en el campo de batalla se gestionarán de la mejor manera posible para el conjunto del Estado. En todo caso, la victoria militar es la que, en definitiva, decide la disputa entre los dos Estados enfrentados (FREEDMAN, 2019, págs. 151-155).

Para Clausewitz la guerra es, por tanto, un instrumento subordinado a la política cuya finalidad es la paz, entendiendo ésta como la nueva situación generada tras el conflicto, de tal forma que sin la política no puede entenderse la guerra, pero tampoco la paz, que al igual que aquella es un acto político (AZNAR FERNÁNDEZ-MONTESINOS, 2011, págs. 29-31).

Pero este concepto clásico de la guerra es matizado por la necesaria adaptación al contexto y la lógica evolución que, para superar al contrario, lleva a las partes a mejorar sus propias capacidades y recursos o, aplicando otra estrategia, debilitar los del adversario. Esto viene condicionado tanto por el progreso de la técnica aplicada al combate -la innovación militar- como por otros factores de carácter político, económico o social. En este sentido, el siglo XIX supone un punto de inflexión por cuanto las sinergias generadas entre la ciencia moderna y la guerra alcanzan una nueva dimensión, auspiciada por la dedicación en exclusiva de un sector de la rama investigativa a la evolución tecnológica castrense:

> "A partir de entonces, la ciencia y la técnica se subordinaría de manera inevitable a la guerra, en una dinámica que culminaría en el paradigma nuclear, conocido como Proyecto Manhattan, que apenas un siglo después se convertiría en el más célebre y estremecedor exponente de la aplicación de los conocimientos científicos al desarrollo de la tecnología armamentística" (GARCÍA HERNÁN & CATALÁ MARTÍNEZ, 2012, pág. 233).

La innovación militar entendida como "transformación significativa en la forma de combatir de los ejércitos motivada por cambios en los procedimientos operativos y en la organización militar" (COLOM PIELLA & VALES CALDERÓN, 2023, pág. 76), modifica los procedimientos de combate de los ejércitos e incluso, si su aplicación comporta la obsolescencia del estilo de batallar anterior, puede trascender el ámbito castrense otorgando una superioridad estratégica determinante y de ámbito global al Estado que la posea, con las consiguientes transformaciones que conlleva a todos los niveles, incluidos el social, el político o el económico. El término que define este proceso es el de *Revolución Militar (RM)*, siendo que a lo largo de la historia únicamente podemos referirnos a 5 de ellas: la creación del Estado Moderno y los ejércitos permanentes, la Revolución Francesa como generadora de las bases del estado-nación actual, la Revolución Industrial y su aportación de nuevos recursos para crear armas altamente

Ediciones Universidad de Salamanca | CC BY-NC-ND

destructivas, el concepto de guerra total y la subordinación de toda la sociedad en beneficio de la maquinaria militar que supusieron las dos Guerras Mundiales, y la revolución nuclear (NIETO FERNÁNDEZ, 2012, págs. 853-854).

Cuestión relacionada pero distinta es la *Revolución en los Asuntos Militares (RAM)*, que implica una mejora en los procedimientos de combate por la aplicación de la innovación tecnológica, que supone un mayor eficacia y eficiencia operativa, pero necesariamente respaldada por nuevas doctrinas y nuevas formas de organización de las propias FFAA, para que la revolución alcance el nivel estratégico adecuado. La tecnología es así uno de los mejores catalizadores de cualquier transformación pero no es suficiente en sí misma, por lo que será la profundidad con que ésta se acometa -doctrina, organización- la que determine si estamos ante una RM o una RAM, sin olvidar que la transformación, aún siendo necesaria, no garantiza el progreso (NIETO FERNÁNDEZ, 2012, pág. 857).

En todo caso, los avances tecnológicos se identifican a lo largo de la historia como uno de los principales motores de cambio en lo concerniente a la guerra, de manera que:

> "[…] aunque la naturaleza del conflicto -que es política, social, violenta e impredecible- persista, cuando se analiza la evolución de su carácter, el impulso tecnológico es uno de los elementos invariables que contribuyen a marcar la diferencia con el anterior" (HERNÁNDEZ GARCÍA, 2024, pág. 9).

Es así que los ejércitos se ven forzados, desde siempre, a evolucionar adaptándose de manera continua y, a poder ser, más rápido que sus contendientes, a las nuevas tecnologías y modos de combatir para tratar de garantizar su prevalencia en el campo de batalla. Aprovechando esta realidad, la disciplina castrense ha tratado de organizar este proceso evolutivo marcando hitos con los que teorizar sobre las características definitorias de la guerra y sus procedimientos a lo largo de los tiempos, para distinguirlas, clasificarlas y parametrizarlas hasta llegar al momento actual, global, ambiguo y tecnologizado, con las denominadas *guerras híbridas*.

A estas nos referiremos a continuación, no sin antes advertir que no serán desarrolladas aquí esas tipologías que distinguen los teóricos de la guerra, cuya sistematización en guerras de primera, segunda, tercera y cuarta generación[922] (AZNAR FERNÁNDEZ-MONTESINOS, 2024, págs. 177-254) o, en otro sentido, guerras premodernas, modernas y postmodernas, no es pacíficamente reconocida por la doctrina ya que, otros autores,

[922] Siguiendo a Aznar Fernández-Montesinos, las guerras de primera generación ocupan el periodo temporal entre el Renacimiento y el siglo XVII, caracterizadas por ejércitos nacionales y organizados que luchan en *orden de batalla* y buscan el enfrentamiento directo. Las guerras de segunda generación abarcan desde el siglo XVIII hasta la Segunda Guerra Mundial, en las que se implica a la nación en su conjunto y se llevan al campo de batalla a través de ejércitos burocratizados. Las guerras de tercera generación engloban desde mitad del siglo XX hasta comienzos del XXI, y son conflictos donde la clave es la integración de movimiento, velocidad y capacidad de maniobra de las tropas que, aplicando su fuerza superior, tratan de establecer contacto con el enemigo lo antes posible para vencer rápidamente y no sufrir bajas. Las guerras de cuarta generación, propias del siglo XXI, se caracterizan por la asimetría de los contendientes, que se enfrentan en conflictos desmilitarizados y privatizados cuyos límites ya no marcan los Estados. Frente a la velocidad, la tecnología y sofisticación armamentística de los ejércitos convencionales aparece la estrategia lenta de las guerrillas, con armas sencillas y combatientes dispuestos a suicidarse para desgastar el enemigo.

Ediciones Universidad de Salamanca | CC BY-NC-ND

entienden que las líneas de continuidad histórica señaladas son demasiado evidentes como para marcar tantas diferencias entre los distintos tipos de conflictos cinéticos a lo largo del tiempo (BAQUÉS QUESADA, 2021, págs. 63-69), y ello nada habría de aportar al objeto de nuestro estudio orientado a las amenazas modernas y, en concreto, la desinformación como amenaza a la seguridad nacional.

5.1.2. La guerra híbrida

Por esta razón nos centramos en la guerra híbrida, cuyo concepto trata de definir los conflictos del siglo XXI como una lógica evolución de la guerra clásica. Para ello, hay que retrotraerse a finales de los años noventa del pasado siglo cuando la doctrina militar comienza a manejar el término de *guerra compuesta*, en la que, de un mismo lado, fuerzas regulares -convencionales- e irregulares -no convencionales- combaten como fuerzas separadas pero coordinadas bajo una misma dirección, la cual ordena sus acciones para alcanzar los objetivos planificados. En este modelo las fuerzas irregulares, a modo de insurgencia, se utilizan para favorecer el avance de las convencionales, que son las que soportan el peso del triunfo final en la contienda (GARCÍA GUINDO & MARTÍNEZ-VALERA GONZÁLEZ, 2015, pág. 3).

El concepto teórico de *guerra híbrida* es desarrollado en el año 2005 por los militares estadounidenses Mattis y Hoffman en su artículo *Future Warfare: The Rise of Hybrid Wars*[923], en el que comienzan a plantear la *guerra híbrida* como una fusión de modos, medios y tácticas de combate donde el enfrentamiento se produce entre tropas regulares o convencionales y adversarios irregulares o, simplemente, menos convencionales. A su entender, esta situación se genera como una adaptación natural al escenario marcado por la supremacía militar occidental, por cuanto el enemigo también es un ser humano que, a través de su inteligencia creativa, analiza el modo clásico de hacer la guerra, saca conclusiones y trata de compensar sus propias debilidades mitigando la superioridad del contrario:

> "But our conventional superiority creates a compelling logic for states and non-state actors to move out of the traditional mode of war and seek some niche capability or some unexpected combination of technologies and tactics to gain an advantage. Thus, we need to explore the nature of alternative challenges and the corresponding investments we must make to better posture ourselves for a projected world of more unconventional adversaries" (MATTIS & HOFFMAN, 2005)[924].

[923] *Guerra futura: el auge de las guerras híbridas*. Autores: teniente general James N. Mattis y el teniente coronel Frank Hoffman, del Cuerpo de Marines de EE.UU. Disponible en: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars (09/03/2024).

[924] "Pero nuestra superioridad convencional crea una lógica convincente para que los estados y los actores no estatales abandonen el modo tradicional de hacer la guerra y busquen alguna capacidad de nicho o alguna combinación inesperada de tecnologías y tácticas para obtener una ventaja. Por lo tanto, necesitamos explorar la naturaleza de los desafíos alternativos y las correspondientes inversiones que debemos hacer para posicionarnos mejor ante un mundo proyectado de adversarios menos convencionales" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Desde esta perspectiva de Mattis y Hoffman, la *guerra híbrida* no acaba con el arquetipo westfaliano sino que, al contrario, supone una nueva adaptación, interpretándose así como una guerra moderna en la que se combinan, por un lado, las fuerzas convencionales con sus procedimientos y medios tradicionales y, por otro, los actores no estatales que con sus tácticas asimétricas acrecientan su protagonismo, obligando con ello a reformular el paradigma del empleo de la fuerza como ejercicio supremo de la autoridad del Estado (BAQUÉS QUESADA, 2021, pág. 78).

Es así que en la guerra híbrida se trata de compensar la supremacía del adversario aprovechando las limitaciones que el uso de dicha fuerza impone, como la sujeción al Derecho Internacional Humanitario (DIH) y el resto del acervo normativo que conforma la deontología militar, la voluntad y decisión de los dirigentes políticos para soportar el desgaste consustancial al esfuerzo de guerra, o el respaldo de la prensa y de la opinión pública al conflicto. Conforme a ello, la idiosincrasia de la guerra híbrida se construye en torno a la supervivencia de los contendientes y el equipo para sostener el esfuerzo[925], el uso de armas altamente eficaces y efectivas[926], con alta capacidad de causar bajas al enemigo[927], y el aprovechamiento de todas las esferas de comunicación para manejar la narrativa y tratar de socavar la moral y la legitimidad del oponente, de forma que:

> "[…] podemos concluir que los actores que utilizan la guerra híbrida definen sus objetivos estratégicos y emplean para ello el arte operacional sin restricciones para alcanzarlos. Utilizan asimismo en el campo táctico, operaciones distribuidas y simultáneas, tanto regulares como irregulares junto con acciones de nivel operacional, que desafían la cultura e incluso las normas de la guerra de los estados occidentales, todo ello coordinado en tiempo, espacio y propósito para alcanzar los objetivos estratégicos" (GARCÍA GUINDO & MARTÍNEZ-VALERA GONZÁLEZ, 2015, pág. 9).

Esta situación pone a los países occidentales en la tesitura de tener que adaptarse a estas nuevas formas de acción cinética que cambian el paradigma del enfrentamiento con el enemigo, hasta el punto de que lo que está en juego, en definitiva, es la manifestación creíble de la voluntad de utilizar la fuerza por quien ostenta la supremacía militar y tecnológica que, por cuestiones internas como la desafección política, la volubilidad de la opinión pública, el escepticismo social, el arraigo de la *doctrina de las cero bajas* o el cálculo de costes políticos y consecuencias electorales, puede ver como la capacidad disuasoria de su poder queda cuestionada frente a esos adversarios irregulares que aprovecharán esta debilidad para plantear su estrategia y compensar la superioridad de aquel en el terreno convencional (COLOM PIELLA, 2018, pág. 42).

[925] Para este fin se utilizan los bunkers, las técnicas de camuflaje y engaño, la confusión intencionada de instalaciones civiles y militares, el enfrentamiento en zonas urbanas, el uso de tácticas de guerrilla, el empleo de fuerzas especiales y paramilitares, etc.

[926] Se trata de utilizar armas de contenida inversión económica y alta rentabilidad en combate, como cohetes guiados y munición de artillería de precisión que contrarresten la supremacía aérea o de plataformas de combate del adversario.

[927] Se busca el mayor número posible de bajas de civiles o de combatientes, tanto personales como materiales.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Siguiendo al profesor Colom Piella, podemos especificar la esencia de la guerra híbrida como un estilo de confrontación propia del siglo XXI, donde se combinan de manera eficaz a la vez que se integran temporal y espacialmente procedimientos, medios y tácticas convencionales e irregulares en los dominios físicos y digital -terrorismo, propaganda, subversión, insurgencia, conexión con el crimen organizado, ciberoperaciones-, para cuya ejecución se emplea armamento tecnológicamente avanzado de distinta procedencia, con manifiesto desprecio por el *ius in bello*, y en cuyo contexto se maximiza la explotación de la *propaganda* y las *narrativas en red* para legitimar la causa propia y erosionar el soporte social del oponente (COLOM PIELLA, 2018, pág. 42).

Es evidente con ello que, en la guerra híbrida, ni los procedimientos, ni los medios ni la interlocución de los combatientes se parecen a los empleados en épocas pretéritas. Se ha producido un cambio en la esencia misma del conflicto sustentado, en parte, por la propia evolución social, fruto de la cual muchos de los combatientes ya son *nativos digitales*, lo que supone una serie de destrezas y habilidades *per se* en el componente humano de la fuerza que, a su vez, se traduce en una mayor disposición para aprovechar en el ámbito de confrontación de los nuevos dominios, como el ciberespacio, lo que viene a apoyar la tesis de que la *guerra híbrida* es:

> "[…] un terreno de juego en el que las capacidades del teóricamente más débil y del más fuerte, están mucho más equilibradas de lo que lo estarían en una guerra convencional, al margen de si en unas ocasiones el fiel de la balanza se desequilibra en beneficio del uno, o del otro" (BAQUÉS QUESADA, 2021, pág. 108).

Sin embargo, a pesar del gran salto que supone respecto a la teoría clásica clausewitziana, el concepto de guerra híbrida desde el punto de vista académico es impreciso y se diluye por el uso inapropiado que se le da para referirse a cualquier tipo de acción no convencional que se produce en ese continuo que existe en las relaciones entre Estados, y que discurre desde la máxima corrección diplomática hasta la declaración abierta de guerra, en lo que viene denominándose como la *Zona Gris*.

Y es en este punto donde hay que precisar que, como analizaremos más adelante, la utilización de acciones coordinadas y sincronizadas de carácter híbrido -ciberataques, desinformación, propaganda, maniobras en frontera- para explorar o atacar las vulnerabilidades sistémicas de un oponente, quedarán encuadradas en la ambigüedad propia de la *Zona Gris* en tanto en cuanto no exista una confrontación armada declarada y abierta, momento en que pasarán a formar parte de esa guerra híbrida entre contendientes -estatales o no estatales- que, ampliando la tradicional linde del campo de batalla, integran el uso sincronizado de medios militares -convencionales y menos convencionales- con otros instrumentos de poder -económicos, políticos, diplomáticos- que se ponen a disposición del objetivo final, que no es otro que socavar la capacidad de respuesta del adversario y llevarle a la derrota.

De esta forma, habremos de referirnos a guerra híbrida solo en el supuesto de que exista un conflicto armado. A partir de esta consideración, es decir, de que nos hallemos ante una guerra *stricto sensu*, será de aplicación el DIH asi como el resto del Derecho

Ediciones Universidad de Salamanca | CC BY-NC-ND

Internacional, por ejemplo, en lo relativo a la activación del *derecho de legítima defensa* ante una agresión que, conforme al artículo 51 de la Carta de las NNUU, solo se activa por el ataque armado de otro Estado (GALÁN, 2018, págs. 12-16).

En este *campo de batalla extendido* que supone la guerra híbrida, la morfología militar convencional que opera desde el código de conocimiento del entorno, la protección frente a la detección y el ataque al enemigo, ya no alcanza a cubrir todo el espectro de acción y necesita ser complementada para lograr sus objetivos. De esta forma, la política, la economía, la diplomacia, las capacidades militares, civiles e informativas y cualquier otra faceta del poder nacional o internacional del actor en liza se combinan de manera simultánea en los dominios terrestre, marítimo, aéreo, espacial y cibernético, y, a su vez, en las tres dimensiones de efectos -física, virtual y cognitiva-[928] para que el comandante de la fuerza ofensiva pueda tener un completo y acertado *engagement space*[929] que le permita llevar a cabo *operaciones multidominio (MDO),* en las que utilizar todas estas capacidades a su disposición para obtener la ventaja frente al adversario. Para ello, es necesario también integrar el componente de *transformación digital* que conlleva la permanente innovación informática y de las comunicaciones, la ventaja asociada a las Tecnologías Emergentes y Disruptivas (EDT)[930] y, sobre todo, la disposición de *información* de calidad y en tiempo real que permita la generación de *inteligencia* con la que apoyar la toma de decisiones oportunas.

Son las MDO las que definen el éxito en el *campo de batalla extendido*, integrando acciones simultáneas en todos los dominios para aprovechar cualquier tipo de ventaja que pueda derivarse y utilizarla para abrir paso a las tres dimensiones de efectos. Pero todo este complejo componente de la guerra híbrida no es fácil de coordinar ni, tampoco, debe interpretarse como la epifanía de la llamada *ciberguerra* a costa de la pérdida de efectividad de la operación cinética convencional. Estas, al menos, parecen ser algunas de las lecciones aprendidas de la última guerra en activo que vivimos en Europa: la guerra de Rusia contra Ucrania.

5.1.3. El nuevo modelo de confrontación: la simbiosis entre el pasado y el futuro

La invasión rusa de Ucrania ha despertado a Europa de la feliz ensoñación por la que, tras la traumática experiencia de la Segunda Guerra Mundial, no era posible una guerra en su territorio. Y esta ilusión, bruscamente rota por el Kremlin el 24 de febrero de 2022, pone de manifiesto, entre otras cuestiones, la ingenuidad y el idealismo que subyacían en el afán europeo de manejar sus relaciones con Rusia desde el *soft power*, presumiendo que la imbricación de intereses económicos, comerciales e, incluso,

[928] Los dominios tienen tres dimensiones de efectos: la física, donde se produce la actividad física que trata de anular la capacidad del contrario, la virtual, donde se genera la actividad intangible principalmente referida al flujo de la información, y la cognitiva, donde se origina la percepción humana y, conforme a ella, se toman las decisiones.

[929] El *engagement space* puede considerarse la visión global del entorno de conflicto, la comprensión de la situación exacta del *campo de batalla extendido* de la guerra híbrida, en el que se integra toda la información disponible para la toma de decisiones que permitan operativizar las capacidades ofensivas en los cinco dominios.

[930] Dentro de las Tecnologías Emergentes y Disruptivas (EDT) cabe considerar el Big Data, la tecnología cuántica, la IA y la tecnología espacial, entre otras.

Ediciones Universidad de Salamanca | CC BY-NC-ND

políticos entre ellos supondría un aval para mantener apaciguada a la bestia por mucho que, en la Conferencia de Seguridad de Múnich de 2007[931], Putin ya dejara claro su parecer en cuanto a la falta de respeto a los valores democráticos y al Derecho en el *nuevo orden mundial* exento de la amenaza de la *destrucción mutua asegurada*[932], al tiempo que se mostraba preocupado por el ánimo expansionista de la OTAN y anticipaba un papel mucho más activo de Rusia como actor de relevancia internacional, dando inmediata prueba de esta política asertiva con su actuación en Georgia y, posteriormente, en Crimea[933].

A ello hay que sumar que ni la diplomacia ni la disuasión han funcionado, probablemente por el exceso de confianza mostrado por ambas partes: Europa suponiendo que Rusia nunca aplicaría la fuerza militar convencional para manejar su política exterior, y ésta creyendo que ese uso de la fuerza -la cual estaba sobrevalorada respecto a sus capacidades- le garantizaría una superioridad absoluta con la que alcanzar fácilmente su objetivo en Ucrania (CALVO ALBERO, 2022, pág. 90).

La *operación militar especial* que el Kremlin vendió internamente como una maniobra rápida, precisa, quirúrgica, supuestamente apoyada por la población rusófila ucraniana que necesitaba ser auxiliada frente al neonazismo de Kiev y que, conforme a la experiencia reciente, no comportaría respuesta alguna por parte de la inoperante Europa, se desvaneció al primer contacto con la realidad:

> "Cuando el 24 de febrero los ciberataques rusos no paralizaron las infraestructuras críticas ucranianas, sus misiles no destruyeron su sistema de mando y control o defensa antiaérea, sus acciones de sabotaje no surtieron los efectos esperados, sus operaciones informativas no minaron la moral de la población, las tres columnas que debían converger en Kiev quedaron atascadas lejos de la capital y el asalto aerotransportado sobre el aeropuerto Hostómel quedó aislado sin refuerzos terrestres, la "operación militar especial" aprobada por Putin chocó con la realidad. Ni el Gobierno ucraniano se derrumbó, ni la resistencia civil se diluyó, ni el Ejército ruso entró como liberador del país" (COLOM PIELLA & CÓZAR MURILLO, 2023, pág. 10).

Y esta misma realidad se ha ocupado de lanzar a la palestra el papel que el ciberespacio está teniendo en la evolución del conflicto ucraniano y, también, su nivel de integración en el planeamiento estratégico de ambos bandos, máxime cuando gran parte de las proyecciones sobre el desarrollo de los conflictos del futuro sostiene que la capacidad ofensiva en el quinto dominio representa la clave del esfuerzo de guerra.

Para analizar el alcance de la contribución de las operaciones cibernéticas al esfuerzo conjunto implicado en un conflicto amado de características convencionales, como por ahora está siendo el de Ucrania, debemos antes comprender cómo entiende cada una de las partes beligerantes el ciberespacio. En este sentido, el documento publicado en

[931] Vid. Supra. Apartado 2.2.3.
[932] Vid. Supra. Apartado 2.1.1.
[933] Con los territorios ocupados ilegalmente por Moscú en 2008 en Osetia del Sur y Abjasia (Georgia) y, en 2014, en Crimea (Ucrania).

Ediciones Universidad de Salamanca | CC BY-NC-ND

junio de 2021 por el NATO STRATCOM COE y el NATO Cooperative Cyber Defence COE, titulado *Russia´s Strategy In Cyberspace*, señala que:

> "From the Russian perspective, cyber warfare or the Russian equivalent 'information technological warfare', is only a part of the overarching concept of "information confrontation" (*informatsionnoe protivoborstvo*). The Russian Ministry of Defence describes the information confrontation as the clash of national interests and ideas, where superiority is sought by targeting the adversary's information infrastructure while protecting its own objects from similar influence […].
> The confrontation includes a significant psychological remit, whereby an actor attempts to affect informational resources (documents in information systems) as well as the minds of the adversary's military personnel and population at large. Ultimately, cyber operations (or information-technical means) are one of many methods used to gain superiority in the information confrontation. Russia, and particularly Russian President Putin's regime, sees the information confrontation as a constant geopolitical zero-sum competition between great powers, political and economic systems, and civilizations"[934].

Quiere ello decir que Rusia concibe el ciberespacio como el entorno en el que opera la *confrontación informativa*, que incluye no solo los intereses y valores nacionales que se hacen valer frente al adversario, sino también un componente psicológico enfocado al *ámbito cognitivo*, centrado en las opiniones de las personas y, consecuentemente, en su manipulación directa o indirecta. Desde esta perspectiva, la *confrontación informativa* implica una competencia geopolítica de suma cero entre los actores enfrentados, que la Federación Rusa viene haciendo visible en el tablero de juego internacional desde finales de la primera década del siglo XXI, donde la actividad en el ciberespacio ha funcionado como herramienta esencial en la Zona Gris, tanto para ganar influencia -a través de campañas desinformativas o de propaganda- como para recopilar información de sus enemigos -mediante el ciberespionaje-.

Este mismo documento recoge cómo interpreta la doctrina de la OTAN el *entorno de la información* dentro del quinto dominio[935], en respuesta a esa concepción geopolítica del

---

[934] "Desde la perspectiva rusa, la guerra cibernética o su equivalente ruso, la "guerra tecnológica de la información", es sólo una parte del concepto general de "confrontación informativa" (*informatsionnoe protivoborstvo*). El Ministerio de Defensa ruso describe la confrontación informativa como el choque de intereses e ideas nacionales, donde se busca la superioridad atacando la infraestructura de información del adversario y, al mismo tiempo, protegiendo sus propios objetivos de influencias similares […].
La confrontación incluye un importante cometido psicológico, mediante el cual un actor intenta afectar los recursos de información (documentos de los sistemas de información), así como las mentes del personal militar del adversario y de la población en general. En última instancia, las operaciones cibernéticas (o medios técnicos de información) son uno de los muchos métodos utilizados para ganar superioridad en la confrontación informativa. Rusia, y en particular el régimen del presidente ruso Putin, ve la confrontación informativa como una competencia geopolítica constante de suma cero entre grandes potencias, sistemas políticos y económicos, y civilizaciones" (Traducción propia).
Russia´s Strategy In Cyberspace, publicado en junio de 2021 por el NATO STRATCOM COE y el NATO Cooperative Cyber Defence COE. Página 5. Disponible en: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf (01/04/2024).

[935] La OTAN reconoce el ciberespacio como el quinto dominio de operaciones desde la Cumbre de Varsovia de 2016.

Ediciones Universidad de Salamanca | CC BY-NC-ND

ciberespacio que esgrime Rusia y que, desde 2014[936], ha demostrado saber utilizar en la Zona Gris. En este sentido:

> "NATO doctrine understands cyberspace as an operational domain and considers it as part of the information environment. This environment is '[…] comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information'. The information processed through this environment provides the base for cognitive processes that affect individual decision-making and subsequently, behaviour. Those processes happen in three dimensions – physical, virtual and cognitive – and cyberspace involves all three of them. In this respect, NATO's concept of the information environment is not that different from Russia's understanding of 'information space' and the role of cyberspace within it"[937].

Así, la doctrina OTAN entiende el ciberespacio como un dominio de las operaciones que forma parte del *entorno de información*, integrado por la propia *información*, por un *componente físico* -los sistemas que procesan, reciben y transmiten dicha información- e, indudablemente, por un *componente personal* -los individuos-. Este *entorno de información* que opera en las dimensiones física, virtual y cognitiva, sustenta las claves que determinan las decisiones y los comportamientos de las personas involucradas en el mismo. Parece, conforme a lo anterior, que tanto Rusia como OTAN coinciden en su interpretación del ciberespacio como parte del *entorno de confrontación informativa* y, por ello, elemento fundamental de la estrategia geopolítica.

Por su parte, la doctrina de la Fuerza Aérea estadounidense, al definir el ciberespacio como dominio global, también lo ubica en el *entorno de la información* y considera que se compone de los sistemas de soporte de red y los datos alojados, las telecomunicaciones y el hardware sobre el que opera:

> "Cyberspace is a global domain within the information environment (IE) consisting of the interdependent networks of information technology infrastructures and

[936] A raíz de la invasión de la península de Crimea, Rusia ha podido llevar a cabo operaciones desinformativas, habrá utilizado proxies para lanzar ciberataques contra infraestructuras críticas ucranianas, ha podido obtener información mediante el ciberespionaje y otras similares sin entrar en una guerra abierta y declarada, moviéndose en la Zona Gris. Todas estas operaciones cibernéticas, prácticamente imposibles de atribuir jurídicamente a Rusia a pesar del convencimiento de su autoría, han sido útiles para articular la disuasión del Kremlin y, dentro de la ambigüedad propia de la Zona Gris, no han sido consideradas como ataques o actos de guerra.

[937] IBIDEM página 7.

"La doctrina de la OTAN entiende el ciberespacio como un dominio operativo y lo considera parte del entorno de la información. Este entorno está "[…] compuesto por la información misma, los individuos, las organizaciones y los sistemas que reciben, procesan y transmiten la información". La información procesada a través de este entorno proporciona la base para los procesos cognitivos que afectan a la toma de decisiones individuales y, posteriormente, al comportamiento. Esos procesos ocurren en tres dimensiones –física, virtual y cognitiva– y el ciberespacio involucra a las tres. En este sentido, el concepto de entorno de información de la OTAN no es tan diferente de la comprensión que tiene Rusia del "espacio de información" y el papel del ciberespacio dentro de él" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers"[938].

La conclusión que se impone es doble: primeramente, la íntima relación que existe entre la información y su uso en el marco de la confrontación violenta y, en segundo lugar, la instrumentalización de la información como arma auspiciada por "las tecnologías que pretenden afianzar el control sobre el mundo" (SANSÓ-RUBERT PASCUAL, 2024, pág. 31).

Asi pues, una vez precisado que el ciberespacio actúa sobre un componente físico y que se integra en el entorno de la información, debemos fijarnos en la *ciberguerra* como actividad que se desarrolla en este dominio, y para la que existen múltiples definiciones que vienen a coincidir en sus elementos esenciales "como es el carácter agresivo y hostil de esta actividad, cuyas acciones se ejecutan a través de ataques informáticos en sus distintas variantes" (MIGUEL-GIL, 2023, pág. 118). Los elementos diferenciales de la definición de *ciberguerra* se refieren a la naturaleza de los actores implicados -estatales y/o no estatales-, el tipo de acciones que conllevan -ofensivas, defensivas, ciberataques, ciberhacktivismo, desinformación, etc.- y los potenciales daños que pueden ocasionar -directos, indirectos, materiales, personales, etc.-. Esta cuestión a su vez determinará si los ciberataques están o no sujetos al Derecho Internacional de la guerra, como habremos de estudiar en el capítulo siguiente.

Queda así señalada la idea de que, en el ciberespacio, evoluciona no sólo el ámbito de las operaciones ofensivas -la *ciberguerra*- sino, también, todo el espectro de acciones de apoyo a las operaciones cinéticas convencionales -*guerra de la información*-. A partir de ella, podemos tratar de analizar si el quinto dominio ha actuado en el conflicto ucraniano, por lo visto hasta el momento, como un instrumento de guerra revolucionario que haya contribuido al esfuerzo bélico de ambas partes, hasta el punto de poder catalogarlo como una RAM o, incluso, como una RM.

En definitiva, el debate radica en la interpretación que se haga del alcance que las operaciones cibernéticas pueden tener de cara a la consecución de los objetivos militares que inclinen la balanza a favor de uno de los contendientes y, con ello, del triunfo final en un conflicto armado. En este sentido, siguiendo a Javier Miguel-Gil, podemos decir que son tres las opciones a considerar sobre la ciberguerra en relación con la guerra convencional: como sustitutiva, como complementaria o como herramienta independiente (MIGUEL-GIL, 2023, págs. 121-124).

La primera de las teorías, la ciberguerra como *sustitutiva* de la guerra convencional, entiende que las operaciones cibernéticas destinadas a destruir las capacidades del enemigo en tiempo de paz pueden ser empleadas como sustitutos de las operaciones

[938] "El ciberespacio es un dominio global dentro del entorno de la información (IE) que consta de redes interdependientes de tecnología de la información y sus datos internos, incluyendo Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados." (Traducción propia).
Air Force Doctrine Publication 3-12. Cyberspace Operations. U.S. Air Force, 1 February 2023. Página 1. Disponible en: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf (01/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

militares convencionales[939], contando a su favor con la dificultad de atribución, la ambigüedad en su valoración y el menor coste de ejecución (MIGUEL-GIL, 2023, pág. 122).

Respecto a la segunda, las operaciones cibernéticas como *complemento* de la guerra convencional, estas se subclasifican en dos tipos de acciones en atención a los objetivos pretendidos: las *ciberoperaciones disruptivas*, con efecto directo tanto sobre las capacidades militares del enemigo, disminuyéndolas[940], como sobre las propias, aumentando su efectividad y eficiencia[941]; y las *ciberoperaciones de información*, orientadas a la influencia en la opinión pública y, por ello, con un efecto indirecto en el campo de batalla[942] (MIGUEL-GIL, 2023, págs. 122-123).

En cuanto a la tercera de las teorías, la ciberguerra como *herramienta independiente*, considera que ésta evoluciona de manera autónoma al resto de operaciones cinéticas convencionales, por dos razones: por la distinta naturaleza de los dominios en que operan -virtual y físico, respectivamente-, y por la dificultad de integrar estas capacidades de manera efectiva y eficiente en las MDO (MIGUEL-GIL, 2023, pág. 124).

Dispuestas estas consideraciones ya podemos analizar las ciberoperaciones y su alcance estratégico en el contexto de la guerra de Ucrania, teniendo en cuenta que, cuando se iniciaron las primeras acciones de guerra, la opinión generalizada era que Rusia emplearía en su táctica ofensiva ciberataques a gran escala (TORRES SORIANO, 2023, pág. 285).

Coincidiendo con esta suposición, previamente a la invasión de Ucrania por las tropas rusas el 24 de febrero de 2022, el Kremlin lanza un ciberataque[943] contra relevantes infraestructuras gubernamentales, entre las que se encuentran las comunicaciones del ejército ucraniano, echando abajo el servicio de soporte satelital de Viasat[944], con el objetivo de apoyar las operaciones aéreas y el avance de las unidades de tierra soviéticas. Sin embargo, en poco tiempo las comunicaciones son restablecidas gracias al plan de contingencia que, desde hacía meses, tenía previsto el gobierno ucraniano y en el que se contaba con la ayuda de empresas civiles y plataformas internacionales, principalmente estadounidenses[945], que pusieron su tecnología, su capacidad y su

[939] Por ejemplo, un ciberataque a través de un malware que se aloje en los sistemas de control de las principales infraestructuras energéticas del Estado objetivo, se haga persistente y, poco a poco, vaya escalando privilegios para, finalmente, tener capacidades de administrador y poder controlar toda esa red de infraestructuras, con las consecuencias derivadas sobre el suministro de energía en el país.

[940] Por ejemplo, interrumpiendo sus comunicaciones de mando y control, alterando el espectro electromagnético de las frecuencias de los sistemas de detección, respuesta y geolocalización, etc.

[941] Por ejemplo, echando abajo el sistema de seguridad y control de una infraestructura crítica del enemigo, cuya posición haya que tomar para reforzar las operaciones de nuestra fuerza aérea.

[942] Por ejemplo, la difusión de narrativas que intoxiquen y confundan a la población del enemigo, atacando a la credibilidad de sus dirigentes y mandatarios.

[943] La encargada de este ciberataque fue la unidad 74455 de la Dirección Principal de Inteligencia Rusa (GRU).

[944] El ataque ruso tuvo como objetivo la empresa norteamericana de satélites Viasat, que daba soporte a la estructura de mando y control del ejército ucraniano.

[945] Microsoft, Cloudfare, Starlink, Google o Amazon Web Services, entre otras.

Ediciones Universidad de Salamanca | CC BY-NC-ND

desempeño de naturaleza eminentemente civil al servicio de Ucrania para, por un lado, apoyar la defensa frente al ataque ruso y, por otro, armar la ofensiva ucraniana.

En este sentido, el informe de Microsoft, de junio de 2022, titulado *Defending Ukraine: Early Lessons from the Cyber War*, señala que la estrategia rusa en el ciberespacio se construye desde, al menos, tres ámbitos de acción distintos y, a veces, coordinados: "los ciberataques con efectos destructivos contra Ucrania, la penetración en las redes y el ciberespionaje fuera de Ucrania, y las operaciones de influencia contra personas en cualquier parte del mundo"[946].

Por su parte, en febrero de 2023, el Grupo de análisis de amenazas de Google, *Mandiant y Trust & Safety* elabora un informe[947] en el que constata que las infraestructuras gubernamentales ucranianas están "bajo un ataque digital casi constante", destacando el papel representado por los grupos respaldados por el Kremlin, llevando a cabo ciberataques catalogados como destructivos contra las infraestructuras militares y civiles ucranianas, de ciberdelincuencia -phishing- contra miembros de la OTAN, y del ámbito informativo -exfiltración de datos- para influenciar a distintos objetivos. En segundo lugar, el informe destaca que Moscú ha aprovechado todo el espectro de las operaciones de información para construir la narrativa de la guerra adaptada a su propia población -mantener el respaldo ruso a la *operación militar especial*-, hacia la ciudadanía ucraniana -socavar el apoyo al gobierno y la estrategia de Zelenski- y hacia el resto del mundo -fracturar el apoyo internacional a Ucrania-. En tercer lugar, el informe resalta el dato de que el conflicto ha originado un posicionamiento por *lealtades políticas y geopolíticas* de los principales grupos de ciberdelincuencia, junto con la especialización en el uso de ransomware y la combinación de técnicas, tácticas y procedimientos (TTP) entre actores.

Estos dos informes vienen a confirmar la forma de operar de Rusia en el ciberespacio, como entorno para la *confrontación informativa*, donde tienen cabida los ciberataques con efectos destructivos, el ciberespionaje y la obtención de información y, desde luego, las operaciones de influencia. En este sentido, autores como Pardo de Santayana llaman la atención sobre el relevante papel desempeñado por las redes sociales en el periodo previo a la invasión rusa de Ucrania como campo de batalla de las narrativas desinformadoras, así como por la IA y sus algoritmos de aprendizaje automático en el curso de la guerra, generando y amplificando desinformación con la que distorsionar la percepción del conflicto por parte de ambos bandos (PARDO DE SANTAYANA, 2024, pág. 11).

[946] Defending Ukraine: Early Lessons from the Cyber War. Microsoft, 22 de junio de 2022. Disponible en: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (01/04/2024).

[947] Fog of war: how the Ukraine conflict transformed the cyber threat landscape. 16 de febrero de 2023. Disponible en: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/ (02/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Sin embargo, las acciones rusas en el quinto dominio que, hasta ahora, han podido constatarse en el conflicto ucraniano[948], son interpretadas de distinta manera por los analistas, posicionándose en alguna de las tres teorías expuestas anteriormente.

Parte de ellos, como Manuel R. Torres Soriano, hablan de "la ciberguerra que no fue" entendiendo que el empleo de capacidades cibernéticas soviéticas como complemento de la acción militar en la guerra de Ucrania responde a:

> "[…] un conjunto escaso de operaciones cibernéticas, poco sofisticadas, pobremente planificadas, mal integradas con actividades en otros dominios, pero, sobre todo, intrascendentes en comparación con el papel que ha ejercido el armamento convencional, incluyendo aquel que, como la artillería, hacía tiempo que venía menospreciándose, por considerarse que había quedado superado por la realidad de la guerra hiper-tecnológica" (TORRES SORIANO, 2023, pág. 289).

Desde este punto de vista, las capacidades cibernéticas de la Federación Rusa para causar daños críticos estaban sobrevaloradas, fueron únicamente relevantes en los primeros meses del conflicto y, en vista del desempeño operacional de las unidades convencionales una vez estabilizado el frente de guerra, cabe pensar que la doctrina soviética aún no tiene capacidad para ejecutar auténticas MDO en las que se integren los ataques cibernéticos y el resto de dominios.

Otra parte de la doctrina, como Josué Expósito Guisado, interpreta el desarrollo de la guerra de Ucrania como una demostración de que las operaciones en el ciberespacio, desde la perspectiva del Kremlin, evolucionan con cierto nivel de autonomía respecto al resto de maniobras cinéticas convencionales, por tres razones. La primera de ellas es que Rusia se ha servido del ciberespacio, principalmente, para recopilar información con la que generar inteligencia sobre sus objetivos[949]. La segunda razón se refiere a la priorización del ámbito cognitivo en el uso del quinto dominio, donde las operaciones se enfocan a la influencia a través de la narrativa, la intimidación de la población ucraniana o el descrédito del Estado adversario[950]. La tercera es la particular visión rusa del ciberespacio como parte del entorno en el que opera la *confrontación informativa*

---

[948] En este sentido, un informe de abril de 2024 de la empresa de ciberseguridad WithSecure (www.withsecure.com) alerta de que el grupo hacktivista ruso Sandworm –o APT44-, vinculado al GRU (servicio de inteligencia militar de las FFAA rusas) estaría utilizando una puerta trasera instalada, probablemente, desde el inicio de la invasión, actuando como una amenaza persistente avanzada para atacar infraestructuras ucranianas. Esta backdoor denominada Kapeka fue utilizada probablemente para el despliegue del ransomware Prestige a finales de 2022, dirigido contra las infraestructuras logísticas y de transporte ucranianas y polacas. Disponible en: https://www.infosecurity-magazine.com/news/russian-sandworm-backdoor-ukraine/ (18/04/2024).

[949] Por ejemplo, para identificar objetivos críticos y afinar datos de geolocalización con los que aumentar la precisión y efectividad de sus ataques con misiles.

[950] En este sentido, Putin justifica la decisión de iniciar la *operación militar especial* rusa para defender al pueblo ucraniano que lleva años sufriendo la persecución y el genocidio por parte del régimen de Zelenski, para lo cual es necesario proceder a la desmilitarización y desnazificación de Ucrania. Este es el discurso que utiliza el Kremlin para lanzar la narrativa justificativa de la invasión, en la que Rusia se ve *obligada* a ir a defender a los rusos que viven en el régimen nazi de Ucrania. Hay amplia cobertura mediática de este discurso inicial. Disponible en: https://www.bbc.com/mundo/noticias-internacional-60524958 https://elpais.com/internacional/2023-06-16/putin-zelenski-cubre-a-los-monstruos-neonazis.html (03/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

con las implicaciones de competencia geopolítica que comporta[951]. Estas tres cuestiones referidas a la generación de inteligencia, el ámbito cognitivo y la visión estratégica del ciberespacio por parte de Rusia, vienen a reafirmar una idea ya avanzada previamente, cual es la de entender las operaciones cibernéticas desde el particular enfoque que del quinto dominio hace cada nación (EXPÓSITO GUISADO, 2024, págs. 192-198).

Hay ejemplos en este sentido, como la actividad desarrollada por el grupo hacktivista[952] *Sandworm*, manejado como frente de ciberataques por el Servicio de Inteligencia Militar de las Fuerzas Armadas rusas (GRU), que ha venido desempeñando un papel fundamental en la guerra de Ucrania a través de la identificación de objetivos estratégicos, el desarrollo de campañas disruptivas y destructivas contra infraestructuras y organizaciones gubernamentales a través de una variada gama de herramientas –explotación de routers, ransomware específico, etc.- y, también, la obtención de información mediante actividades de ciberespionaje para generar la inteligencia que, posteriormente, pueda ser aplicada en el campo de batalla. Pero este mandato de Sandworm es global y su actividad, que comenzó mucho antes de la invasión, no acaba en Ucrania, sino que atiende a objetivos como la OTAN, la Unión Europea, los EE.UU., Corea del Sur o Polonia, entre otros, lo que demuestra que estas ciberoperaciones son de alcance mundial y responden a las necesidades e intereses de Rusia[953].

En relación con esta visión particular y distinta que del ciberespacio puede llegar a hacer cada contendiente, autores como Guillermo Pulido Pulido ponen en valor las operaciones cibernéticas ucranianas en el marco de la guerra multidominio y mosaico[954], considerando que este es el primer conflicto del siglo XXI como tal, por

[951] Esta competencia geopolítica, objetivo principal de la confrontación informativa en el quinto dominio, podría explicar por qué Rusia al inicio del conflicto utilizó los ciberataques contra las infraestructuras ucranianas y que, posteriormente, el uso del ciberespacio por su parte haya evolucionado hacia nuevos objetivos más amplios, de carácter internacional, como por ejemplo la articulación de operaciones de influencia en países que, estratégicamente, interesan a Moscú, como Bosnia, Moldavia o Georgia, en los que la UE tiene puestas grandes expectativas de aproximación, o el Norte de África y el Sahel, donde su presencia es cada vez más relevante y que es fuente de preocupación para la Unión, como flanco sur de sus fronteras, y donde se ha visto relegada por la acción soviética. Amplia referencia en prensa. Disponible en: https://www.elmundo.es/internacional/2024/03/31/66097805fc6c8340408b4570.html https://elpais.com/internacional/2024-04-03/la-otan-alerta-de-los-intentos-de-rusia-de-desestabilizar-bosnia-moldavia-y-georgia-los-eslabones-mas-debiles-de-europa.html (03/04/2024).

[952] El concepto de *hacktivismo* nace de la unión de dos palabras: *hacker* y *activismo*. El INCIBE define a los *hacktivistas* como "activistas que aprovechan sus conocimientos cibernéticos para perseguir una causa, en este caso, de manera delictiva. Impulsados por sus ideales, llevan a cabo acciones como la filtración de datos confidenciales de compañías o Estados, a fin de generar cambios sociales y políticos". Disponible en: https://www.incibe.es/ed2026/talento-hacker/blog/explicacion-de-los-distintos-tipos-de-hackers (15/04/2024).

[953] Puede ampliarse la información sobre el grupo Sandworm como principal unidad de ciberataque rusa en la página web especializada DarkReading. Disponible en: https://www.darkreading.com/ics-ot-security/-sandworm-group-is-russia-s-primary-cyber-attack-unit-in-ukraine (19/04/2024).

[954] La guerra mosaico se basa en operaciones militares articuladas a través de drones en formación de enjambre, que permiten una gran flexibilidad de configuración para poder responder a cada situación de batalla en concreto, y que tienen una alta efectividad de impacto por la interconexión entre las plataformas, que intercambian información entre ellas en tiempo real para alimentar los parámetros de los proyectiles guiados.

Ediciones Universidad de Salamanca | CC BY-NC-ND

cuanto ha puesto de manifiesto los límites de "las viejas plataformas y conceptos operativos desarrollados en las últimas décadas del siglo precedente" (PULIDO PULIDO, 2023, pág. 88).

Para ello se refiere al uso del *dominio ultraterrestre* como habilitador de las capacidades tecnológicas que han permitido al ejército ucraniano llevar a cabo operaciones de reconocimiento y observación del campo de batalla, anticiparse a los movimientos de tropas del Kremlin, aplicar a sus técnicas de combate el uso de cohetes y municiones de artillería de precisión guiados por GPS, la geolocalización precisa de objetivos a gran distancia, o la explotación de enjambres de drones de ataque, por lo que concluye que "el dominio de batalla espacial ha sido el verdadero lugar donde se ha decidido el destino de la guerra de Ucrania" (PULIDO PULIDO, 2023, pág. 89).

En nuestra opinión, en tanto que una cosa es la *guerra cibernética* -operaciones cibernéticas ofensivas y del entorno de información- y otra el *apoyo de la tecnología digital* en las acciones de guerra convencionales, esta es una apreciación excesiva del papel desempeñado por los dominios del ciberespacio y ultraterrestre en el balance actual del conflicto ucraniano. No obstante, sí es cierto que este *empleo combinado* de tecnologías y dominios confirma la importancia de avanzar en la doctrina de las MDO, como base de las operaciones del futuro. Pero consideramos que no se puede decir aún que esto se haya conseguido en el *engagement space* de ninguno de los dos contendientes.

Como conclusiones, para entender el marco de acción del ciberespacio en un conflicto armado convencional, podemos destacar que los conflictos del futuro, dado el nivel de dependencia digital de la sociedad actual, lógicamente van a tener un marcado componente ciberespacial, pero eso no implica que la acción cinética convencional sea desplazada o, incluso, anulada por aquel.

Todo parece indicar que la clave sea la integración de acciones y efectos -físicos, virtuales y cognitivos- en los cinco dominios para alcanzar auténticas y efectivas MDO, lo cual no es ni sencillo ni accesible para cualquier Estado. Además, para conseguirlo, será necesario no solo la innovación y el desarrollo tecnológico, sino su adecuada incorporación a la doctrina militar para que oriente la acción futura de los ejércitos (COLOM PIELLA & VALES CALDERÓN, 2023, págs. 76-80).

También parece lógico considerar, por tanto, que las acciones en el ciberespacio, que tienen un marcado carácter transversal, alcanzan su máxima eficacia en combinación sincrónica con otro tipo de acciones, en otros dominios. Por sí solas, al igual que le ocurre al resto de operaciones militares convencionales, limitan su capacidad ofensiva o defensiva.

Finalmente, volver a insistir en que cada Estado enfoca sus operaciones en el ciberespacio conforme a su estrategia y su forma de entender el conflicto. En el caso de Rusia es el entorno de la *confrontación informativa* el que determina su interpretación del ciberespacio, sus posibilidades, sus objetivos y su forma de explotación, como una parte de la *cultura estratégica* propia de cada nación ligada a su historia, a su percepción

Ediciones Universidad de Salamanca | CC BY-NC-ND

de la amenaza, a sus capacidades presupuestarias y militares, a su gestión de la Zona Gris, al contexto geoestratégico del momento y, desde luego, a la visión que tengan del conflicto sus líderes políticos. Coincidir o no en la interpretación de este enfoque del ciberespacio por parte de los contendientes será, pues, decisivo para hablar de ciberguerra o de guerra convencional. En todo caso, como señala el profesor Colom Piella:

> "[…] sea cual sea el desenlace de esta guerra, ni la Comunidad Internacional regresará al mundo previo a la invasión, ni Rusia recuperará un estatus de gran potencia que hace tiempo que perdió, ni la democracia habrá triunfado sobre las autocracias, ni será un indicativo de la buena salud del orden basado en reglas tan anhelado por los pensadores liberales. Al contrario, su inicio, desenlace y derivaciones globales son signos inequívocos de la crisis del orden internacional de la posguerra fría, la pérdida del poder relativo de Estados Unidos, la consolidación de nuevas potencias regionales y su voluntad de revisar el reparto de poder preexistente" (COLOM PIELLA, 2023, pág. 100).

5.2. El terrorismo

5.2.1. El reto de la conceptualización del terrorismo

Podemos convenir que el terrorismo es un concepto jurídicamente difícil de interpretar porque, desde siempre, ha generado emociones intensas, encontradas, incluso violentas, sobre las que se han forjado opiniones muy distintas. Los terroristas, independientemente de la época, han contado con admiradores, con difusores de su mensaje, con seguidores comprometidos con su *lucha*, que han contribuido a la idealización grotesca y pérfida del terrorismo como representación del compromiso con la libertad y la justicia que, forzada por las crueles circunstancias y la indiferencia de la mayoría, tiene que recurrir a la violencia para defender aquellas. Pero, además, la dificultad de su conceptualización viene determinada por el carácter político y cambiante del fenómeno terrorista en cuanto a sus métodos, sus objetivos y sus vinculaciones sociales, y porque no se trata de una ideología sino de una estrategia violenta que puede ser instrumentalizada por convicciones de cualquier signo político, religioso, social o de otra naturaleza. Por ello, ninguna definición de terrorismo puede abarcar todas las manifestaciones que ha tenido a lo largo de la historia:

> "[…] las guerras campesinas, las disputas laborales y el bandidaje estuvieron acompañados de actos de terror sistemático, y lo mismo puede decirse respecto de las guerras generales, las guerras civiles, las guerras revolucionarias, las guerras de liberación nacional y los movimientos de resistencia contra ocupantes extranjeros. En la mayoría de esos casos, no obstante, el terrorismo no fue sino una más entre las diversas estrategias, y, por lo común, una estrategia de segundo orden" (LAQUEUR, 2003, págs. 33-35).

Pero la dificultad de la tarea no debe implicar el desistimiento de la comunidad internacional en la misión de tratar de acordar una serie de características que, a modo de mínimo común, sirvan para señalar a una determinada acción violenta como terrorista, pues la universalización de la amenaza exige una respuesta consensuada:

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "Precisamente la universalización de la amenaza terrorista contra los Estados de todo el mundo hace de la lucha contra el terrorismo global un reto para la gran política, en la que hay que fraguar nuevas alianzas entre bandos contrarios, mitigar los conflictos regionales y, de este modo, barajar nuevamente las cartas de la política mundial" (BECK, 2003, págs. 20-21).

En esta idea, la Asamblea General de NNUU adopta en enero de 1997 la Resolución 51/210 sobre medidas para eliminar el terrorismo internacional[955] en la que, aunque no se acuerda una definición como tal, sí decide establecer un Comité Especial en la materia, se condena la existencia del terrorismo y se hace una aproximación aludiendo a una serie de actos censurables:

> "Reitera que los actos criminales con fines políticos concebidos o planeados para provocar un estado de terror en la población en general, en un grupo de personas o en personas determinadas son injustificables en todas las circunstancias, cualesquiera sean las consideraciones políticas, filosóficas, ideológicas, raciales, étnicas, religiosas o de cualquier otra índole que se hagan valer para justificarlos"[956].

Preocupados por la persistencia de los actos terroristas y conscientes de la necesidad de liderar desde NNUU los avances en la cooperación entre Estados, organizaciones y organismos internacionales para prevenir, combatir y eliminar el terrorismo, la Asamblea General acuerda en diciembre de 2004 la *Resolución 59/46 sobre medidas para eliminar el terrorismo internacional*[957] en la que reitera la condena a este tipo de acciones criminales e insta al Comité Especial a elaborar "con rapidez un proyecto de convenio general sobre el terrorismo internacional"[958].

Esta encomienda culmina con la *Estrategia Global de las Naciones Unidas contra el Terrorismo de septiembre de 2006*[959], consensuada por todos los Estados miembros, acordando por primera vez un enfoque común para luchar contra el terrorismo a través de cuatro tipos de medidas:

1. Las enfocadas a evitar las condiciones que propician este tipo de acciones en cualquiera de sus formas y manifestaciones.
2. Las de prevención y respuesta.

---

[955] Resolución aprobada por la Asamblea General de Naciones Unidas sobre medidas para eliminar el terrorismo internacional. A/RES/51/210, de 16 de enero de 1997. En esta Resolución se comienza recordando el camino iniciado en diciembre de 1994 con la Declaración sobre medidas para eliminar el terrorismo internacional y su Declaración Complementaria de 1996, que figura como Anexo a la misma. Disponible en: https://www.un.org/depts/dhl/resguide/r51_resolutions_table_es.htm (10/03/2024).

[956] IBIDEM, página 2.

[957] Resolución aprobada por la Asamblea General de Naciones Unidas sobre medidas para eliminar el terrorismo internacional. A/RES/59/46, de 16 de diciembre de 2004. Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2005/3461.pdf (10/03/2024).

[958] IBIDEM, página 5, considerando 18.

[959] Resolución aprobada por la Asamblea General de Naciones Unidas el 8 de septiembre de 2006. Estrategia global de las Naciones Unidas contra el terrorismo. A/RES/60/288, de 20 de septiembre de 2006. Esta Estrategia se examina y evalúa periódicamente, dando lugar a una Resolución de la Asamblea General con las correspondientes conclusiones y consideraciones. Disponible en: https://www.un.org/counterterrorism/es/un-global-counter-terrorism-strategy (10/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

3. Las dedicadas a la mejora de capacidades y el refuerzo del sistema colaborativo a través de NNUU.
4. Y las aseguravitas de los derechos humanos y de la aplicabilidad del ordenamiento internacional a los actos de terrorismo.

Posteriormente, en la Resolución 2178 (2014) del Consejo de Seguridad[960], se insta a los Estados miembros a intensificar la cooperación internacional y a fomentar el intercambio de información sobre cualquier tipo de actividad o movimiento terrorista, incidiendo en cuestiones específicas como el reclutamiento, la financiación, los *foreign terrorist fighter*[961] o el establecimiento de obligaciones de información avanzada de pasajeros a las compañías aéreas, lanzando un llamamiento a los Estados para que sus instrumentos legislativos internos tipifiquen adecuadamente los delitos graves vinculados con conductas terroristas.

Finalmente, tras examinar y evaluar la Estrategia cada dos años notificando en un Informe *ad hoc* sus conclusiones, la Asamblea General mediante Resolución de junio de 2017 constituye la *Oficina de Lucha contra el Terrorismo* (OLCT)[962] para liderar, coordinar y mejorar las capacidades de los Estados miembros en la lucha contra el terrorismo y la prevención de los extremismos violentos. Como vemos, lo que ha hecho NNUU hasta ahora ha sido *tirar por el camino del medio*, aprobando una serie de medidas relativas a los actos de terrorismo sin conseguir llegar a un acuerdo previo entre sus Estados miembros sobre una definición jurídica de terrorismo. Esta falta de acuerdo nace precisamente del *uso político* que se puede hacer del término, puesto que la motivación es la base de la calificación como terrorista a un determinado acto violento, de tal manera que los mismos hechos pueden ser interpretados de diferente manera por distintos Estados.

La OTAN, en su *Concepto Estratégico de Madrid* de junio de 2022, en el considerando número 10 referido al entorno estratégico, se centra en la visión operativa ofreciendo

[960] Resolución 2178 (2014) aprobada por el Consejo de Seguridad en su 7272ª sesión, celebrada el 24 de septiembre de 2014. S/RES/2178 (2014). Disponible en: https://www.un.org/securitycouncil/es/s/res/2178-%282014%29 (10/03/2024).

[961] El termino *combatientes terroristas extranjeros* hace referencia a personas que viajan al extranjero con fines de terrorismo -combate, instrucción, apoyo- y que a su regreso a sus países de origen, mayormente occidentales, representan una amenaza por el proceso de radicalización que han experimentado en su compromiso terrorista.

[962] Resolución aprobada por la Asamblea General de Naciones Unidas el 15 de junio de 2017. Refuerzo de la capacidad del sistema de las Naciones Unidas de ayudar a los Estados miembros en la aplicación de la Estrategia Global de las Naciones Unidas contra el terrorismo. A/RES/71/291, de 19 de junio de 2017.
En junio de 2023 se inauguró en Madrid una nueva Oficina de Programas de la Oficina de Lucha contra el Terrorismo de las Naciones Unidas, para la prestación de asistencia técnica y proyectos de desarrollo de capacidades a los países de todo el mundo, enfocada principalmente en la protección de objetivos sensibles, la prevención de los radicalismos violentos, la protección de los derechos humanos y el apoyo a las víctimas, así como en el impulso de la cooperación bilateral y multilateral en la lucha contra el terrorismo. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2023/060623-onu-inaugura-madrid-oficina-terrorismo.aspx
https://documents.un.org/doc/undoc/gen/n17/172/62/pdf/n1717262.pdf
https://www.un.org/counterterrorism/es/un-global-counter-terrorism-strategy (10/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

una panorámica actualizada de la amenaza terrorista, con especial incidencia en la mejora de sus capacidades a través de la asimilación de la tecnología, indicando que:

> "10. El terrorismo, en todas su formas y manifestaciones, es la amenaza asimétrica más directa a la seguridad de nuestros ciudadanos y a la paz y la prosperidad internacionales. El objetivo de las organizaciones terroristas es atacar o incentivar ataques contra los Aliados. Han ampliado sus redes, mejorado sus capacidades e invertido en nuevas tecnologías para mejorar su alcance y letalidad. Los grupos armados no estatales, entre ellos redes terroristas transnacionales y actores apoyados por Estados, siguen aprovechando los conflictos y la débil gobernanza para reclutar, movilizar y ampliar su implantación"[963].

Por su parte la UE, habiendo adoptado anteriormente medidas específicas para combatir este tipo de acciones que atentan contra los valores universales de la dignidad humana, la libertad, la igualdad y la solidaridad, el respeto de los derechos humanos y las libertades fundamentales, trata de alcanzar un acuerdo con sus socios sobre qué entender por *delitos de terrorismo* en la Decisión Marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo[964]:

> "1. Todos los Estados miembros adoptarán las medidas necesarias para que se consideren delitos de terrorismo los actos intencionados a que se refieren las letras a) a i) tipificados como delitos según los respectivos Derechos nacionales que, por su naturaleza o su contexto, puedan lesionar gravemente a un país o a una organización internacional cuando su autor los cometa con el fin de:
> - intimidar gravemente a una población,
> - obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo,
> - o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional"[965].

También define al *grupo terrorista* y una serie de delitos ligados a estas actividades criminales como la provocación, la captación y el adiestramiento. Finalmente, se alienta a los EEMM a adoptar medidas de competencia para garantizar que, de oficio, puedan emprenderse acciones legales contra los autores y adoptar medidas protectoras para las víctimas. Posteriormente ésta es modificada por la Decisión Marco del Consejo, de 28 de noviembre de 2008[966], que comienza señalando que el terrorismo no solo es una grave amenaza para los derechos de las personas, sino que también representa uno de los ataques más graves contra las democracias y el Estado de Derecho, principios

[963] Nuevo Concepto Estratégico de la OTAN. Ministerio de Defensa, noviembre de 2022. Disponible en: https://publicaciones.defensa.gob.es/nuevo-concepto-estrategico-de-la-otan-libros-pdf.html (10/03/2024).

[964] Decisión Marco del Consejo de 13 de junio de 2002, sobre la lucha contra el terrorismo. 2002/475/JAI. DO L 164 de 22.6.2002, p.3. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002F0475:20081209:ES:PDF (10/03/2024).

[965] IBIDEM, página 4, artículo 1.1.

[966] Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo. DOUE L 330/21, de 9.12.2008. Disponible en: https://www.boe.es/doue/2008/330/L00021-00023.pdf (10/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

comunes a los EEMM y que fundamentan el espíritu de la Unión Europea. En su articulado avanza en la definición armonizada de *delito de terrorismo* y la adapta a la evolución operativa de estas estructuras criminales que recurren, cada vez más, a las nuevas tecnologías y a Internet como medios para alcanzar sus objetivos, incluyendo estas consideraciones en la catalogación de los delitos de provocación a la comisión de un delito de terrorismo, la captación y el adiestramiento de terroristas, así como en los grados de autoría de la complicidad, la inducción y la tentativa.

En 2017 se adopta una nueva Directiva[967] para abordar el problema de los *foreign terrorist fighter* en Europa proponiendo a los EEMM que adopten nuevas medidas como la tipificación penal de delitos relativos a viajar al extranjero con fines terroristas o la facilitación de dichos viajes, el adiestramiento y la captación, incidiendo también en la importancia de la consideración procesal de las vinculaciones cada vez más evidentes entre el terrorismo y el crimen organizado[968], y en la relevancia del control de los *contenidos en línea* para combatir el terrorismo y la amplia variedad de tipos penales vinculados, especialmente la radicalización y la provocación al delito. En esta Directiva se vuelve a definir al *grupo terrorista* y se ofrece una lista exhaustiva de los *delitos de terrorismo* que los EEMM deben tipificar como tales en sus legislaciones nacionales, pero una vez más no se define como tal el terrorismo. Consecuentemente, tampoco la Unión nos ofrece una definición de terrorismo que, de manera unívoca y precisa, comprenda el alcance de esta manifestación de violencia.

Lo mismo ocurre con nuestra Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo, que en su Preámbulo comienza refiriéndose a la Resolución del Consejo de Seguridad de Naciones Unidas 2178 (2014) para referirse a la necesidad de actualizar la norma penal y adaptarla a la nueva amenaza del terrorismo internacional que pone en riesgo a las democracias y al Estado de Derecho. En el artículo 573[969],

[967] Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión Marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo. DOUE L 88/6. 31.3.2017. Disponible en: https://www.boe.es/doue/2017/088/L00006-00021.pdf (10/03/2024).

[968] En concreto se refiere a la financiación de grupos terroristas a través de actividades criminales vinculadas con el comercio ilícito de armas de fuego, de petróleo, estupefacientes, cigarrillos, mercancías, bienes falsificados y bienes culturales, así como la trata de seres humanos, el chantaje y la extorsión.

[969] El artículo 573 del Código Penal estipula que: "1. Se considerarán delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:

1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2.ª Alterar gravemente la paz pública.

3.ª Desestabilizar gravemente el funcionamiento de una organización internacional.

4.ª Provocar un estado de terror en la población o en una parte de ella.

Ediciones Universidad de Salamanca | CC BY-NC-ND

inspirado en la normativa europea sobre lucha contra el terrorismo[970], se recoge una nueva definición de este tipo de delito pero, de nuevo, no encontramos la ansiada definición de terrorismo, sino que encontramos la enumeración de una serie de tipos delictivos heterogéneos vinculados al terrorismo a través de la finalidad con que se perfeccionan. Esa carga política del concepto que abre la puerta a su interpretación jurídica se aprecia en la disquisición entre el Tribunal Supremo, la Audiencia Nacional y la Fiscalía sobre si los disturbios y actos violentos sucedidos en Cataluña entre el 14 de octubre y el 20 de noviembre de 2019, enmarcados en las protestas por la sentencia del juicio a los líderes del proceso independentista catalán[971], pueden considerarse delitos de terrorismo y, como tales, ser enjuiciados por la Sala de lo Penal de la Audiencia Nacional, o deben ser tratados como desórdenes públicos y, en tal caso, juzgarse en los Tribunales de Cataluña[972]. Una vez más, los datos objetivos –las acciones llevadas a cabo en las referidas algaradas y protestas- pueden ser interpretados de distinta manera –terrorismo o desórdenes públicos- atendiendo a la letra de un mismo Código Penal.

Sirva lo anterior para dejar constancia sobre lo apuntado al inicio de este Capítulo en cuanto a la dificultad de convenir una definición jurídica de terrorismo que, desde el punto de vista objetivo, abarque las múltiples formas que puede adoptar como acción criminal y que, además, sea políticamente aceptada por todos los actores internacionales obligados a aplicar la norma que lo combata, cuestión decisiva por cuanto que, históricamente, el terrorismo ha encontrado acomodo en justificaciones políticas de todo tipo que han alimentado su deriva:

> "El carácter político del terrorismo, sus aspiraciones al uso de los conceptos de lucha, liberación o defensa del pueblo se hacen creíbles para los propios terroristas en la medida en que encuentran un apoyo a su discurso en una parte significativa de la sociedad. Porque el terrorista se alimenta de su propio fanatismo, pero también de las repercusiones de sus atentados y de sus justificaciones en la sociedad a la que dice querer liberar" (URIARTE, 2003, pág. 82).

---

2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.
3. Asimismo, tendrán la consideración de delitos de terrorismo el resto de los delitos tipificados en este Capítulo".

[970] En concreto se refiere a la Decisión Marco 2002/475/JAI del Consejo de la Unión Europea, de 13 de junio de 2002, sobre la lucha contra el terrorismo, modificada por la Decisión Marco 2008/919/JAI, de 28 de noviembre de 2008.

[971] Información sobre la repercusión de los disturbios en Barcelona y resto de Cataluña. Disponible en: https://www.elperiodico.com/es/politica/20191017/barcelona-catalunya-sentencia-proces-directo-7680256
https://www.elconfidencial.com/espana/cataluna/2019-10-27/protestas-barcelona-disturbios-26-octubre-cataluna_2301788/ (19/03/2024).

[972] Esta cuestión tiene amplio seguimiento en prensa nacional. Disponible en: https://elpais.com/espana/2024-03-18/la-audiencia-nacional-rechaza-el-recurso-de-la-fiscalia-y-avala-seguir-investigando-por-terrorismo-el-caso-tsunami.html
https://www.rtve.es/noticias/20240318/audiencia-nacional-avala-investigar-terrorismo-tsunami-democratic/16021204.shtml (19/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por ello, habremos de convenir que las *claves interpretativas* del terrorismo son, por un lado, la persistencia de un grupo fanatizado en el uso de la violencia como medio para alcanzar sus objetivos, que forman parte de un proyecto más amplio -político, social, religioso-, junto con la búsqueda del impacto propagandístico para difundir su ideario y, de otro, el condicionamiento social que ello produce a través del terror que, a su vez, resulta en la justificación de esos actos y en el miedo traducido a silencio frente a la barbarie.

Finalmente, debemos referirnos a otro elemento que determina la efectividad del terrorismo: el régimen político del Estado y, conforme a ello, el tipo de respuesta que pueden articular. Las democracias están fundamentadas en el respeto y la garantía de los derechos y libertades que consagran sus constituciones, las cuáles establecen una serie de restricciones a la acción del Estado, como por ejemplo la prevalencia de la verdad y la libertad de opinión y de prensa para defenderla. Por el contrario, los regímenes autárquicos tienen pocas limitaciones a la hora de responder a cualquier tipo de amenaza que entiendan que pueda socavar su principio de autoridad, incluido el control de los medios de comunicación para configurar la narrativa que interese a su propia supervivencia. De esta manera, como señala Dershowitz:

> "El terrorismo es una táctica que tiene más eficacia cuando va dirigida contra las democracias abiertas. Es mucho menos efectiva contra las tiranías cerradas. Una de las razones de esta diferencia es que el terrorismo, en la medida en que es «propaganda por los hechos», depende de que exista una publicidad muy extensa y tal publicidad está fácilmente al alcance en los países que permiten la libertad de prensa" (DERSHOWITZ, 2004, pág. 125).

Concluimos eligiendo la definición de Carlo Mongardini, que caracteriza al terrorismo como un acto de violencia en el marco de una sociedad siempre compleja, con su historia, sus miedos y sus prejuicios que, con todo, debe permanecer alerta para preservar sus principios y no caer en el alegato finalista que justifica cualquier tipo de acción que la mantenga en la complacencia del cortoplacismo:

> "El terrorismo es la manifestación de una violencia convertida en colectiva en una sociedad compleja y profundamente interconectada. Frente a él, la tesis de los fines que justifican los medios nos resulta peligrosamente fascinante, pero conduce al radicalismo y al totalitarismo, tanto más acentuados cuanto más se refleja en esa tesis el economicismo que se ha convertido en una constante de nuestra conducta cotidiana" (MONGARDINI, 2007, pág. 128).

5.2.2. El fenómeno terrorista en Europa

Una vez acordado el marco conceptual del terrorismo podemos continuar señalando que el de carácter europeo y, por ende, el occidental, remite en sus orígenes al período de la Revolución Francesa, donde se consigna como el *régimen del terror* que institucionalizan Robespierre y sus aliados. A partir de ahí, su uso se consolida en la segunda mitad del siglo XIX para definir a los revolucionarios rusos del *Narodnaya Volya*, a los nacionalistas radicales irlandeses, serbios y macedonios, y a los anarquistas

Ediciones Universidad de Salamanca | CC BY-NC-ND

franceses, italianos y españoles cuyos actos al amparo de la *propaganda por el hecho*[973] protagonizan la última década del XIX y la primera del XX, instrumentalizando la violencia rebelde de cualquier tipo como justificación teórica del atentado anarquista como medio para luchar contra la sociedad injusta y, a su vez, como forma de propaganda más eficaz (RIVAS LARA, 2007, págs. 231-233). De esta manera, hasta la Primera Guerra Mundial hubo una tendencia a vincular el terrorismo con la ideología de izquierdas aunque, ciertamente, muchos de estos movimientos no respondían a dicho patrón ideológico. Por el contrario, a partir de 1920 el terrorismo anida en el espectro político de la derecha radical y nacionalista y entre los movimientos fascistas que comienzan a forjarse en ese momento. Posteriormente, en el contexto de la Segunda Gran Guerra, será el terrorismo individual el que desempeñe un papel secundario en el marco del movimiento de resistencia europeo, con acciones violentas que alcanzan relieve con el asesinato de destacados líderes nazis como Heydrich o Wilhelm Kube (LAQUEUR, 2003, págs. 43-51).

El terrorismo urbano de la postguerra comienza a finales de los años sesenta y se instala en distintos países con manifestaciones heterogéneas, como la del terrorismo nacionalista separatista que sufren, entre otros, España con la ETA[974] e Irlanda con el IRA, pero también la del fundamentalismo religioso que confina al islamismo radical en los límites nacionales -Egipto, Argelia, Irán- hasta la fatídica fecha del 11 de septiembre de 2001, cuando adquiere el estatus de amenaza internacional poniendo de relieve cuestiones hasta entonces obviadas como el alto nivel de conexión entre los terroristas y otros enemigos de un determinado país, su capacidad para el fácil acceso a recursos con alta capacidad destructiva, y las tensiones políticas, económicas y sociales de un mundo globalizado que se traducen en flujos y movimientos de masas de una facilidad y dimensión nunca antes conocidos (CALDERÓN FERNÁNDEZ, 2003, pág. 249).

Los atentados terroristas del 11 de septiembre de 2001 vigorizaron el ideario yihadista convirtiéndose en ejemplo a seguir para miles de islamistas radicales en todo el mundo, consolidando la amenaza del terrorismo internacional:

[973] Según Rivas Lara, la *propaganda por el hecho* se define en el congreso revolucionario celebrado entre el 14 y el 19 de julio de 1881 en Londres, al que acuden algunos de los líderes más relevantes del anarquismo internacional. En esta reunión se aprueba la violencia individual como táctica y se vincula a la *propaganda por el hecho* para llamar la atención sobre las desigualdades sociales e injusticias, creando una situación de terror que provoque una espiral de atentados y lleve a la revolución.

[974] En clave nacional, no podemos pasar por alto en este epígrafe que desde la década de los sesenta del siglo XX España se enfrenta al terrorismo autóctono de ETA, de ideología etnicista, antiespañolista e independentista, que inicia su sangrienta historia de atentados el 7 de junio de 1968 con el asesinato del Cabo de la Guardia Civil José Antonio Pardines por parte del terrorista Txabi Etxebarrieta. Desde ese día y hasta el 20 de octubre de 2011, fecha en que la banda anuncia el *cese de su actividad armada*, ETA asesina a 853 personas y deja heridas a otras 2.632, aparte de personas secuestradas, amenazadas, exiliadas o de otra forma victimizadas. Otras cifras hablan de 861 víctimas mortales, como las de la Fundación Víctimas del Terrorismo. Disponible en: https://www.abc.es/espana/abci-historia-cifras-853-asesinatos-3500-atentados-y-mas-7000-victimas-202110200115_noticia.html
https://www.rtve.es/noticias/20211020/cifras-barbarie-eta-mas-850-asesinatos-2600-heridos-casi-90-secuestrados/2195448.shtml
https://fundacionvt.org/fundacion/victimas-mortales-de-eta/ (09/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "Vieron cómo un grupo de hermanos fieles a sus ideales yihadistas, residentes en Europa, con paciencia y decisión, habían sabido proyectar y llevar a cabo, burlando a todos los servicios de seguridad del mundo, unos hechos que para ellos significaron un logro grandioso ya que, además de castigar a su principal enemigo, EE.UU., representaron un ataque directo a la cultura occidental, que colapsó todos los sistemas de seguridad, el comercio, vías de comunicación, etc., causaron la muerte a 2.986 personas de 79 nacionalidades diferentes y heridas a más de 3.000, para ellos *infieles que merecían morir*, y habían conseguido establecer en todo el mundo la otra clase de terrorismo: «el terrorismo psicológico o el miedo a ser atacados»" (RUBIO MUÑOZ, 2006, pág. 318).

Ya desde antes, en la década de los ochenta, comienzan a asentarse en España diferentes comunidades islámicas controladas en su mayoría por la Hermandad Musulmana siria, de carácter salafista, y otras tantas apoyadas por Arabia Saudita, de ideología wahabita, cuyo número de integrantes crece de manera exponencial durante los años noventa con la llegada de ciudadanos musulmanes procedentes de Túnez, Argelia, Libia, Marruecos y Mauritania, principalmente. Este flujo de inmigración da cobertura a la entrada en España de personas ya radicalizadas en origen por el fundamentalismo islámico y permite, también, la creación de una bolsa de perfiles aptos para la captación provenientes del ámbito delincuencial (RUBIO MUÑOZ, 2006, págs. 314-315). En este contexto social y con el aliento que para los seguidores de la yihad suponen los atentados en EE.UU. del 11 de septiembre, un grupo de terroristas islamistas pertenecientes a la organización *Takfir Wal Hijra* llevan a cabo el 11 de marzo de 2004 el terrible atentado de Atocha, en Madrid, en el que fallecieron 193 personas y más de 2.000 resultaron heridas[975].

Desde entonces Europa sufre más de un centenar de atentados perpetrados por grupos islamistas radicales[976] como, entre otros, los del centro de Londres del 7 de julio de 2005[977], el de la sede de la revista Charlie Hebdo en París el 7 de enero de 2015[978], el del 14 de febrero de 2015 en Copenhague en un acto homenaje a Charlie Hebdo y la libertad

[975] Amplio tratamiento de la prensa. Disponible en: https://elpais.com/diario/2004/03/22/espana/1079910017_850215.html https://edition.cnn.com/2004/WORLD/europe/03/11/spain.blasts/index.html https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2024/060324-marlaska-exposicion-11m.aspx (09/03/2024).

[976] El terrorismo en la UE: datos y cifras (2010-2021). Página web del Consejo Europeo/Consejo de la Unión Europea. Disponible en: https://www.consilium.europa.eu/es/infographics/terrorism-eu-facts-figures/ (10/03/2024).

[977] Atentados del 7 de julio de 2005 en la red de transporte público del centro de Londres, con resultado de 56 personas fallecidas y más de 300 heridas. Disponible en: https://web.archive.org/web/20051005095829/http://www.liberation.fr/page.php?Article=309592 https://elpais.com/internacional/2005/07/07/actualidad/1120687212_850215.html (10/03/2024).

[978] Atentado el 7 de enero de 2015 en las oficinas del semanario satírico Charlie Hebdo y otras zonas de París en los dos días siguientes, con resultado de 17 personas fallecidas y más de 20 heridas. Disponible en: https://www.independent.co.uk/news/world/europe/charlie-hebdo-shooting-10-killed-as-shots-fired-at-satirical-magazine-headquarters-according-to-reports-9962337.html (10/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de expresión[979], de nuevo en París el 13 de noviembre de 2015 en la sala Bataclán[980], el doble atentado en el metro y el aeropuerto de Bruselas el 22 marzo 2016[981], el atentado de Niza del 14 de julio de 2016 en la celebración del Día Nacional de Francia[982], el del 22 de mayo de 2017 en Manchester al finalizar un concierto de una famosa cantante[983], el 3 de junio 2017 en el Puente de Londres[984], los atentados de la Rambla de Barcelona y de Cambrils el 17 de agosto de 2017[985], los de Carcasona y Trèbes en el sur de Francia el 23 de marzo de 2018[986], el del mercado navideño de Estrasburgo el 11 de diciembre de

[979] El 14 de febrero de 2015 una persona armada dispara contra los asistentes a un acto en favor de la libertad de expresión y de homenaje al reciente atentado a la revista francesa Charlie Hebdo, apenas cinco semanas antes, y posteriormente en una sinagoga. Fallecieron 3 personas y otras 5 resultaron heridas. Disponible en: https://elpais.com/internacional/2015/02/14/actualidad/1423930814_931343.html https://www.elconfidencial.com/mundo/2015-02-15/un-segundo-tiroteo-en-una-sinagoga-pone-a-copenhague-en-alerta-terrorista-maxima_712337/ (10/03/2024).

[980] Atentados simultáneos el viernes 13 de noviembre de 2015, en la sala Bataclán de París y en el suburbio de Saint-Denis, con resultado de 131 personas fallecidas y 415 heridas. Disponible en: https://www.lemonde.fr/societe/article/2015/11/13/fusillade-meurtriere-a-paris_4809485_3224.html https://www.rtve.es/noticias/atentados-paris/en-vivo/ (10/03/2024).

[981] Doble atentado en Bruselas del 22 de marzo de 2016, en el aeropuerto internacional de Zaventem y en la estación de metro de Maelbeek, con el resultado de 35 personas fallecidas y 340 heridas. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/atentados-terroristas-bruselas-22-marzo-2016 https://www.elmundo.es/internacional/2016/03/22/56f0f2cf22601d20498b4648.html https://www.lavanguardia.com/internacional/20160328/40714242870/cifra-muertos-atentados-bruselas-eleva-35.html (10/03/2024).

[982] Un camión de alto tonelaje arrolla a una multitud de personas que celebran el Día Nacional de Francia, en el Paseo de los Ingleses, de Niza. Posteriormente el conductor del camión se apeó de la cabina y, con un arma, abrió fuego contra los viandantes y la Policía, que terminó abatiéndole. Fallecieron 86 personas y resultaron heridas otras 434. Disponible en: https://www.bbc.com/mundo/noticias-internacional-36800755 https://www.rtve.es/noticias/atentado-niza/ (10/03/2024).

[983] Atentado perpetrado el 22 de mayo de 2017 en el estadio Manchester Arena, al finalizar un concierto, con el resultado de 22 personas fallecidas y 116 heridas. Disponible en: https://www.bbc.com/news/uk-england-manchester-40010124 https://elpais.com/internacional/2017/05/23/actualidad/1495525781_483597.html https://www.bbc.com/news/uk-england-manchester-40008389 (10/03/2024).

[984] Atentado del 3 de junio de 2017 en el puente de Londres y en Borough Market, con el resultado de 8 personas fallecidas y 48 heridas. Disponible en: https://www.telegraph.co.uk/news/2017/06/05/london-bridge-attack-latest-gunshots-heard-police-launch-fresh/ https://elpais.com/internacional/2017/06/06/actualidad/1496744463_102889.html (10/03/2024).

[985] Doble atentado en la Rambla de Barcelona y en Cambrils del 17 de agosto de 2017, con resultado de 16 personas fallecidas y más de 95 heridos. Disponible en: https://www.dsn.gob.es/en/actualidad/sala-prensa/nota-informativa-sobre-atentados-barcelona-cambrils https://www.rtve.es/noticias/20170818/atentado-barcelona-directo/1599220.shtml (10/03/2024).

[986] Atentados en las ciudades francesas de Carcasona y Trèbes del 23 de marzo de 2018, con resultado de 4 personas fallecidas y 15 heridas. Disponible en: https://www.lavanguardia.com/internacional/20180323/441859630190/hombre-armado-retiene-personas-supermercado-sur-francia.html https://www.france24.com/en/20180323-liveblog-shooting-hostage-taking-southwest-france-carcassone-trebes (10/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

2018[987], el de la Prefectura de la Île de la Cité en París del 3 de octubre de 2019[988], o el atentado de la basílica de Notre-Dame de Niza el 29 de octubre de 2020[989]. Sin ánimo de exhaustividad a través de una pormenorizada relación de todos estos atentados sufridos en suelo europeo, que son muchos más de los aquí enunciados, podemos concluir que, a día de hoy, la amenaza yihadista en Europa continúa vigente tal y como atestiguan los ataques terroristas en Renania del Norte-Westfalia (Alemania)[990], donde en abril de 2023 un sirio autocalificado como combatiente de DAESH perpetró un apuñalamiento mortal en un gimnasio de Duisburgo[991], o el apuñalamiento indiscriminado durante la celebración de un festival en Solingen el 23 de agosto de 2024[992].

Esta evolución de la amenaza terrorista en suelo europeo, perfectamente adaptada a un mundo interconectado y globalizado con gran movilidad internacional, exige una respuesta de la Unión sobre la base de dos consideraciones: por un lado, el mantenimiento del orden público, la salvaguarda de la seguridad interior y la protección

[987] Atentado del martes 11 de diciembre de 2018 en Estrasburgo, con resultado de 5 personas fallecidas y 11 heridas. Disponible en: https://www.lefigaro.fr/actualite-france/2018/12/12/01016-20181212ARTFIG00276-cherif-c-un-delinquant-tombe-dans-l-islam-radical.php https://elpais.com/internacional/2018/12/11/actualidad/1544557124_955716.html (10/03/2024).

[988] Atentado en la Prefectura de la Île de la Cité en París del 3 de octubre de 2019, con resultado de 4 personas fallecidas y 2 heridas. Disponible en: https://www.bbc.com/mundo/noticias-internacional-49919687 https://www.lemonde.fr/societe/article/2019/10/04/ce-que-l-on-sait-de-l-attaque-a-la-prefecture-de-police-de-paris_6014194_3224.html (10/03/2024).

[989] Atentado en la basílica católica de Notre-Dame de Niza, el 29 de octubre de 2020, cuando un lobo solitario entró en el edificio y, armado con un cuchillo, mató a 3 personas e hirió a varias otras. Disponible en: https://www.bbc.com/mundo/noticias-internacional-54732252 https://www.elmundo.es/internacional/2020/10/29/5f9a81effc6c83045b8b45be.html https://www.rtve.es/noticias/20201030/atentado-terrorista-niza-se-sabe-del-ataque-dejo-tres-muertos-iglesia/2050900.shtml (10/03/2024).

[990] En este *lander* alemán desde principios de siglo se conjugado el asentamiento de una intrincada red de mezquitas salafistas que favorecen la difusión de mensajes radicales antioccidentales, la llegada de retornados de zonas de conflicto, y el desarrollo de una amplia comunidad de personas nacidas ya en Alemania y radicalizadas por su entorno, lo cual genera como resultado la alta carga islamista de estas acciones terroristas en el centro de Europa.

[991] El martes 18 de abril de 2023 en Duisburgo (Alemania) varias personas fueron apuñaladas en un gimnasio por un agresor armado con un cuchillo. Disponible en: https://es.euronews.com/2023/04/23/alemania-policia-detiene-a-un-sospechoso-por-el-ataque-con-cuchillos-en-un-gimnasio https://www.agenzianova.com/es/news/germania-al-via-il-processo-contro-laggressore-di-duisburg-ritenuto-un-sostenitore-dello-stato-islamico/ https://www.latimes.com/espanol/internacional/articulo/2023-04-18/alemania-4-heridos-al-ser-apunalados-en-gimnasio (25/08/2024).

[992] Atentado en Solingen (Alemania) el 24 de agosto de 2024, donde fallecen 3 personas y otras 8 resultan heridas de gravedad como resultado del ataque de un ciudadano sirio de 26 años armado con un cuchillo, aprovechando la concentración de personas con ocasión de la celebración del Festival de la Diversidad en la ciudad. Disponible en: https://www.rtve.es/noticias/20240823/varios-muertos-heridos-ataque-con-cuchillo-ciudad-alemana-solingen/16226165.shtml https://www.elmundo.es/internacional/2024/08/23/66c8fb70fdddff9e808b4590.html https://www.eldiario.es/internacional/detenido-presunto-autor-ataque-alemania-entregarse-policia_1_11607534.html https://www.rtve.es/noticias/20240825/policia-detiene-presunto-autor-apunalamiento-mato-tres-personas-solingen/16226618.shtml (25/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de la seguridad nacional que, por ahora, siguen constituyendo una responsabilidad exclusiva de cada uno de los EEMM conforme a lo estipulado en los artículos 72 y 73 TFUE. Y por otro, que ese enfoque nacional no es suficiente para alcanzar el objetivo final de conseguir una Europa más segura para todos, que requiere de un compromiso conjunto y complementario basado en la responsabilidad compartida, la confianza mutua y la cooperación policial y judicial efectiva.

Esta es la base de la estrategia que guía la *Agenda Europea de Seguridad* de 2015, donde se marca como prioridad la lucha contra el terrorismo y la prevención de la radicalización -junto con la delincuencia organizada y la ciberdelincuencia-, y la posterior *Estrategia de la UE para una Unión de la Seguridad* (EEUS) de 2020, que definitivamente apuesta por una acción europea multidisciplinar e integrada que sirva de apoyo a las políticas de seguridad de los EEMM que, cada vez más, se muestran insuficientes para proteger a sus nacionales frente al terrorismo, la radicalización y la delincuencia organizada.

Una vez más se presenta complicada la cuestión de alcanzar un enfoque europeo frente a la amenaza común por cuanto las acciones violentas tienen distinto alcance y afectación territorial, lo que hace que cada Estado adopte de manera soberana las medidas de respuesta que estime oportunas. Un claro ejemplo de ello es el paquete de medidas adoptadas por el Gobierno alemán a raíz del ataque terrorista de carácter islamista de Solingen y del auge de la ultraderecha en el país, entre las que destacan el endurecimiento de la ley de armas, la agilización de las deportaciones de criminales y personas peligrosas para la seguridad del Estado, la exclusión de las prestaciones sociales a los asilados que viajen a sus países de origen sin motivo justificado, la potenciación de la lucha contra el islamismo violento y la habilitación de un marco jurídico que permita a la Policía el uso de armas tipo *táser*[993]. Estas medidas implican un viraje en la postura del Gobierno alemán en materia migratoria, con un evidente giro desde postulados *woke* hacia lo que su Ministro de Justicia califica como *realpolitik*.

Este cambio de actitud ahonda en la tendencia que se viene atestiguando en otros países europeos respecto a la toma de conciencia del riesgo asociado a la irrupción de los movimientos islamistas radicales, legitimadores de una violencia estructural que descansa en las tesis de la guerra de religiones y que defiende la incompatibilidad de la identidad musulmana con la convivencia pacífica en un país democrático y europeo.

Por todo ello, en el análisis del fenómeno terrorista nos centraremos en la faceta internacional de dicha amenaza por su mejor adecuación al objeto de nuestro estudio, que no es otro que la exploración de cómo éste evoluciona en el tiempo para,

[993] Amplio seguimiento en la prensa nacional e internacional. Disponible en: https://www.dw.com/es/el-gobierno-alem%C3%A1n-presenta-plan-contra-migraci%C3%B3n-irregular-con-restricciones-a-refugiados/a-70197330
https://www.rtve.es/noticias/20240912/gobierno-aleman-plan-migracion-irregular-restricciones-refugiados/16245903.shtml
https://www.swissinfo.ch/spa/el-gobierno-alem%C3%A1n-presenta-plan-contra-migraci%C3%B3n-irregular-con-restricciones-a-refugiados/87536335
https://es.euronews.com/my-europe/2024/07/23/el-gobierno-aleman-refuerza-el-tribunal-constitucional-contra-la-extrema-derecha (15/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

adaptándose al nuevo ámbito digital, conseguir el mejor aprovechamiento del ciberespacio para sus fines.

5.2.3. El ciberterrorismo: el Estado Islámico y la vertebración de la amenaza a través de la yihad digital

Como se ha señalado anteriormente, los atentados terroristas del 11 de septiembre de 2001 impactaron en los valores de Occidente, mostrando una imagen de debilidad de EE.UU., líder de esa forma de vida, y actuaron como efectiva arenga de llamada al combate para todos los islamistas radicales, que los interpretaron como una evidencia de que la imposición de su ideal al resto del mundo era un objetivo alcanzable. Osama Bin Laden estudió a su enemigo desde dentro, detectó sus debilidades y, adaptándolas a su favor, las utilizó para atacarlo, lanzarle un desafío a largo plazo y justificar la lucha ante sus seguidores. En este sentido, podemos decir que:

> "El principal logro de Al Qaeda fue desafiar a la primera potencia mundial y ser capaz de subsistir; pero, más allá de ello, habría sido el haber sido capaz de popularizar el término "yihadista", que sirve de apellido y mínimo común denominador a distintos movimientos locales, dotándoles de una cierta vertebración y generando sinergias a nivel global" (AZNAR FERNÁNDEZ-MONTESINOS, 2024, pág. 291).

Después, con la caída del régimen de Saddam Hussein en diciembre de 2003 a consecuencia de la *Operación Libertad* de Irak liderada por EE.UU., y el caos posterior por el desmantelamiento de las estructuras administrativas y de seguridad -ejército y policía- iraquíes, Abu Musab Al Zarqaui[994], junto con el grupo terrorista Jamaat al Tawhid wal Yihad que lidera, hace acto de presencia en la insurgencia iraquí asumiendo la definición de sus objetivos operativos que, a partir de entonces, se focalizan en la comisión de atentados en Jordania y los países apóstatas del entorno, la comunidad chií y los países occidentales.

En 2004 Al Qaeda[995], liderada por Osama Bin Laden, busca expandirse en Irak, ocasión que aprovecha Al Zarqaui para jurarle fidelidad y, con ello, incrementar su prestigio, conseguir financiación para su organización terrorista y ampliar la capacidad de reclutamiento, pasando a denominarse Al Qaeda en Irak (AQI)[996]. Esta alianza funciona inicialmente e Irak se convierte a partir de 2005 en uno de los principales focos de la yihad, actuando AQI como polo de atracción para combatientes reclutados en el extranjero, los cuales son empleados para perpetrar atentados extremadamente violentos en el país, especialmente contra la comunidad chií. Estas acciones tan violentas incomodan a la matriz de Al Qaeda que, a través de Ayman Al Zawahiri[997] y de

[994] Abu Musab al Zarqaui fue un terrorista musulmán salafista, de origen jordano, que estableció los orígenes del conocido como *Estado Islámico*.

[995] Al Qaeda es incluida en la Lista de terroristas de NNUU en octubre del año 2001, inmediatamente después de los atentados del 11-S.

[996] Al Qaeda en Irak es incluida en la Lista de terroristas de NNUU el 18 de octubre de 2004.

[997] Ayman Al Zawahiri es en ese momento el lugarteniente de Osama Bin Laden, al que sucede en el liderazgo de la organización terrorista a raíz de su muerte en 2011 en Pakistán, en una operación de los Navy Seal de los EE.UU.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Atiya Abd Al Rahman[998], hacen notar su disconformidad con los métodos de AQI y el enconamiento sangriento mostrado contra la comunidad chií.

En 2006 Al Zarqaui, junto con siete de sus más próximos incondicionales, muere a consecuencia de un ataque aéreo estadounidense en una aldea al noreste de Bagdad. Cinco días después es nombrado líder de AQl el egipcio Abu Hamza Al Muhajir, que mantiene invariable la operatividad y la estrategia de la organización terrorista. En octubre de ese mismo año se anuncia la creación del Estado Islámico de Irak y Levante (EIIL)[999], predecesor de DAESH, a cuyo frente se encuentra Abu Omar Al Bagdadi, al que jura fidelidad Abu Hamza Al Muhajir.

El 29 de junio de 2014 el portavoz del EIIL anuncia la restauración del Califato Islámico[1000], que tendrá a Abu Bakr Al Bagdadi como califa y la zona de al-Sham[1001] como ámbito territorial, así como el cambio de denominación por la de Estado Islámico (DAESH)[1002], desapareciendo la referencia a Irak y Levante para alcanzar un enfoque mundial, por lo que se convierte en un claro competidor de Al Qaeda en el liderazgo de la yihad global. Esta proclamación del Califato Islámico exige obediencia al califa por los musulmanes de todo el mundo y, de hecho, tiene un efecto llamada que potencia la captación de militantes y simpatizantes que pasan a engrosar las filas de DAESH. Con Abu Bakr Al Bagdadi comienza el uso masivo de terroristas suicidas y las ejecuciones sistemáticas de prisioneros[1003] grabadas en directo, entre otros crímenes, como parte de la estrategia propagandística de DAESH.

Entre agosto y septiembre de 2014 el DAESH dirige sus acciones contra el Kurdistán iraquí, tomando las localidades de Sinjar y Erbil y amenazando con el asalto a Bagdad, lo

[998] Atiya Abd Al Rahman era un miembro del Grupo Islámico Combatiente Libio, que posteriormente llegó a ser considerado número dos de Al Qaeda bajo el mando de Ayman Al Zawahiri.

[999] El Estado Islámico de Irak y Levante (EIIL) pretendía constituir un Estado Islámico *de facto* circunscrito al territorio de Irak y Siria -País del Sham, Gran Siria o Levante-, lo cual incomoda a Al Qaeda por dos razones: la primera que no fue consultada para llevar a cabo este movimiento y, la segunda, porque entendían que las implicaciones de proclamar un Estado Islámico obligaba a estar en condiciones de garantizar una estructura de Estado, so pena de perder el apoyo de la población local, y Al Qaeda consideraba que no estaban en disposición de hacerlo. Y esta es la gran diferencia entre ambas organizaciones terroristas, ya que mientras Al Qaeda entiende la yihad global como una lucha contra el infiel en cada Estado, y a partir de ahí la creación final de una *umma* o comunidad islámica universal, por su parte DAESH proclama la creación de un auténtico Estado Islámico independiente desde el primer momento, con las características propias como tal -territorio, población y organización administrativa-. Por ello, la emigración al Califato Islámico (la *hégira*) se convierte en una obligación para todo musulmán y, solo el que no pueda migrar, deberá luchar en su país de origen. El Estado Islámico facilita a todos los musulmanes una infraestructura de vida propia de un Estado: alojamiento, sustento, enseñanza, sanidad, etc.

[1000] El Califato Islámico representa el estado islámico ideal con la *Sharía* o ley islámica como única forma legítima de gobierno y de ordenamiento jurídico, de carácter universal para todos los musulmanes. La *Sharía* es, por definición, contraria a los principios y valores democráticos.

[1001] País del Sham -Gran Siria o Levante- es un área que comprende Siria, Irak y algunas partes del territorio de Jordania, Líbano y Turquía.

[1002] Estado Islámico, ISIS en inglés o DAESH en árabe.

[1003] Estos vídeos de asesinatos tenían una producción profesional y una escenografía visual muy estudiada, mostrando a los prisioneros enfundamos en monos de color naranja a imitación de los uniformes de los presos de la cárcel estadounidense de Guantánamo.

Ediciones Universidad de Salamanca | CC BY-NC-ND

que precipita la intervención de la Coalición Internacional[1004] liderada por EE.UU. que se concreta en bombardeos selectivos sobre las posiciones de DAESH, con el objetivo de facilitar el avance del ejército iraquí y las milicias kurdas para recuperar territorios ocupados y consolidar estructuras que impidan que vuelvan a caer bajo el control de los terroristas. La ofensiva de la Coalición Internacional hace que el DAESH cambie su operativa de combate, pasando del enfrentamiento abierto a la guerra de insurgencia y a la utilización de la población civil como escudo, camuflando sus efectivos y armamento en las poblaciones ocupadas. Al mismo tiempo, a finales de septiembre de 2014, DAESH emite un nuevo comunicado a través de su portavoz, Abu Muhammad Al Adnani, en el que lanza una amenaza genérica contra occidente y, de forma más explícita, contra EE.UU. y Europa, incitando a cualquier yihadista de cualquier parte del mundo a llevar a cabo cualquier tipo de atentado que esté a su alcance contra objetivos militares, policiales, servicios de inteligencia y sus agentes, sin necesidad de consulta o autorización previa, lo que incentiva la actuación de los terroristas autónomos. En enero de 2015 el califato controla cerca de 90.000 kilómetros cuadrados desde el oeste de Siria hasta el este de Irak e ingresa millones de dólares diariamente gracias a la venta en el mercado negro del petróleo de los pozos que se encuentran en su territorio, y al fruto de la actividad delictiva de sus fieles seguidores -robo, extorsión, secuestro, tráfico de personas-.

Dicho llamamiento es desde entonces insistentemente reiterado en la propaganda proselitista de DAESH y se traduce en acciones terroristas localizadas principalmente en EE.UU. y Europa, con un recrudecimiento entre 2015 y 2019. El 23 de marzo de 2019 las Fuerzas Democráticas de Siria (FDS)[1005] anuncian la toma de Baguz, último enclave territorial controlado por DAESH ubicado en la frontera este de Siria con Irak, y el fin del califato y la derrota de la organización terrorista tras más de cinco años de combates[1006].

Ciertamente este significativo hito no supone el fin de DAESH, aunque la pérdida del control del territorio supone un duro golpe para la organización terrorista por cuanto pierde el escaparate fáctico y sustento físico de su califato. A ello se suma la falta de un liderazgo carismático y la nula presencia mediática de sus últimos máximos dirigentes, abatidos entre 2022 y 2023[1007]. No obstante, la amenaza de DAESH sigue existiendo

[1004] La Coalición Internacional contra DAESH se crea en la cumbre de la OTAN de Gales, celebrada entre los días 4 y 5 de septiembre de 2014, que obtiene el respaldo de las NNUU y se conforma por más de 60 países, entre los que se encuentra España desde octubre de 2014, fecha en que el Congreso de los Diputados lo autoriza. Sus objetivos son derrotar a la organización terrorista, la prevención de la radicalización y el reclutamiento, y la estabilización de los territorios liberados de la acción de DAESH, tratando de impedir que vuelva a recuperarlos reconstruyéndolos mediante la creación de suministros de servicios para la población y la consolidación de estructuras de gobierno y seguridad locales.
Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/lucha-contra-DAESH-un-compromiso-reforzado (15/09/2024)

[1005] Milicias kurdo-árabes aliadas de la Coalición Internacional contra DAESH, fuertemente apoyadas por EE.UU.

[1006] Seguimiento en la prensa nacional e internacional. Disponible en: https://elpais.com/internacional/2019/03/23/actualidad/1553329466_793785.html https://www.france24.com/es/20190211-siria-fds-estado-islamico-trump (17/03/2024).

[1007] El 30 de noviembre de 2022 DAESH difundió sorpresivamente a través de su productora oficial *Al Furqan* un comunicado en el que informaba de la muerte de su líder y califa, Abu al Hassan al Hashimi al Qurashi, nombrando a su sucesor Abu al Hussein al Husseini al Qurashi, si bien Turquía anunció su muerte

Ediciones Universidad de Salamanca | CC BY-NC-ND

gracias a su maquinaria propagandística[1008], su capacidad para financiarse y la atracción que ejerce sobre otros grupos yihadistas desplegados en distintos escenarios de conflicto que juran su lealtad y se erigen en filiales del Califato Islámico, conformando una amenaza de carácter global, no circunscrita a Siria o Irak.

En este sentido, durante el año 2022 las acciones de los grupos terroristas filiales de DAESH en la zona del Sahel han supuesto más de la mitad de los atentados de la organización. Esta zona concentra el 35% de los muertos por acciones terroristas de todo el planeta y, en el año 2021, incrementa en un 70% los actos de violencia yihadista sufridos (SÁNCHEZ HERRÁEZ, 2022, págs. 87-88), lo que viene a confirmar la estrategia del Estado Islámico de potenciar las acciones en el continente africano para utilizarlo como escenario de conflicto y base territorial sobre la que actuar para proyectar una imagen de fuerza, ampliar su capacidad de financiación -más recursos y materias primas, más población, más impuestos-, reafirmar su rol protector de los musulmanes oprimidos y consolidar el Califato Islámico:

> "El avance yihadista hacia el golfo de Guinea desde el Sahel occidental lleva produciéndose desde hace varios años, pero hoy tiene lugar en un contexto de degradación de la seguridad en la región a causa de la retirada de las tropas occidentales, la aparición del grupo Wagner y la expansión del crimen organizado. Los terroristas buscan con la conquista territorial establecerse en zonas de refugio, aumentar su financiación, incrementar su capacidad operativa y engrosar sus filas. Mientras tanto, los países del golfo de Guinea presentan debilidades estructurales que pueden hacerlos sucumbir a la amenaza yihadista" (CABREJAS MARTÍNEZ, 2023, pág. 1).

Esta expansión del yihadismo por África es cuestión que preocupa a Europa y sus EEMM por las muchas dimensiones del problema y por su proximidad geográfica, que puede facilitar el desplazamiento de terroristas utilizando las vías empleadas por las estructuras de crimen organizado para gestionar la inmigración ilegal. De hecho, en marzo de 2024, la junta golpista de Níger suspende el acuerdo militar con EE.UU. que permite la presencia en el país de un millar de soldados norteamericanos con el objetivo de luchar contra el terrorismo yihadista[1009].

---

el 30 de abril de 2023. Su muerte fue confirmada en un comunicado del portavoz oficial de DAESH el 3 de agosto de 2023.

[1008] En esta estrategia juegan un papel muy importante tanto su productora oficial *Al Furqan* como su revista *al Naba*.

[1009] La junta militar que gobierna Níger bajo el mando del general Abdourahamane Tchiani escenifica la ruptura con el mando militar estadounidense poco después de haber llegado a un acuerdo trilateral con Burkina Faso y Mali para conformar una fuerza conjunta con la que, en teoría, abordar los problemas de seguridad en la zona del Sahel sin contar con la tutela occidental, buscando con ello una aproximación estratégica a su nueva aliada Rusia, que opera en la zona a través de la fuerza mercenaria de Wagner. Disponible en: https://elpais.com/internacional/2024-03-22/niger-quiere-expulsar-al-ejercito-de-estados-unidos.html https://www.france24.com/es/%C3%A1frica/20240317-n%C3%ADger-la-junta-golpista-revoca-un-acuerdo-militar-con-ee-uu-y-pide-la-salida-de-las-tropas (25/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

No obstante, el grupo yihadista predominante en la región del Sahel en la actualidad es *Jama`at Nusrat al Islam wal Muslimeen* (JNIM)[1010], coalición en la órbita de Al Qaeda que detenta el control sobre el centro y el sur de Mali y que avanza con fuerza hacia el norte del Golfo de Guinea, con acciones terroristas simultáneas como las perpetradas el 17 de septiembre de 2024 en la capital, Bamako, contra la Escuela de la Gendarmería y la Base Aérea militar 101[1011], que vienen a confirmar la fortaleza y la capacidad de acción del JNIM, que no encuentra oposición de poder institucional alguno -ni siquiera con el apoyo ruso- que pueda contener su avance en la zona.

Por esta razón, las políticas de fomento del desarrollo económico, la cohesión social, el aseguramiento de la convivencia pacífica en las zonas de conflicto y la cooperación institucional son tan importantes y forman parte de la Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea y de la Estrategia de Seguridad Nacional española, entre otras.

En cuanto al área del Levante, Irak y Siria han experimentado una disminución de la actividad de DAESH, en gran parte debido a la presión contraterrorista internacional y local. A pesar de ello, la tasa de atentados en la zona supone la segunda en el cómputo global de la organización, lo que evidencia que mantiene su capacidad operativa. Por su parte, la Wilayat Khorasan[1012] o ISKP, filial afgana del DAESH, ha basado su estrategia en alimentar el enfrentamiento entre etnias en el país para desestabilizarlo mientras se alimenta de milicianos de países fronterizos como Tayikistán, con los que mantener su fuerza criminal operativa. Afganistán se presenta como una oportunidad para expandir la yihad por el entorno próximo e, incluso, con proyección a Occidente, a través de la propaganda política y religiosa, que además le consolida en la zona[1013]. Como prueba de esta capacidad, el 4 de enero de 2024 el ISKP reivindicó el atentado perpetrado en Irán durante los actos conmemorativos del fallecimiento del general iraní Qasem Soleimanini, en el que más de 300 personas resultaron muertas o heridas[1014] y, dos meses después, reivindica también el atentado perpetrado el viernes 22 de marzo contra los asistentes a un concierto en la sala Crocus City Hall de Krasnogorsk, a las afueras de Moscú, donde mueren 139 personas y otras casi 200 resultan heridas[1015].

[1010] Se puede traducir como Grupo de Apoyo al Islam y los Musulmanes.

[1011] Seguimiento en prensa de estos ataques. Disponible en: https://www.europapress.es/internacional/noticia-registradas-varias-explosiones-tiroteos-capital-mali-bamako-20240917103819.html
https://www.larazon.es/internacional/13-terroristas-suicidas-perpetraron-ataque-instalaciones-militares-capital-mali_2024092166eec8cbfcf7b300013c44fd.html
https://elpais.com/internacional/2024-09-21/un-ataque-terrorista-contra-unas-instalaciones-militares-en-bamako-causa-mas-de-50-muertos.html (22/09/2024).

[1012] Se puede traducir como Estado Islámico Provincia de Jorasán.

[1013] La propia ENCOT 2023, en el apartado referido al marco geoestratégico del Capítulo 2 (páginas 26 a 28), hace referencia a esta compleja situación en Afganistán tras la salida de las tropas estadounidenses en 2021, que facilitó el retorno al poder del movimiento talibán y el posterior asentamiento de células de DAESH.

[1014] Puede consultarse en prensa la repercusión del atentado reivindicado por DAESH. Disponible en: https://www.elconfidencial.com/mundo/2024-01-05/iskp-atentado-iran_3805653/ (23/03/2024)

[1015] Varios asaltantes con armas largas abren fuego contra los asistentes a un concierto en la sala Crocus City Hall, en Krasnogorsk, y posteriormente provocan un incendio en las instalaciones del Centro

Ediciones Universidad de Salamanca | CC BY-NC-ND

La última evolución de la estrategia de lucha yihadista se viene observando desde comienzos del 2024 en Francia, en lo que se podría considerar una *guerra judicial* contra todo aquel que se manifieste crítico con el islamismo rigorista. Esta *yihad judicial*, apoyada por sectores inspirados en los Hermanos Musulmanes y colectivos de extrema izquierda, conlleva la inmediata demanda en tribunales de cualquier manifestación, escrito o actividad crítica y, aunque la mayoría de las causas han sido archivadas, se consigue el desgaste reputacional y económico del denunciado, además de mantener activa en la sociedad francesa la narrativa del discurso victimista de estos grupos. Dicha estrategia es coincidente en objetivos y, como tal, complementaria de la yihad violenta de DAESH, que recientemente[1016] ha realizado un llamamiento expreso a atacar por cualquier medio a los denominados *dignatarios*, en los que incluye a líderes políticos y asesores, economistas, escritores, comunicadores y periodistas, pensadores o jueces, entre otros.

Por todo lo anterior, sería un error considerar extinguido al DAESH que, al contrario, mantiene sus objetivos vinculados a la yihad violenta y la capacidad para operar en distintos escenarios, entre los que destaca África como apuesta de futuro para tratar de reconstruir su infraestructura de soporte territorial para el califato, así como su habilidad para revertir situaciones de gran dificultad, de la que ha hecho gala en anteriores ocasiones.

En línea con dicha conclusión que reafirma la operatividad actual del DAESH, debemos referirnos como clave de ésta a la capacidad para integrar la innovación en sus procedimientos. Es aquí donde entra en juego la nueva dimensión de la amenaza terrorista: el ciberespacio.

En este sentido hay que señalar que fue Al Qaeda la pionera en el aprovechamiento del potencial de Internet para la difusión de su ideología y la expansión de su mensaje de terror a partir de la experiencia de los atentados del 11 de septiembre de 2001 en Nueva York, que supusieron un antes y un después no sólo por los daños causados en términos de víctimas y coste económico, sino también por la repercusión mediática que obtuvo. Nunca antes un atentado terrorista había sido retransmitido en directo en todo el mundo.

Su líder en Irak, Abu Musab al Zarqawi, vio la oportunidad y, conocedor de que la violencia por sí sola constituye un reclamo de fácil propagación, quiso aprovecharla editando de manera periódica revistas que divulgaban su ideología y difundiendo en Internet vídeos sobre atentados de Al Qaeda o sobre la vida de sus terroristas suicidas. Ya desde ese momento los yihadistas supieron ver la *complementariedad* de la acción

Comercial aledaño. DAESH reivindica el atentado en su canal de Telegram. Disponible en: https://www.elmundo.es/internacional/2024/03/22/65fdc357e85ece011a8b458a.html https://www.france24.com/es/europa/20240323-atentado-en-mosc%C3%BA-por-qu%C3%A9-el-estado-isl%C3%A1mico-ataca-rusia https://www.bbc.com/mundo/articles/c51wqnlg519o (23/03/2024)

[1016] En la editorial del número 432 de la revista *al Naba*, de principios de marzo de 2024, titulada "Matar a los dignatarios por cualquier medio".

Ediciones Universidad de Salamanca | CC BY-NC-ND

operativa terrorista y la de difusión propagandística de su mensaje que, a través de Internet, tendría un alcance global.

Pero es el DAESH el que, desde sus orígenes en 2004, fecha que coincide con la creación de Facebook, integra definitivamente el uso de las principales redes sociales[1017] en su estrategia comunicativa y propagandística del Califato Islámico, que se diversifica en el uso de idiomas conforme al público objetivo[1018]. De igual manera, comienzan a profesionalizar la producción y edición de los vídeos que elaboran, conscientes de que el público objetivo, con un perfil cada vez más de *nativo digital*, demanda imagen de calidad cinematográfica y una estética próxima a la de los *game shooter* -Call of Duty, Infinity Ops, Counter-Strike, Shadow Warrior-, propios de la cultura occidental. En este sentido, DAESH perfecciona y actualiza el uso de la propaganda que inició Al Qaeda:

> "Al-Qaeda's releases always exalted its leaders, particularly Osama bin Laden. But the Islamic State's propaganda is generally focused on its fighters and followers. Appearances by leader Abu Bakr al-Baghdadi or his senior lieutenants have been rare. Rejecting the lecture format employed by al-Qaeda, the Islamic State's videos are cinematic, emphasizing dramatic scenes, stylized transitions and special effects"[1019] (MILLER & MEKKENNET, 2015).

DAESH entiende que Internet ofrece dos caras. La primera de ellas, de un perfil más pasivo, que comprende su *utilización como fuente abierta*, directa, sin censuras para transmitir y obtener información, que emplean para la difusión de su propaganda. Este uso de la Red para sus campañas mediáticas presenta un elevado índice de efectividad en la movilización de seguidores:

> "The Islamic State's relentless media campaign has fueled a global migration of militants. More than 30,000 foreign fighters from more than 115 countries have flooded into Syria since the start of that country's civil war. At least a third arrived within the past year, the vast majority of them to join the Islamic State, according to U.S. intelligence estimates.
> Of the defectors interviewed by The Post, all but one said their decisions to leave for Syria could be traced to videos they saw online, or encounters on social media, that ignited a jihadist impulse. The only outlier said that he had been prodded by

[1017] Las principales redes sociales nacen en ese periodo: Facebook en 2004, YouTube en 2005, Twitter en 2006, WhatsApp en 2009, Instagram en 2010 y Telegram en 2013.

[1018] Así, por ejemplo, el árabe se utiliza para comunicarse y arengar a sus seguidores y miembros musulmanes en Oriente, el inglés es el idioma con el que se alcanza la difusión internacional para la propaganda occidentalizada, y otros idiomas como el español o el francés se usa para, específicamente, lanzar mensajes dirigidos a esos países concretos -con referencias a su historia o a hechos particulares, como el caso de Al Andalus-.

[1019] "Las liberaciones de Al Qaeda siempre exaltaron a sus líderes, en particular a Osama bin Laden. Pero la propaganda del Estado Islámico se centra generalmente en sus combatientes y seguidores. Las apariciones del líder Abu Bakr al-Baghdadi o de sus lugartenientes de alto rango han sido raras. Rechazando el formato de conferencia empleado por Al Qaeda, los videos del Estado Islámico son cinematográficos, enfatizando escenas dramáticas, transiciones estilizadas y efectos especiales" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> a friend to come to Syria and was promptly imprisoned for refusing to fight"[1020] (MILLER & MEKKENNET, 2015).

La segunda cara de Internet, de marcado carácter dinámico, es la *capacidad de interactuar* que ofrece a través de las aplicaciones de mensajería instantánea y las redes sociales, que DAESH va a integrar en sus procedimientos de captación y radicalización:

> "Las redes sociales se han convertido en una poderosa herramienta para los grupos extremistas, no sólo como amplificadores de sus campañas de propaganda, sino también como medios desde los que realizan labores de reclutamiento, incitación y radicalización de nuevos terroristas. La promesa de que la participación en la yihad electrónica es tan válida como la lucha sobre el campo de batalla, ha convertido las plataformas en un terreno abonado al que es muy difícil poner coto" (LEJARZA ILLARO, 2015, pág. 1).

Estas dos caras de la Red representan la propia evolución de la civilización en la Era Digital, y el terrorismo yihadista, que se nutre de esa misma sociedad, trata de amplificar el eco de su discurso proselitista aprovechando las múltiples ventajas que aquellas le ofrecen: fácil accesibilidad a contenidos actualizados y en tiempo real, ingentes audiencias potenciales, anonimato, reducidos costes y la posibilidad de segmentar el discurso conforme a la audiencia a la que se dirige. De esta manera el yihadismo internacionaliza su ideología y su narrativa para la difusión de su mensaje, que se mantiene único: el Califato Islámico.

Queda así demostrado que el DAESH ha creado una potente infraestructura comunicativa centralizada, altamente controlada, profesionalizada y perfectamente planificada[1021] basada en su capacidad para adaptarse al ciberespacio de modo permanente y dinámico, abriendo un nuevo frente de batalla virtual que no solo complementa al militar sino que, además, es tan peligroso como éste:

> "De este modo, todo lo enunciado hasta ahora permite concluir y reafirmar la existencia de una estrategia comunicativa altamente planificada y que es una de las claves del éxito de estos grupos, cuyo peso es equiparable al de sus actos sociales y militares. Este triunfo se debe a una diferenciación de los mensajes, a

[1020] "La implacable campaña mediática del Estado Islámico ha impulsado una migración global de militantes. Más de 30.000 combatientes extranjeros de más de 115 países han inundado Siria desde el inicio de la guerra civil de ese país. Al menos un tercio llegó el año pasado, la gran mayoría de ellos para unirse al Estado Islámico, según estimaciones de la inteligencia estadounidense. De los desertores entrevistados por The Post, todos menos uno dijeron que sus decisiones de partir hacia Siria podrían atribuirse a videos que vieron en línea o encuentros en las redes sociales que encendieron un impulso yihadista. El único caso atípico dijo que un amigo lo había incitado a venir a Siria y que rápidamente lo encarcelaron por negarse a luchar" (Traducción propia).

[1021] Para ello DAESH dispone de su editorial propia -Al Himma-, una productora de contenidos multimedia -Al Hayat-, una agencia de noticias -AMAQ-, una plataforma propagandística -Global Islamic Media Front-, una revista electrónica en inglés -Dabiq-, una publicación de carácter semanal para la difusión de las noticias actualizadas del Califato Islámico -Al Nabaa-, entre otras.
En este sentido, es AMAQ la que difunde las imágenes de los cuatro supuestos autores del atentado de la sala de conciertos Crocus City Hall de Krasnogorsk. Disponible en: https://www.20minutos.es/noticia/5230157/0/estado-islamico-difunde-video-masacre-moscu-grabado-por-terroristas/ (26/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> la selección de públicos y a una paradójica relación que han conseguido generar entre un mensaje poco renovado unido al uso de las últimas tecnologías" (TAPIA ROJO, 2016, pág. 14).

En cuanto a los objetivos de este *pilar virtual* de la estrategia terrorista de DAESH, podemos decir que son múltiples y variados, así como que complementan a la yihad que lucha en el mundo físico: la propaganda y amplificación de sus acciones violentas, la justificación de éstas en base a su particular interpretación del Corán o la narrativa de la victimización musulmana bajo el yugo represor al que les somete Occidente, infundir el terror en los países infieles atemorizando a su población, la movilización y el reclutamiento de nuevos muyahidines[1022] idealizando su forma de vida en torno a una visión romántica y aventurera del frente bélico y del compañerismo de los combatientes, la difusión de mensajes de cohesión y motivación, fomentar la emigración hacia el Califato Islámico con sus familias para establecerse allí y procrear para traer al mundo nuevos muyahidines, conseguir financiación y donaciones, el adiestramiento y la radicalización de sus adeptos, la coordinación y planificación de acciones terroristas -*networking*-, compartir conocimiento técnico o táctico a través de manuales o mediante la puesta en común de las experiencias de sus seguidores[1023] o, simplemente, desinformar a los posibles agentes infiltrados que patrullan en los foros que utilizan para comunicarse (CARLINI, 2015, págs. 4-5).

Para asegurar la efectividad de este frente de batalla virtual el propio DAESH sustenta ante sus seguidores la doctrina de que la yihad tiene una naturaleza poliédrica y, al tiempo que se muestra única en sus objetivos, ofrece al musulmán comprometido diferentes caminos para conseguirlos, todos ellos complementarios e igualmente efectivos. De esta manera DAESH consolida el *activismo digital* y lo pone al mismo nivel que el *operativo*:

> […] "Internet también puede ser contemplado como un ámbito de actuación sustitutivo, donde los radicales despliegan un activismo que les permite alimentar su identidad como musulmanes comprometidos. Se trata por tanto, de una elección secundaria ante la imposibilidad de participar en otras actividades más «atractivas», las cuales les están vetadas por dificultades logísticas, limitaciones personales o la ausencia de los contactos adecuados" (TORRES SORIANO, 2017, págs. 2-3)

Es así como se otorga carta de naturaleza al muyahidín que hace la yihad desde el ciberespacio, sin participar en acciones violentas, sino con labores tan importantes para el Califato Islámico como la potenciación del alcance propagandístico de las acciones terroristas, la identificación en los foros de los candidatos más idóneos para captarlos y, posteriormente, radicalizarlos en chats privados[1024] en donde se les somete a un

[1022] El muyahidín es el que lucha por la yihad, el combatiente militar islamista.

[1023] Los terroristas pueden aprovechar estos foros o chats privados para, por ejemplo, compartir conocimiento sobre la manera de confeccionar un artefacto explosivo con productos caseros, o cómo planificar un ataque armado con un simple cuchillo usando métodos de guerra de guerrillas.

[1024] La primera fase de difusión del mensaje yihadista se hace en la Red abierta, el Internet accesible para cualquier persona a través de los buscadores normales -World Wide Web-. En este entorno el mensaje radical llega a mucho público, parte del cual es identificado como candidato idóneo por los *ojeadores*

Ediciones Universidad de Salamanca | CC BY-NC-ND

adoctrinamiento personalizado que intensifica el mensaje de la yihad y donde se comparte material sensible, o la captación de fondos para financiar los gastos de la yihad.

Podemos concluir que el ciberespacio abre una nueva dimensión al enfrentamiento contraterrorista, donde la dependencia tecnológica y la hiperconectividad propia de la sociedad digital del siglo XXI se convierten en vías de agua que organizaciones como DAESH pueden aprovechar para alcanzar sus objetivos terroristas. Al fin y al cabo, la guerra contra el terrorismo yihadista es una "guerra total, que no se combate solo en el campo de batalla o a través de los servicios de espionaje sino en la arena digital también" (CARLINI, 2015, pág. 12).

5.3. Las operaciones en el ciberespacio

Una vez realizado el primer acercamiento a las operaciones en el ciberespacio al tratar la guerra de Ucrania, conviene a nuestro estudio acordar una aproximación doctrinal que nos permita un análisis más enfocado a su particular consideración en el marco del Derecho Internacional, comenzando por valorar si éste le resulta o no aplicable por cuanto que, lógicamente, su cuerpo normativo no contempla reglas específicamente orientadas a regular las actividades que pueden desarrollarse en el quinto dominio, y las existentes fueron redactadas en un tiempo que no corresponde con la evolución tecnológica actual.

5.3.1. El ciberespacio como nuevo escenario de confrontación y la cuestión de la aplicabilidad del Derecho Internacional

Antes de comenzar nos permitimos recordar la visión que la OTAN maneja del ciberespacio[1025] y sus puntos de conexión y divergencia con la interpretación que la Federación de Rusia hace del mismo, como entorno en el que opera la *confrontación informativa*, en la que confluyen los intereses estratégicos nacionales a defender y el ámbito cognitivo. Como ya dijimos, lo que cada Estado pueda entender como ámbito de afectación del quinto dominio va a determinar su forma de relacionarse con el resto de actores internacionales y, al mismo tiempo, la interpretación que haga de determinadas obligaciones que, como Estado, le vinculan.

Por su parte, el Servicio Europeo de Acción Exterior (EEAS) elabora en 2021 el documento *Visión y estrategia militar de la Unión Europea sobre el ciberespacio como*

terroristas en base a las opiniones que manifiestan sobre los temas que, premeditadamente, se han ido proponiendo. A partir de aquí se inicia una fase de aproximación a cada uno de los candidatos que lleva a pasar a foros y chats privados, en la Deep Web, con acceso restringido y donde no se accede con los buscadores normales. Estas medidas de seguridad son necesarias porque aquí ya se entra en el proceso de captación propiamente dicho, mediante el adoctrinamiento y el intercambio de material terrorista seleccionado para el perfil concreto de ese nuevo seguidor.

[1025] Vid. Supra. Apartado 5.1.3.

Ediciones Universidad de Salamanca | CC BY-NC-ND

ámbito de operaciones[1026], en el que señala su transversalidad respecto a los demás –tierra, mar, aire y espacio-, y la necesidad de implementar los cambios a distinto nivel que conlleva para garantizar su máximo aprovechamiento operativo:

> "To establish cyberspace fully as the fifth domain of operations, crosscutting through the other domains of operations, the understanding of the interdependencies of this domain with the other domains and the subsequent and consistent implementation of the required cultural shifts, enhanced processes, capability developments, organizational adaptations, and cyber skills, are essential. Potential adversaries often operate in cyberspace, which fundamentally changes the operational environment"[1027].

Alineada también con esta transversalidad del ciberespacio, la doctrina española para el empleo de las Fuerzas Armadas lo define como un ámbito[1028] lógico y artificial, creado por el ser humano, compuesto por diversas infraestructuras, redes y sistemas, así como por la información que contienen, transversal al resto de dominios y no sujeto a un espacio geográfico concreto:

> "El ámbito ciberespacial es el ámbito artificial compuesto por infraestructuras, redes, sistemas de información y telecomunicaciones y otros sistemas electrónicos, por su interacción a través de las líneas de comunicación sobre las que se propaga y el espectro electromagnético (EEM), así como por la información que es almacenada o transmitida a través de ellos. Es transversal a los demás ámbitos y no está sujeto a un determinado espacio geográfico. Le caracterizan su extensión, el anonimato, la inmediatez y su fácil acceso. Finalmente, su carácter artificial y su rápida evolución generan continuas vulnerabilidades y oportunidades"[1029].

La Estrategia Nacional de Ciberseguridad de 2019[1030] señala que se trata de un espacio común global, que ofrece oportunidades y presenta desafíos, que posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas:

> "El ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se

[1026] EEAS (2021) 706 REV4. European Union Military Vision and Strategy on Cyberspace as a Domain of Operations. Disponible en: https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf (07/04/2024).

[1027] "Para establecer el ciberespacio como el quinto dominio de operaciones, transversal a los demás dominios, es esencial la comprensión de las interdependencias entre este y los demás dominios y la consistente implementación posterior de los cambios culturales, procesos mejorados, desarrollos de capacidades, adaptaciones organizacionales, y las habilidades cibernéticas. Los adversarios potenciales a menudo operan en el ciberespacio, lo que cambia fundamentalmente el entorno operativo" (Traducción propia).

[1028] En la doctrina anglosajona y de la OTAN se consideran *dominios* lo que la doctrina española nombra como *ámbitos*. Nosotros seguimos en nuestro trabajo el criterio de denominación utilizado por la OTAN, sabedores de que hay grupos de trabajo activos para unificar la terminología empleada por las FFAA españolas y la OTAN.

[1029] *PDC-01 (A) Doctrina para el empleo de las FAS*. Ministerio de Defensa. Febrero 2018. Apartado 3.1.5. Página 81.

[1030] Vid. Supra. Apartado 4.7.7.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad".

Llamamos a recordar nuestra discrepancia, argumentada en su momento[1031], sobre la nota definitoria del ciberespacio que apunta la ESN 2021 al referirse a *su débil regulación y la ausencia de soberanía*, por cuanto es aceptado por la doctrina y la gran mayoría de los miembros de la comunidad internacional que la soberanía es un principio fundamental del Derecho Internacional que, como tal, aplica también al ciberespacio y, por ende, a las ciberoperaciones (SCHMITT, 2017, p. 11).

Por su parte, el Manual Tallinn 2.0 define el ciberespacio como un entorno con componentes físicos y no físicos:

> "The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks"[1032] (SCHMITT, 2017, p. 564).

Asimismo, en su Regla número 1, después de estipular que las capas física, lógica y social del ciberespacio están incluidas en el principio de soberanía de los Estados, las define señalando que la *capa física* comprende los componentes físicos de la red, la *capa lógica* alude a las conexiones entre los dispositivos, y la *capa social* incluye a los individuos y grupos involucrados en las actividades cibernéticas (SCHMITT, 2017, p. 12).

Pero estudiar el ciberespacio como nuevo ámbito de conflicto entre los Estados implica, como haremos seguidamente, atender a la cuestión de si las actividades que en él se desarrollan están bajo el arbitrio del Derecho Internacional, asunto tan esencial como complejo de afrontar por cuanto, como señala el profesor Michael N. Schmitt, las ciberoperaciones difieren de las actividades convencionales que aborda el marco jurídico preexistente, por lo que al tratar de aplicarlo habrá ocasiones en que no tenga sentido, en otras no conseguirá ajustarse a su propósito original y, en tantas otras, deberá ser interpretado para buscar su acomodo a las características propias de las operaciones cibernéticas (SCHMITT, 2022).

A causa de esta complejidad manifiesta que requiere de la interpretación de la norma para su adaptación al caso concreto, la aplicación del Derecho Internacional al ciberespacio es una labor viva, en continuo avance y a la que contribuyen actores como NNUU, con sus dos grupos *ad hoc*, el Grupo de Expertos Gubernamentales (GEG) y el Grupo de Trabajo de Composición Abierta (GTCA)[1033], iniciativas como la del *Derecho cibernético internacional: kit de herramientas interactivo*[1034] en el que se recopilan las posiciones nacionales al respecto, o proyectos como el Manual Tallinn 2.0 que recoge la

[1031] Vid. Supra. Apartado 1.1.2.

[1032] "El entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos mediante redes informáticas" (Traducción propia).

[1033] Vid. Supra. Apartado 2.1.4.

[1034] Esta iniciativa liderada por el NATO CCDCOE, tiene también la participación de la National Cyber and Information Security Agency (NÚKIB), del Comité Internacional de la Cruz Roja (CICR), de la University of Exeter, de la Wuhan University y del U.S. Naval War College. Disponible en: https://cyberlaw.ccdcoe.org/wiki/Main_Page?oldid=4044 (07/04/2024)

Ediciones Universidad de Salamanca | CC BY-NC-ND

opinión de expertos internacionales en colaboración con el NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE), y que conforma actualmente la base de la doctrina existente al respecto. De esta forma, como señala el profesor Schmitt, el cuerpo normativo internacional evoluciona para garantizar su aplicabilidad a lo largo del tiempo:

> "International law necessarily evolves over time in order to ensure that the applicable normative architecture remains responsive to the context in which it applies. That dynamic occurs in three ways – through new treaty law, through the crystallization of new norms of international customary law, and by means of interpretation of existing treaty or customary law"[1035] (SCHMITT, 2022).

Pero esta labor de interpretación de la norma existente no es tarea sencilla, pues la casuística que puede generar la evolución de la tecnología y el nuevo dominio ciberespacial en el marco de las relaciones entre Estados va a llevar al límite la exégesis del Derecho Internacional para tratar de adaptar *lésprit des lois* a ese caso concreto que, por sus peculiaridades digitales, no va a ponérselo fácil a la norma que se pretende aplicar. Un claro exponente de esta situación se presenta, por ejemplo, en el *ius in bello*, con el concepto de *ataque* aplicado al contexto de las ciberoperaciones (CORN, 2020).

El artículo 49.1 del Protocolo Adicional I de los Convenios de Ginebra de 1949, define *ataque* como todo acto de violencia, ofensivo o defensivo, contra el adversario. La norma es clara en su aplicación a una acción cinética convencional, sin embargo, no ocurre lo mismo con las ciberoperaciones maliciosas de un Estado por cuanto sus efectos, de amplio espectro, no siempre pueden calificarse como *actos de violencia contra el adversario*. A este respecto, Gary Corn puntualiza que la violencia conlleva muerte o lesión de personas o daños para las cosas:

> "Of course, substituting "violence" for "attack" itself adds little clarity. To understand the legal definition of attack, one must dive even deeper. It is generally accepted that to qualify as an act of violence, an action must cause some injury or death to persons, or some degree—greater than de *minimis*—of damage or destruction to objects. Where the employment of a means or method of warfare crosses this threshold of harm, the full panoply of targeting law kicks in. In contrast, while not unfettered, non-violent measures are not subject to anywhere near the degree of regulation and restriction as are acts of violence"[1036] (CORN, 2020).

[1035] El Derecho Internacional necesariamente evoluciona con el tiempo para garantizar que la arquitectura normativa aplicable continúe respondiendo al contexto en el que se aplica. Esa dinámica se produce de tres maneras: a través del nuevo derecho convencional, a través de la cristalización de nuevas normas de derecho consuetudinario internacional, y mediante la interpretación del derecho convencional o consuetudinario vigente" (Traducción propia).

[1036] "Por supuesto, sustituir el término *ataque* por *violencia* aporta poca claridad. Para comprender la definición legal de ataque, hay que profundizar aún más. Es generalmente aceptado que para ser calificada como violenta, una acción debe causar alguna lesión o muerte a personas, o algún grado (por encima de *mínimo*) de daño o destrucción de objetos. Cuando el empleo de un medio o método de guerra traspasa este umbral de perjuicio, entra en acción toda la variedad de leyes sobre objetivos. Por el contrario, aunque no sin restricciones, las medidas no violentas no están sujetas ni de lejos al mismo grado de regulación y restricción que los actos de violencia" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Conforme a este planteamiento, si en el contexto de un conflicto armado entre Estados uno de los adversarios lanza un ciberataque que genera daños a objetos o lesiones, incluso muerte, a personas, claramente se concluye que se aplican las normas del derecho de guerra. Ahora bien, la cuestión se complica si los efectos causados están por debajo de esa línea de referencia, por ejemplo, si se exfiltran los datos alojados en servidores del territorio del adversario que permiten, por parte de las empresas particulares, la gestión de las claves de acceso de sus clientes a distintos servicios digitales en la Red[1037]. ¿Constituyen los datos el tipo de bienes a proteger por el DIH, afectando por tanto a las ciberoperaciones destinadas a eliminarlos?.

La calificación de este tipo ciberataque genera un dilema por cuanto el derecho de guerra estipula que solo pueden atacarse objetivos militares y censura los que atañen a personas y bienes de carácter civil. De esta manera, si atendemos al innegable valor de los datos personales en la sociedad digital actual, los daños generados en este supuesto no son precisamente insignificantes y, sin embargo, son eminentemente de carácter civil, por lo que entraría a aplicarse el *ius in bello* ya que esa operación cibernética supondría un *ataque*. Pero si atendemos a una interpretación literal del concepto de *bienes de carácter civil* que protege el Capítulo III del Protocolo Adicional I de los Convenios de Ginebra, y el posterior Comentario del Comité Internacional de la Cruz Roja (CICR) de 1987 sobre la *protección general de los bienes de carácter civil*[1038], en la que los bienes son concebidos como *algo visible y tangible*, esos datos exfiltrados en el ciberataque que nos ocupa quedarían fuera de la definición de bienes y, consecuentemente, no se calificaría la acción como *ataque*[1039], por lo que el derecho de guerra no aplicaría al caso. Esta segunda interpretación literal y restrictiva, alejada del sentido actual de los bienes, llevaría a la paradoja de que la operación cibernética de exfiltración masiva de datos quedaría por debajo el umbral de aplicación de la *lex specialis*.

Por ello, a la luz de los altos niveles de digitalización y dependencia tecnológica de la sociedad actual, parece difícil entender que un ciberataque dirigido a eliminar datos que resultan esenciales para el desarrollo de la vida civil ordinaria, queden fuera del ámbito de aplicación del DIH, dado que:

[1037] Un caso similar al supuesto planteado representa el ciberataque del grupo Blackjack, vinculado al Servicio de Seguridad ucraniano (SBU), que a principios de abril de 2024 destruyen 300 terabytes de datos alojados de un complejo TIC ruso con alrededor de 400 servidores virtuales y 42 físicos, donde se almacenaba información utilizada por industrias militares, de energía y telecomunicaciones rusas, entre las que se encuentra Gazprom, Lukoil, Ural Works of Civil Aviation, NPP Rubin y Rostelecom, entre otras. Disponible en: https://cybernews.com/cyber-war/ukraine-blackjack-destroys-russian-data/ (09/04/2024).

[1038] Comentario de 1987, del CICR, al artículo 52 del Protocolo Adicional a los Convenios de Ginebra de 12 de agosto de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I), de 8 de junio de 1977. Disponible en: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52/commentary/1987 (09/04/2024)

[1039] De hecho, así se manifiestan también parte de los expertos del Manual Tallinn 2.0 en su regla 92.6, señalando que los datos son entidades *no físicas* respecto a la consideración de *ataque* en el contexto de un conflicto armado. Por lo tanto, los datos no serían considerados *bienes* conforme al DIH, por cuanto no son objetos materiales, visibles y tangibles, y por lo tanto no activarían la protección internacional del *ius in bello*.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "La protección de los datos contra las operaciones cibernéticas maliciosas durante un conflicto armado está adquiriendo una importancia cada vez mayor, porque los datos son un componente esencial del dominio digital y un pilar de la vida en muchas sociedades" (GISEL, RODENHÄUSER, & DÖRMANN, 2021, pág. 53).

Con este ejemplo vemos los desafíos que puede comportar la aplicabilidad del Derecho Internacional, conjunto normativo desarrollado a lo largo de distintas épocas, con sociedades, culturas y fases de evolución pretéritas, en el actual contexto digital y tecnológico que caracteriza al ciberespacio y, con ello, a las operaciones cibernéticas que involucran a los Estados en sus relaciones que van desde la más armoniosa paz hasta la más enconada guerra, transitando la ambigüa y extensa Zona Gris.

Por todas estas consideraciones, los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional ocupan a las NNUU desde el año 1998 cuando, a propuesta de la Federación de Rusia, se presentó la primera resolución de la Asamblea General en este sentido[1040], en la que expresa su preocupación "ante la posibilidad de que estos medios y tecnologías se utilicen con fines incompatibles con el objetivo de garantizar la estabilidad y la seguridad internacionales y afecten negativamente a la seguridad de los Estados". Desde entonces y hasta 2015, se nombran tres Grupos de Expertos Gubernamentales (GEG) que examinan las amenazas cibernéticas y las posibles respuestas conjuntas, cada uno de los cuales presenta un informe a la Asamblea General con sus conclusiones, que dan lugar a las respectivas resoluciones en ese lapso de tiempo.

Así, en 2010 el GEG presenta un primer informe[1041] en el que se señala la compleja interconectividad de las telecomunicaciones y de Internet como elemento facilitador para que las TIC puedan ser el origen, debido a su naturaleza de doble uso, de amenazas para la paz y la seguridad internacionales. Como consecuencia, en 2011 la Asamblea General aprueba la resolución A/RES/66/24[1042] en la que, entre otras cuestiones, considera necesario avanzar en "el examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones".

[1040] Resolución aprobada por la Asamblea General -sobre la base del informe de la Primera Comisión (A/53/576)-, relativa a los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/53/70, de 4 de enero de 1999. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F53%2F70&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

[1041] Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/65/201, de 30 de julio de 2010. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F65%2F201&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

[1042] Resolución aprobada por la Asamblea General el 2 de diciembre de 2011 -sobre la base del informe de la Primera Comisión (A/66/407)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/66/24, de 13 de diciembre de 2011. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F66%2F24&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

El segundo informe del GEG se presenta en 2013[1043], y en él se señala que los Estados miembros requieren la necesidad de colaborar en la lucha contra las amenazas derivadas del uso malicioso de las TIC, al tiempo que se reconoce la aplicabilidad de las normas derivadas del Derecho Internacional al uso de este tipo de tecnologías como forma de reducir los riesgos generados y mejorar la seguridad internacional. En diciembre de ese mismo año, la Asamblea General aprueba la resolución A/RES/68/243[1044] donde exhorta a los Estados miembros a seguir colaborando para examinar las amenazas en la esfera de la seguridad de la información y, a su vez, definir estrategias de defensa que sean compatibles con la libre circulación de la información.

El tercer informe del GEG es de junio de 2015[1045] y se ocupa, entre otras materias, de las normas de conducta responsable de los Estados en el ciberespacio, de las medidas para fomentar la confianza y la cooperación entre los países miembros, así como de la forma de aplicar el Derecho Internacional al uso de las TIC por los Estados. En diciembre de ese año 2015, la Asamblea General de NNUU aprueba la resolución A/RES/70/237[1046] en la que, a la vista de los avances logrados, considera necesario seguir trabajando de manera conjunta para analizar la amenaza, acordar las formas de combatirla al tiempo que se preserva el derecho a la libre circulación de la información, y a seguir examinando los conceptos internacionales pertinentes aplicables a las TIC.

Posteriormente, el GEG continuó con su labor pero no logró emitir un informe de consenso, debido a desacuerdos en torno a la forma en que el Derecho Internacional se debe aplicar, si es así, al ciberespacio. Ante esta situación inconciliable, la Asamblea General de NNUU adoptó dos resoluciones diferentes.

La primera de ellas, la resolución A/RES/73/27[1047] de diciembre de 2018, apoyada por Rusia -que promueve la creación de un Grupo de Trabajo de Composición Abierta (GTCA)[1048] paralelo al GEG- en la que expresa preocupación por el hecho de que, algunos

[1043] Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/68/98*, de 24 de junio de 2013. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F68%2F98&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

[1044] Resolución aprobada por la Asamblea General el 27 de diciembre de 2013 -sobre la base del informe de la Primera Comisión (A/68/406)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/68/243, de 9 de enero de 2014. Disponible en: https://documents.un.org/doc/undoc/gen/n13/454/06/pdf/n1345406.pdf?token=LwFmQKlkDjKtsaIiTB&fe=true (09/04/2024).

[1045] Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/70/174, de 22 de julio de 2015. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

[1046] Resolución aprobada por la Asamblea General el 23 de diciembre de 2015 -sobre la base del informe de la Primera Comisión (A/70/455)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/70/237, de 30 de diciembre de 2015. Disponible en: https://www.un.org/es/ga/70/resolutions.shtml (09/04/2024).

[1047] Resolución aprobada por la Asamblea General el 5 de diciembre de 2018 -sobre la base del informe de la Primera Comisión (A/73/505)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/73/27, de 11 de diciembre de 2018. Disponible en: https://www.un.org/es/ga/73/resolutions.shtml (09/04/2024).

[1048] En el que se integran, entre otros, Países Bajos, Alemania, Reino Unido, Finlandia y Brasil.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Estados, están desarrollando capacidades TIC con fines militares cuya utilización en futuros conflictos entre ellos es cada vez más probable, siendo así que NNUU debe impulsar un proceso de negociación sobre la seguridad en la utilización de las TIC "más democrático, inclusivo y trasparente" para, desde el entendimiento común sobre el modo de aplicar el Derecho Internacional, seguir elaborando reglas, normas y principios de comportamiento responsable de los Estados aplicables al uso de las TIC.

La segunda, la resolución A/RES/73/266[1049] de enero de 2019, apoyada por EE.UU. –que fomenta un nuevo GEG- , que comienza confirmando las conclusiones de los informes anteriores de 2013 y 2015, en el sentido de que el Derecho Internacional y, en concreto, la Carta de las NNUU "son aplicables y fundamentales para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico en la esfera de la tecnología de la información y las comunicaciones", exhortando posteriormente a los Estados miembros a apoyar la aplicación de medidas de cooperación para afrontar las amenazas en este ámbito y garantizar un entorno TIC abierto, interoperable, confiable y seguro desde la aplicación de las normas internacionales ya existentes.

En el año 2021 ambos Grupos de Trabajo presentaron sus informes. El GTCA –en el que estaba Rusia- presenta su informe final en enero[1050] y concluye que el continuo aumento del uso malintencionado de las TIC por agentes estatales y no estatales es una tendencia preocupante que, además, puede tener consecuencias humanitarias devastadoras en atención a los objetivos atacados, al tiempo que señala la necesidad de comprender mejor cómo se aplica el Derecho Internacional al uso de las TIC por parte de los Estados, y que la responsabilidad de estos con respecto a los hechos internacionalmente ilícitos se extiende a su empleo de las TIC debiendo "tratar de que ningún agente no estatal, siguiendo instrucciones de un Estado o bajo su control, utilice su territorio para cometer estos actos". Por su parte, el GEG –apoyado por EE.UU.- presenta su informe en julio de ese mismo año 2021[1051], en el que analiza las amenazas actuales y emergentes originadas en el uso malintencionado de las TIC por actores estatales y no estatales, reafirma la existencia de normas voluntarias y no vinculantes de comportamiento responsable de los Estados como clave para la reducción de los riesgos para la paz, la seguridad y la estabilidad internacionales, insiste en la aplicabilidad del Derecho Internacional y la Carta de las NNUU al uso de la estas tecnologías por parte de los Estados, para concluir que, "a medida que los Estados se vuelven cada vez más

[1049] Resolución aprobada por la Asamblea General el 5 de diciembre de 2018 -sobre la base del informe de la Primera Comisión (A/73/505)-. Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. A/RES/73/266, de 2 de enero de 2019. Disponible en: https://www.un.org/es/ga/73/resolutions.shtml (09/04/2024).

[1050] Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Proyecto de informe sustantivo (borrador preliminar). A/AC.290/2021/L2, de 19 de enero de 2021. Disponible en: https://documents.un.org/doc/undoc/ltd/n20/378/97/pdf/n2037897.pdf?token=3hbyOaT0dPfWANsJxK&fe=true (09/04/2024).

[1051] Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional. A/76/135. 14 de julio de 2021. Disponible en: https://documents.un.org/doc/undoc/gen/n21/075/89/pdf/n2107589.pdf?token=wXs1DUNUVgApEXlef4&fe=true (09/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

dependientes de las TIC, es esencial que se observe un marco común de comportamiento estatal responsable en el uso de las TIC en el contexto de la seguridad internacional".

Con el ánimo de continuar avanzando en la consolidación de las normas y principios que deben regular la seguridad y el uso de las TIC por los Estados y, de paso, corregir la duplicación de Grupos de Trabajo avanzando en paralelo, la Asamblea General de NNUU dicta la resolución A/RES/75/240 de enero de 2021[1052], en la que destaca su labor como:

> "[…] rector en la promoción del diálogo entre los Estados Miembros para llegar a un entendimiento común sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones, así como en la elaboración de un entendimiento común sobre la aplicación del Derecho Internacional y de las normas, reglas y principios internacionales para el comportamiento responsable de los Estados en esta esfera".

Es así que NNUU decide crear un nuevo GTCA para el periodo 2021-2025 para seguir elaborando las reglas, normas y principios de comportamiento responsable de los Estados y convenir la forma en que el Derecho Internacional debe aplicarse a la utilización de las TIC por los Estados.

Fruto de los resultados de estos trabajos, en diciembre de 2023 la Asamblea General[1053] presenta los avances del programa de acción para promover el comportamiento responsable de los Estados en el uso de las TIC, y nuevamente decide "crear, una vez que concluya la labor del GTCA (2021-2025) y a más tardar en 2026, un mecanismo permanente, inclusivo y orientado a la acción"[1054] para avanzar en la tarea de comprensión común de las normas y de la aplicación del Derecho Internacional vigente al uso de las TIC y sopesar la creación de nuevas normas voluntarias y no vinculantes, como otras obligaciones jurídicamente vinculantes.

En agosto de 2024 NNUU presenta el *Proyecto de convención de las Naciones Unidas contra la ciberdelincuencia*[1055], como resultado de su compromiso con la necesidad de avanzar en la determinación de acuerdos internacionales contra la ciberdelincuencia, fijando el alcance de los tipos delictivos y el nivel de protección de los derechos humanos frente a ellos. Las posturas encontradas entre los distintos actores estatales intervinientes, entre ellos Rusia, conlleva que en noviembre de 2024 la Asamblea General apruebe sin someter a votación la resolución de *Lucha contra la utilización de*

[1052] Resolución aprobada por la Asamblea General el 31 de diciembre de 2020 -sobre la base del informe de la Primera Comisión (A/75/394, párr. 17)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/75/240, de 4 de enero de 2021. Disponible en: https://international.vlex.com/vid/res-75-240-resolution-861186671 (09/04/2024).

[1053] Resolución aprobada por la Asamblea General el 4 de diciembre de 2023. Programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. A/RES/78/16, de 6 de diciembre de 2023. Disponible en: https://digitallibrary.un.org/record/4029924/files/A_RES_78_16-ES.pdf (09/04/2024).

[1054] IBIDEM página 5/5.

[1055] Ver Capítulo 2, apartado 2.1.4.

Ediciones Universidad de Salamanca | CC BY-NC-ND

las tecnologías de la información y las comunicaciones con fines delictivos[1056], para su firma y entrada en vigor a lo largo de 2025.

Con ello parece tomar forma la teoría de que la interpretación del Derecho Internacional debe ir de la mano de un grupo de trabajo *ad hoc* que, representando distintas posiciones y sensibilidades ideológicas y políticas, vaya consensuando la manera de traducir aquellas normas pretéritas para un mundo físico que, ahora, deben aplicarse en el ciberespacio. No obstante, esa misma voluntad de involucrar a todos los actores internacionales puede, paradógicamente, ser la causa de su estancamiento ante la dificultad de convenir las bases de una interpretación común de la norma que, por la diferente naturaleza política de los Estados, sea prácticamente imposible de alcanzar.

5.3.2. El uso de operaciones cibernéticas maliciosas en las relaciones entre Estados: posicionamiento de la Unión Europea y de la Federación de Rusia

Definido ya el ciberespacio y analizada la utilidad del Derecho Internacional para regular las acciones que en él se desenvuelven en el marco de las relaciones entre los Estados, será nuestro propósito examinar las ciberoperaciones y los posicionamientos que, al respecto, han publicado recientemente algunos de los países miembros de la UE –Irlanda, Alemania y Dinamarca[1057]- y, por su significación en el contexto geopolítico actual, el de la Federación de Rusia.

El Manual Tallinn 2.0 define las ciberoperaciones como medio para alcanzar objetivos en o a través del ciberespacio:

> "The employment of cyber capabilities to achieve objectives in or through cyberspace"[1058] (SCHMITT, 2017, p. 564).

Respecto a los ciberataques, la regla 92 del referido Manual ya incorpora a la ciberoperación el elemento volitivo orientado a la causación, perfeccionada o esperada, de unos efectos dañinos para personas o bienes, estableciendo que:

> "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[1059] (SCHMITT, 2017, p. 415).

Una perspectiva más focalizada en el objetivo, en concreto en la información atacada, la encontramos en la definición que ofrece la Orden Ministerial de 2013 por la que se

---

[1056] Ver Capítulo 2, apartado 2.1.4. Disponible en: https://documents.un.org/doc/undoc/gen/n24/372/07/pdf/n2437207.pdf (01/03/2025)

[1057] Se han elegido estos tres Estados para analizar la orientación europea porque tanto Irlanda como Dinamarca han publicado su posición nacional en el año 2023, y Alemania –que lo hizo en 2021- por su amplia y bien argumentada exposición jurídica de los conceptos tratados.

[1058] "El empleo de capacidades cibernéticas para lograr objetivos en o a través del ciberespacio" (Traducción propia).

[1059] "Un ciberataque es una operación cibernética, ya sea ofensiva o defensiva, de la que razonablemente se espera que cause lesiones o la muerte de personas o daños o destrucción de bienes". (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas –actual Mando Conjunto del Ciberespacio-, al determinar que ciberataque es una acción que compromete la información:

> "Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o de las infraestructuras que los soportan"[1060].

Conforme a lo anterior, podemos proponer una definición de operación cibernética maliciosa (OCM) -o ciberataque- como aquella acción en o a través del ciberespacio, de carácter ofensivo o defensivo que, mediante el ataque a un sistema, sus aplicaciones o sus datos, busca provocar daños a bienes o personas, o comprometer la disponibilidad, la integridad o la confidencialidad de la información que aquel aloja.

Insistimos en la relevancia de los datos y su control como uno de los principales objetivos de los ciberataques, por cuanto la protección de los tres principios que conforman la seguridad de la información, esto es, la confidencialidad de los datos, su integridad y accesibilidad –la *tríada de la CIA*-[1061], son la base sobre la que se evalúa su vulnerabilidad, es decir, el impacto potencial que una amenaza tiene sobre la información y sus sistemas críticos de soporte (WALKOWSKI, 2019). La pugna por el control de los datos es una cuestión estratégica para cualquier Estado en la era digital, lo cual le obliga a tomar acciones preventivas y proactivas en el ciberespacio para garantizar su seguridad[1062].

En cuanto al sujeto pasivo de la OCM, puede tratarse de una persona física o jurídica, de carácter público o privado, un Estado o cualquier otro sujeto de derecho, tanto en su componente físico como virtual y, también, en la esfera de sus derechos. Los daños a personas físicas pueden referirse, por ejemplo, a su salud o integridad física, a su patrimonio, al derecho a la intimidad, a la libre expresión de sus ideas o al acceso a información veraz con la que poder conformar su propio juicio sobre determinada cuestión –claro ejemplo de derecho conculcado por la desinformación-. Tratándose de Estados, el objetivo del ciberataque puede ser la afectación de sistemas esenciales –por ejemplo, servicios de salud o de abastecimiento de agua potable - o infraestructuras críticas –por ejemplo, la red eléctrica o de telecomunicaciones-, e incluso la celebración

[1060] Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Boletín Oficial del Ministerio de Defensa número 40. Martes, 26 de febrero de 2013. Disponible en: https://emad.defensa.gob.es/Galerias/prensa/noticias/Documentos/20130226_CIBERDEFENSA.pdf (08/04/2024).

[1061] La *confidencialidad* de la información se refiere al control del conocimiento sobre los datos para, por un lado, garantizar que solo las personas que tengan la necesidad de conocerlos puedan hacerlo y, por otro, que quien no tenga necesidad de conocer dicha información no llegue a ella. La *integridad* se refiere a la garantía de que la información a la que se accede sea original y no esté manipulada, que sea confiable. En cuanto a la *accesibilidad* –o *disponibilidad*- implica el control de acceso a los datos, para garantizar su disponibilidad y que solo las personas autorizadas puedan tener acceso seguro y fiable a la información cuando lo necesiten.

[1062] Vid. Supra. apartado 1.1.2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

sin injerencias externas de procesos esenciales para las democracias, como las elecciones generales.

En cualquiera de estos casos, la atribución jurídica de una OCM a un Estado en concreto es muy complicada de alcanzar –por no decir imposible-, por mucho que el agredido tenga firmes elementos de convicción moral que le permitan sostener una atribución política, máxime cuando es la Zona Gris el ámbito preferido en el que se desarrollan mayormente este tipo de acciones.

El posicionamiento oficial de los Estados ante las dudas que pueden suscitarse en el trascurso de la aplicación del Derecho Internacional al ciberespacio está siendo compilado por el CCDCOE, a través de su proyecto *Cyber Law Toolkit*[1063], que es un recurso abierto para consulta, disponible en su web, orientado específicamente a la interrelación entre el Derecho Internacional y las operaciones cibernéticas.

Como indicábamos al comenzar el epígrafe, nos centraremos en la posición europea a través de las posturas oficiales recogidas por el CCDCOE en el *Cyber Law Toolkit* de Irlanda, Alemania y Dinamarca, y en la de su principal adversario en el contexto actual de guerra en Ucrania: la Federación de Rusia. Para ello, seguiremos el orden de presentación de las normas y principios que regulan la responsabilidad del Estado por hechos internacionalmente ilícitos, tal y como se recogen en la Resolución A/RES/56/83[1064] aprobada por la Asamblea General en 2002, al tiempo que consultaremos la opinión que sobre el tema manifieste el Manual Tallinn 2.0.

5.3.2.1. El hecho internacionalmente ilícito del Estado: principios generales y atribución

La primera parte del Anexo de la citada Resolución A/RES/56/83, en su capítulo I de principios generales, se refiere al hecho internacionalmente ilícito del Estado (HII), definiéndolo como una acción u omisión atribuible a un Estado, que en sí misma constituya una violación de una obligación internacional y que, consecuentemente, genera responsabilidad para dicho Estado conforme al Derecho Internacional.

Posteriormente, en el capítulo II dedicado a la atribución del comportamiento a un Estado, se considera *hecho del Estado* el comportamiento de los órganos del Estado –tanto del ámbito central como territorial-, de las personas o entidades que ejercen atribuciones del poder público sin ser órgano estatal, de los órganos puestos a disposición de un Estado por parte de otro, de las personas que actúan siguiendo instrucciones, la dirección o el control del Estado, de las personas que ejercen atribuciones de poder público en ausencia o defecto de autoridades oficiales, de los movimientos insurreccionales que se conviertan en el nuevo gobierno del Estado o logren establecer un nuevo Estado y, finalmente, si el comportamiento no es atribuible al Estado conforme a lo anterior pero lo reconoce y adopta como propio.

[1063] Disponible en: https://cyberlaw.ccdcoe.org/wiki/Main_Page (09/04/2024).

[1064] Resolución aprobada por la Asamblea General –sobre la base del informe de la Sexta Comisión (A/56/589 y Corr. 1)- Responsabilidad del Estado por hechos internacionalmente ilícitos. A/RES/56/83, de 28 de enero de 2002. Disponible en: https://international.vlex.com/vid/resolucion-aprobada-asamblea-general-248406 (09/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

En este sentido, el Manual Tallinn 2.0, en su Regla 14 -Actos cibernéticos internacionalmente ilícitos-, especifica que los actos cibernéticos atribuibles a un Estado no son únicamente los ejecutados en manera directa, sino que:

> "The term 'cyber-related acts' is employed in this Rule to denote the fact that a State sometimes may bear responsibility for acts other than cyber operations that it conducts or that are attributable to it. For instance, a State can make its cyber infrastructure available to non-state groups or other States, fail to take required measures to terminate cyber operations from its territory (Rules 6-7), or provide hardware or software to conduct cyber operations. Such activities, *inter alia*, fall within the scope of application of this Rule, as well as others employing the term"[1065] (SCHMITT, 2017, p. 84).

En su posicionamiento sobre esta cuestión, Irlanda sostiene que todo HII de un Estado conlleva necesariamente responsabilidad conforme al Derecho Internacional, de conformidad con la máxima *lex specialis derogat legi generali*. En cuanto a la atribución, distingue entre la de carácter jurídico –evaluación legal basada en el Derecho Internacional y las normas de responsabilidad de los Estados-, y la atribución política –apreciación de carácter político y técnico mayormente basada en datos de inteligencia obtenidos por medios propios.

Alemania coincide en la aplicación en el ámbito del ciberespacio de las normas de Derecho Internacional sobre la responsabilidad de los Estados por HII, insistiendo en que los Estados deben tener control sobre las operaciones cibernéticas que ejecuten actores no estatales siguiendo sus instrucciones, aunque no se les exige un conocimiento detallado de todos los pormenores técnicos involucrados. Respecto a la atribución formal de una OCM a un Estado con arreglo al Derecho Internacional, se trata de una prerrogativa nacional, pero la cooperación y el intercambio de información con socios y aliados es esencial para alcanzar un nivel suficiente de confianza jurídica en dicha asignación de responsabilidad a otro Estado. Asimismo, no existe para el Estado obligación de hacer pública una decisión de atribución de una OCM, de presentar pruebas ni de justificar las posibles medidas de respuesta. No obstante, se acepta la recomendación del GEG de NNUU en su informe de 2015[1066] en cuanto a que las acusaciones de OCM a otro Estado deben fundamentarse y, previamente a la adopción de contramedidas, entablar diálogo para tratar de reconvenir la situación. Sin embargo, la atribución política se hace con discreción y constituye una manifestación de la soberanía del Estado.

[1065] "El término 'actos cibernéticos' se emplea en esta Regla para denotar el hecho de que, a veces, un Estado puede ser responsable de actos distintos de las operaciones cibernéticas que lleva a cabo o que le son atribuibles. Por ejemplo, un Estado puede poner su infraestructura cibernética a disposición de grupos no estatales u otros Estados, no tomar las medidas necesarias para poner fin a las operaciones cibernéticas de su territorio (Reglas 6-7), o proporcionar hardware o software para llevar a cabo operaciones cibernéticas. Dichas actividades, *entre otras cosas*, entran dentro del ámbito de aplicación de esta Regla, así como otras que emplean el término" (Traducción propia).

[1066] Vid. Supra. apartado 5.3.1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Sin embargo, Dinamarca considera que cada Estado puede resolver atribuir públicamente una OCM a otro Estado, siendo que el Derecho Internacional no obliga a compartir las evidencias que respalden esta decisión puesto que, la responsabilidad internacional de ese Estado señalado, no depende de la atribución pública.

Rusia, por su parte, entiende que en el ámbito de la confrontación informativa en el que se desenvuelven las operaciones cibernéticas, puede resultar difícil determinar si una persona o un grupo de ellas actúan bajo la dirección o control de un Estado. Por ello, considera que las acusaciones sobre HII contra un Estado deben ser fundamentadas y, en cualquier caso, para poder atribuírselo hay que aportar las evidencias técnicas que lo justifiquen.

5.3.2.2. La violación de una obligación internacional por parte de un Estado en el ciberespacio: análisis de casos

En base a lo anterior, podemos decir que la existencia de un HII requiere la acción u omisión de un Estado, la correspondiente atribución y que, además, constituya una violación de una obligación internacional que le vincule en el momento de la ejecución.

En cuanto a las ciberoperaciones entre Estados, no están prohibidas por el Derecho Internacional aunque, como cualquier otra acción en el ámbito físico, pueden ser instrumentalizadas para faltar a las obligaciones existentes en el marco de las relaciones internacionales (SALAZAR ALBORNOZ, 2022, pág. 15).

El Manual Tallinn 2.0, en su Regla 14 -Actos cibernéticos internacionalmente ilícitos-, señala que un Estado se encuentra jurídicamente vinculado por sus propias obligaciones convencionales, por el Derecho Internacional consuetudinario y por los principios generales del derecho, constituyendo un HII la falta a cualquiera de ellos:

> "The breach required to establish an internationally wrongful act may consist of a violation of a State´s treaty obligations, customary international law, or general principles of law, 'regardless of [their] origin or character'. As a result, this Rule extends to all obligations in international law that are binding on the responsible State. It encompasses breaches of obligations owed by one State to another, as well as those owed to the international community as a whole"[1067] (SCHMITT, 2017, p. 84).

Siguiendo a la doctora Mariana Salazar Albornoz en su informe al Comité Jurídico Interamericano sobre *El Derecho Internacional aplicable en el ciberespacio* (SALAZAR ALBORNOZ, 2022, págs. 15-22), atenderemos a algunas de las principales obligaciones internacionales que pueden ser vulneradas a través de las ciberoperaciones de Estados.

[1067] "La violación requerida para establecer un hecho internacionalmente ilícito puede consistir en una violación de las obligaciones convencionales de un Estado, del Derecho Internacional consuetudinario o de principios generales del derecho, 'independientemente de [su] origen o carácter'. En consecuencia, esta Regla se extiende a todas las obligaciones de Derecho Internacional que son vinculantes para el Estado responsable. Abarca el incumplimiento de las obligaciones que un Estado tiene con respecto a otro, así como las que tiene con la comunidad internacional en su conjunto" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

A) La soberanía como principio fundamental del Derecho Internacional

La soberanía es un principio fundamental del Derecho Internacional que implica la potestad de ejercer, de forma exclusiva sobre un territorio, las actividades propias de un Estado y que, al mismo tiempo, genera el deber de proteger, dentro de ese territorio, los derechos de los demás Estados, especialmente su integridad e inviolabilidad, en consonancia con lo establecido en el artículo 2.1 de la Carta de las NNUU, que reconoce el principio de la igualdad soberana de todos sus miembros.

El referente para la interpretación de este principio es el laudo arbitral del Tribunal Permanente de Arbitraje, de 1928, sobre el Asunto de la Isla de Palmas[1068], que enfrentó a EE.UU. y los Países Bajos por la reclamación de la soberanía sobre la mencionada isla. El Árbitro del litigio consideró necesario consensuar el significado de la soberanía, dictaminando que:

> "[…] La soberanía referida a una parte de la superficie del globo (terrestre) es la condición jurídicamente necesaria para que dicha parte pueda ser adscrita al territorio de un determinado Estado. […]
> La soberanía en las relaciones interestatales equivale a independencia. La independencia respecto a una parte del globo (terrestre), es el derecho a ejercer en dicho lugar las funciones estatales, con exclusión de cualquier otro Estado. El desarrollo de la organización de las naciones en forma estatal y, correlativamente, el desarrollo del Derecho Internacional, han establecido este principio de la competencia exclusiva del Estado respecto de su propio territorio, de suerte que han hecho de dicho principio el punto de partida para resolver la mayoría de las cuestiones relativas a las relaciones internacionales" (CASANOVAS Y LA ROSA & RODRIGO HERNÁNDEZ, 2016, pág. 382)

El Manual Tallinn 2.0 en su Regla 1 sobre el principio general de la soberanía establece, directamente, que este principio aplica al ciberespacio:

> "The principle of State sovereignty applies in cyberspace"[1069] (SCHMITT, 2017, p. 11)

En la Regla 2 -soberanía interna- señala que el Estado es soberano dentro de su territorio sobre las infraestructuras y actividades cibernéticas, así como respecto a las personas que operen con ellas, lo cual tiene consecuencias en el ámbito del Derecho Internacional respecto a los derechos y obligaciones que comporta en cuanto a su seguridad, las condiciones de uso o la jurisdicción exclusiva, entre otras:

[1068] Laudo arbitral de la Corte Permanente de Arbitraje. Asunto de la Isla de Palmas, Estados Unidos de América vs. Países Bajos. Abril de 1928. Disponible en: https://es.scribd.com/document/440736120/Fallo-Isla-de-Palmas (20/04/2023).
[1069] "El principio de la soberanía del Estado aplica en el ciberespacio" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations"[1070] (SCHMITT, 2017, p. 13).

Siendo aceptado mayormente en la comunidad internacional que la soberanía es una norma fundamental e independiente, estrechamente vinculada a la prohibición del uso de la fuerza y al principio de no intervención, cuya conculcación genera responsabilidad del Estado, debe determinarse en qué casos una ciberoperación puede afectar a la soberanía de otro Estado, es decir, si cualquier penetración en la red de sistemas e infraestructuras de soporte alojados en su territorio ya es suficiente o, por el contrario, debe tener una mínima entidad en sus efectos.

En este sentido, los expertos del Manual Tallinn 2.0 coinciden en que las ciberoperaciones, por sí solas, tienen el potencial de cruzar el umbral de un conflicto armado internacional[1071] (SCHMITT, 2017, p. 384) y, por lo tanto, pueden vulnerar las obligaciones para con la soberanía de otros Estados. En igual sentido se pronuncian, por ejemplo, países líderes en el ciberespacio como EE.UU. que afinan aún más la cuestión por cuanto consideran que las ciberoperaciones de un Estado que involucran a estructuras TIC de otro no suponen *per se* una violación de su soberanía, aunque pueden hacerlo si superan unos efectos mínimos. Se apoyan para sostener su tesis en que el Derecho Internacional no prohíbe el ciberespionaje (SALAZAR ALBORNOZ, 2022, pág. 16), cuestión que también comparte el Manual Tallinn 2.0 en su Regla 32 –ciberespionaje en tiempo de paz- en cuanto que:

> "Although peacetime cyber espionage by States does not *per se* violate international law, the method by which it is carried out might do so"[1072] (SCHMITT, 2017, p. 168).

En el ámbito europeo, Irlanda entiende que el respeto a la soberanía es una obligación en sí misma por lo que su afectación a través de una ciberoperación supone, en todo caso, un HII si causa daños físicos o deterioro funcional a infraestructuras críticas o sistemas TIC, o si interfiere con los datos o despliega efectos secundarios. Es decir, la naturaleza y consecuencias de la OCM son relevantes para determinar la existencia de una violación al principio de soberanía de otro Estado. En todo caso, un Estado no puede invocar la soberanía para justificar el incumplimiento de sus obligaciones internacionales.

Alemania piensa igualmente que el principio de soberanía de los Estados se aplica a sus actividades en el ciberespacio, que no es un foro desterritorializado. Se protege la soberanía y el correspondiente ejercicio legítimo de jurisdicción respecto a las actividades cibernéticas y las personas que participan en ellas, y sobre las

[1070] "Un Estado disfruta de autoridad soberana con respecto a la infraestructura cibernética, las personas y las actividades cibernéticas ubicadas dentro de su territorio, sujeto a sus obligaciones legales internacionales" (Traducción propia).
[1071] Regla 82, apartado 16.
[1072] "Aunque el ciberespionaje de los Estados en tiempos de paz no viola *per se* el Derecho Internacional, el método mediante el cual se lleva a cabo podría hacerlo" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

infraestructuras TIC que les dan servicio, en el ámbito de su territorio. En este sentido, señala que por la alta interconexión transfronteriza de las infraestructuras cibernéticas, el ejercicio de jurisdicción de un Estado en el ciberespacio puede repercutir en la esfera jurisdiccional de otro Estado, por lo que es necesario prestar la debida atención a posibles efectos adversos en estos casos. El reconocimiento de la soberanía de los Estados en el ciberespacio supone también su independencia para decidir libremente qué papel desempeñan las TIC en su organización gubernamental y administrativa, así como en su política exterior. Por ello, la injerencia de un Estado extranjero en el proceso de elecciones democráticas de otro supone una violación de su soberanía y constituye un HII. Por tanto, las OCM atribuibles a un Estado que violan la soberanía de otro son contrarias al Derecho Internacional, para lo cual deben valorarse los efectos físicos y daños causados en su territorio a las infraestructuras TIC y dispositivos conectados –analógicos y digitales-, así como las deficiencias funcionales y efectos físicos secundarios derivados en dichas infraestructuras, teniendo presente que no constituyen por sí solos violación de la soberanía de un Estado las ciberoperaciones que causen meros efectos físicos de insignificante entidad, ni las deficiencias funcionales por debajo de un umbral mínimo de impacto. Si la infraestructura atacada es crítica o corresponde a una empresa de especial interés público, sí se considera conculcada la soberanía del Estado, pero requerirá el análisis caso por caso puesto que no existen definiciones internacionalmente consensuadas para algunos de los términos involucrados –infraestructura crítica, interés público, etc.-.

Dinamarca coincide en la consideración de la soberanía como norma primaria del Derecho Internacional, cuya atribución a un Estado presupone el ejercicio de la responsabilidad. Distingue por un lado la soberanía interna, que aplica a las ciberoperaciones del Estado y a cualquier infraestructura TIC alojada en su territorio, así como a las actividades asociadas independientemente de su carácter público o privado, que obliga al Estado a mantener la debida diligencia para evitar que su territorio, y el ciberespacio asociado, sea utilizado para la comisión de HII. Y por otro lado, la soberanía externa que, conforme al artículo 2.1 de la Carta de las NNUU, implica la igualdad de derechos y deberes entre Estados y el reconocimiento entre ellos de su independencia. En cuanto a las OCM, para valorar si violan la soberanía de un Estado habrá que analizar tanto su naturaleza como los efectos causados, teniendo para ello en consideración el grado de infracción de la integridad territorial y si ha habido interferencia o, incluso, usurpación de funciones inherentemente gubernamentales. Si causan daños o pérdida de funcionalidad a sistemas TIC, dependiendo de su nivel de afectación y entidad, podrán constituir violación de la soberanía y, por ello, HII una vez atribuidas a un Estado. Si los efectos son insignificantes o la pérdida de funcionalidad mínima, la OCM no supone violación de la soberanía.

En cuanto a la Federación de Rusia, entiende que, por el momento, la comunidad internacional ha llegado a un consenso sobre la aplicabilidad de los principios y normas fundamentales del Derecho Internacional consagrados en la Carta de las NNUU, entre los que se incluyen el principio de igualdad soberana de los Estados, la prohibición del uso de la fuerza, la no injerencia en asuntos internos de los Estados y la solución de controversias por medios pacíficos, entre otros. Conforme a ello, presume que las obligaciones de los Estados derivadas del Derecho Internacional y sus fuentes, son

Ediciones Universidad de Salamanca | CC BY-NC-ND

aplicables al espacio de la información como marco de las ciberoperaciones. Teniendo en cuenta la naturaleza jurídica específica de este entorno y la anonimidad propia de quienes actúan en él, la aplicación del Derecho Internacional a las actuaciones en el ciberespacio no debería ser automática ni, tan siquiera, por simple extrapolación desde el ámbito físico o analógico, por lo que propone que a nivel internacional, y bajo el auspicio de NNUU, se continúe discutiendo en foros específicos y abiertos cómo aplicar a las TIC el Derecho Internacional existente.

B) El principio de no intervención

El principio de no intervención es una norma de Derecho Internacional consuetudinario que entraña no interferir en los asuntos que un Estado puede libremente decidir en el marco de su soberanía, y no utilizar métodos de coerción para ganar ventaja sobre ellos. En el ciberespacio cabe discutir si la coerción aplica en el caso de que se trate de modificar específicamente el comportamiento del otro Estado o, al contrario, basta con que la OCM busque privarle de su capacidad de controlar aquellos asuntos que caen en el ámbito de su *domaine réservé* (SALAZAR ALBORNOZ, 2022, pág. 17)

El Manual Tallinn 2.0 en su Regla 2.10 considera que la soberanía de un Estado incluye su independencia y, con ella, la prohibición de intervenir por parte de otros en su dominio reservado:

> "Internal sovereignty also includes the authority of a State to independently decide on its political, social, cultural, economic, and legal order. Accordingly, the principle of sovereignty underlines the prohibition of unlawful intervention into a State´s *domaine réservé*"[1073] (SCHMITT, 2017, p. 15).

Respecto a la aplicabilidad de este principio en el ciberespacio, Irlanda considera que debe tratarse de una intervención de entidad y gravedad suficientes, comparable en escala y efectos a una acción coercitiva en el ámbito físico convencional. No obstante, eso no supone que las OCM puedan ser consideradas formas legales de influencia y presión entre Estados por lo que, por debajo de ese umbral, si se consigue hacer la atribución a un Estado, no incluyen la posibilidad del uso de contramedidas para obligarle a cumplir con sus obligaciones en base a la comisión de un HII, que no existiría.

Alemania, por su parte, entiende que coerción implica uso de fuerza y que las OCM sólo en determinados casos equivalen a ella, proponiendo para su acertada evaluación la equiparación en cuanto a escala y efectos de las OCM con una acción coercitiva en el plano físico convencional. Para apreciar coerción en la acción de un Estado debe, por un lado, superar un umbral mínimo en sus efectos y, por otro, debe ir acompañada del componente de intencionalidad –intervenir en los asuntos propios de otro Estado-. Así, no implicarán coerción las formas duras o mordaces de comunicación ni la crítica aguda, como tampoco los intentos persistentes de obtener una determinada reacción de otro

[1073] "La soberanía interna también incluye la autoridad de un Estado para decidir independientemente sobre su orden político, social, cultural, económico y jurídico. En consecuencia, el principio de soberanía subraya la prohibición de la intervención ilegal en el *dominio reservado* de un Estado" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Estado, en el marco ordinario de la disuasión política. Especialmente preocupante se considera la interferencia en los procesos electorales ajenos a través de ciberoperaciones que pueden enmarcarse en una campaña de influencia, desprestigio o desinformación más amplia, o actuar más concretamente para apoyar a determinadas opciones políticas o candidatos con el fin de obtener algún tipo de ventaja por parte del actor estatal que la fomenta. Estas OCM son similares, en el plano físico, al apoyo a la insurgencia que, tradicionalmente, se interpreta como coerción desde el Derecho Internacional.

Para que una OCM sea ilícita desde el punto de vista de Dinamarca, esta debe cumplir los dos requisitos ya señalados: interferir en asuntos de exclusiva prerrogativa soberana de otro Estado, e implicar coerción. El problema radica en que este término, coerción, no está definido en los tratados ni acordado en el Derecho Internacional consuetudinario. Por ello, es precisa la interpretación particular de los afectados que, en el caso de Dinamarca, entiende la coerción como la acción con potencial para obligar al Estado objetivo a hacer algo en el ámbito de su dominio soberano que, de no mediar esta influencia, no haría y, además, que ese resultado coincida con la intención del Estado que ejerce la acción coercitiva. Esta afectación lograda a través de la coerción no debe confundirse con la influencia derivada de la persuasión política o la labor diplomática. Finalmente, destacar que Dinamarca entiende que la coerción no se limita al uso de la fuerza, sino que también engloba aquellas medidas de bajo impacto que quedan por debajo del umbral tradicional de fuerza. Esto se traduce en que pueden llevarse a efecto OCM que no superen ese umbral de uso de la fuerza pero que sí resulten coercitivas por los efectos causados, como por ejemplo la alteración del voto electrónico en el proceso electoral de otro Estado con la intención de variar el resultado y favorecer al candidato más propicio para los intereses del actor.

A este respecto, la Federación de Rusia no se pronuncia en su posicionamiento publicado en el CCDCOE.

C) La prohibición del uso de la fuerza

El artículo 2.4 de la Carta de las NNUU proscribe la amenaza o el uso de la fuerza en las relaciones internacionales[1074], siendo que la interpretación que viene haciéndose del término *fuerza* se identifica con el *ataque armado*, aunque no todos los países lo entienden así, como por ejemplo Irlanda. De esta forma, para determinar si una OCM viola esta prohibición del Derecho Internacional, habrá previamente que acordar cuándo puede ésta constituir una fuerza equivalente a la armada.

Se propone para ello interpretar que una OCM iría contra la prohibición del uso de la fuerza si su escala y los efectos causados son comparables a los de una acción cinética convencional a la luz del Derecho Internacional, analizando caso por caso. Para este análisis casuístico algunos países, como EE.UU., consideran que debe atenderse a la

[1074] Artículo 2.4 Carta de las Naciones Unidas: ”Los miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas”.

Ediciones Universidad de Salamanca | CC BY-NC-ND

naturaleza y alcance del daño a las cosas, la causación de muerte o lesiones en personas, el contexto de la OCM y el tipo de actor que la ha lanzado, el objetivo atacado y la intención final del ciberataque. Otros, como Brasil, en línea con la postura defendida por el GTCA sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, consideran complicado establecer analogías directas entre actos de agresión cinética en el plano físico y las ciberoperaciones, creyendo necesario avanzar en un acuerdo internacional de consenso para delimitar qué OCM pueden constituir uso de fuerza a través de las TIC (SALAZAR ALBORNOZ, 2022, pág. 18).

Por su parte, el Manual Tallinn 2.0 dedica tres de sus Reglas al uso de la fuerza. La Regla 68 se refiere a la prohibición de la amenaza o el uso de la fuerza, recurriendo a la reafirmación de la aplicabilidad del artículo 2.4 de la Carta de las NNUU a las ciberoperaciones:

> "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful"[1075] (SCHMITT, 2017, p. 329).

Por su parte, la Regla 6 define el uso de fuerza en las ciberoperaciones, utilizando la escala y los efectos producidos como criterio de comparación respecto a las acciones que conllevan uso de la fuerza en el plano físico:

> "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force"[1076] (SCHMITT, 2017, p. 330).

Y la Regla 70 define la amenaza de fuerza en línea con lo establecido para el ámbito físico:

> "A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force"[1077] (SCHMITT, 2017, p. 338).

El posicionamiento de Irlanda sobre esta cuestión comienza por advertir que no todo uso de la fuerza contrario a la prohibición del artículo 2.4 de la Carta de las NNUU equivale a un ataque armado. Esta prohibición se debe aplicar independientemente de las armas o los medios empleados, y habrá que atender caso por caso a la escala y los efectos de la acción, tanto en el ámbito físico como en el digital. Para Irlanda, una OCM

[1075] "Una operación cibernética que constituya una amenaza o uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o que de cualquier otra manera sea incompatible con los propósitos de las Naciones Unidas, es ilegal" (Traducción propia).
[1076] "Una operación cibernética constituye un uso de la fuerza cuando su escala y efectos son comparables a operaciones no cibernéticas que alcanzan el nivel de uso de la fuerza" (Traducción propia).
[1077] "Una operación cibernética, o una amenaza de operación cibernética, constituye una amenaza ilegal de fuerza cuando la acción amenazada, de llevarse a cabo, constituiría un uso ilegal de la fuerza" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

atribuida a un Estado cuyos efectos sean, por ejemplo, deteriorar significativamente la funcionalidad de una infraestructura crítica, aún sin causar daño físico alguno, equivale al uso de la fuerza y como tal genera responsabilidad internacional. Igualmente, una OCM cuyos efectos estén incluso por debajo del umbral del uso de la fuerza puede constituir una acción ilegal de intervención en los asuntos de jurisdicción o soberanía exclusiva de un Estado, como por ejemplo la exfiltración de datos digitales del censo en un proceso de elecciones con la intención de hacer prospectiva para, posteriormente, su uso en operaciones de influencia o campañas de desinformación.

Alemania opina que, para catalogar una OCM como análoga al uso de la fuerza, hay que atender a los efectos causados, más que a los medios empleados. Una OCM puede cruzar el umbral del uso de la fuerza y causar daños significativos de dos formas: siendo un componente más de un ataque cinético más amplio y coordinado o, por sí sola, en base a la valoración caso por caso de su escala y efectos en comparación al uso de la fuerza convencional, de acuerdo a criterios como el contexto del ciberataque, la gravedad de la interferencia en las redes y sistemas o el nivel de intrusión alcanzado, entre otros.

Dinamarca, por su parte, conviene la equiparación entre ciberoperaciones y ataques armados convencionales caso por caso, en base a la escala física y los efectos ocasionados, de forma que la causación de lesiones o muerte a personas y de daños físicos significativos implican el uso de la fuerza. Los factores de valoración para concluir si una OCM alcanza la entidad de ataque armado son, principalmente, la gravedad, inmediatez, invasividad y mensurabilidad de los efectos, junto con el carácter militar de la OCM, la autoría de un Estado y la ilegalidad de la acción. Finalmente, se llama la atención sobre el hecho de que la coerción económica o política entre Estados, para Dinamarca, pueden significar el empleo de la fuerza, por lo que una OCM que afecte a los sistemas financieros de un Estado provocando daños económicos importantes conllevarán responsabilidad internacional por violar la prohibición del uso de la fuerza entre Estados.

A este respecto, la Federación de Rusia no se pronuncia en su posicionamiento publicado en el CCDCOE, aunque cabe pensar que, como miembro integrante del GTCA sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, no sea partidaria de aplicar la analogía entre los actos de agresión cinética en el plano físico y las ciberoperaciones, y que considere más apropiado avanzar en un acuerdo internacional de consenso para delimitar qué OCM pueden constituir uso de fuerza a través de las TIC.

D) El deber de la debida diligencia

Esta norma de carácter voluntario del Derecho Internacional da carta de naturaleza a la locución latina *sic utere tuo ut alienum non laedas*[1078], en el sentido de que los Estados no sólo se benefician de los privilegios de la soberanía, sino que también tienen el deber de asumir las responsabilidades que comporta para, en su libre ejercicio, no perjudicar

[1078] "Usa lo tuyo para no dañar lo del otro" (Traducción propia)

Ediciones Universidad de Salamanca | CC BY-NC-ND

la de otros. Esta es una de las bases de la seguridad colectiva y todos los miembros de la comunidad internacional comparten la responsabilidad de velar por ella (CASANOVAS Y LA ROSA & RODRIGO HERNÁNDEZ, 2016, pág. 1049).

Esta responsabilidad ejercida a través del deber de la debida diligencia comporta que todo Estado vele por que su territorio no sea utilizado, a sabiendas, para actos que perjudiquen al resto de Estados y, la omisión de este deber, conlleva responsabilidad internacional, tal y como dictaminó en 1949 la Corte Internacional de Justicia en el Caso del Canal de Corfú[1079], ante la inactividad de Albania para prevenir a Reino Unido del peligro existente al cruzar su mar territorial, plagado de minas[1080].

La aplicación por analogía de esta norma al ciberespacio implica que los Estados ostenten la soberanía digital sobre las infraestructuras y sistemas alojados en su territorio, pero también que tengan la obligación de adoptar medidas razonables, conforme a sus capacidades, para que desde ellas no se realicen OCM. En todo caso, si un Estado tuviera conocimiento de que desde su ciberespacio se ha lanzado un ataque contra otro Estado, debe notificárselo para facilitar su mitigación y aclarar los hechos (SALAZAR ALBORNOZ, 2022, págs. 18-19).

Esta es también la postura que refleja el Grupo de Expertos Gubernamentales sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, en su informe a la Asamblea General de NNUU de julio de 2021[1081], donde especifica que los Estados no deben permitir, a sabiendas, que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando las TIC, para lo cual los Estados deben tener en cuenta que:

> "La norma establece la expectativa de que los Estados tomen medidas razonables dentro de su capacidad para poner fin a la actividad que tiene lugar en su territorio por medios que sean proporcionados, apropiados y eficaces y de forma coherente con el Derecho Internacional e interno. No obstante, no se espera que los Estados puedan o deban controlar todas las actividades relacionadas con las TIC que se realizan en su territorio"[1082].

[1079] Caso del Canal de Corfú, fallo de la Corte Internacional de Justicia de 9 de abril de 1949. Disponible en: https://www.dipublico.org/115899/caso-del-canal-de-corfu-fondo-del-asunto-fallo-de-9-de-abril-de-1949/ (12/04/2024).

[1080] Al parecer las minas las habían instalado en dicho paso dos buques yugoslavos, a petición de Albania o, al menos, con su aquiescencia. Aunque no se pudiese comprobar dicha connivencia, al tratarse de aguas territoriales de Albania, su deber de control exclusivo dentro de sus fronteras forma parte del principio de soberanía y, esta, conlleva una serie de obligaciones y responsabilidades internacionales como hemos visto.

[1081] Vid. Supra. Apartado 5.3.1.

[1082] Grupo de Expertos Gubernamentales sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. A 76/135, de 14 de julio de 2021. Disponible en: https://documents.un.org/doc/undoc/gen/n21/075/89/pdf/n2107589.pdf?token=K25XH9WD42U5HeiMa3&fe=true (12/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por su parte, el Manual Tallinn 2.0 dedica las Reglas 6 y 7 a la debida diligencia, estableciendo en la primera de ellas las bases de aplicación de dicho principio al ciberespacio:

> "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States"[1083] (SCHMITT, 2017, p. 30).

La Regla 7 se refiere al cumplimiento de este principio a través del despliegue de todas las medidas posibles, dentro de las capacidades propias, para evitar OCM que perjudiquen a otros Estados:

> "The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States"[1084] (SCHMITT, 2017, p. 43).

En cuanto a la posición de los miembros europeos, Irlanda entiende que el deber de diligencia se deriva del principio de soberanía y constituye una norma de conducta, no de resultado, que es claramente aplicable al ciberespacio. En este dominio, la debida diligencia implica que un Estado debe adoptar todas las medidas posibles dentro de sus capacidades para evitar que, desde su territorio o por personas bajo su jurisdicción, se lleven a cabo OCM que perjudiquen a otros Estados. Además, este deber también incluye un elemento preventivo, referido a la adopción de aquellas medidas razonables que permitan anticiparse a esas ciberoperaciones potencialmente dañinas para la comunidad internacional. La cuestión que Irlanda propone para debate y adopción de un criterio común en los Grupos de Trabajo de NNUU, es el de si el conocimiento implícito de una OCM que puede perjudicar a otro Estado supone, de por sí, incumplir la obligación de la debida diligencia.

Alemania, por su parte, se posiciona a favor de considerar aplicable en el ciberespacio el principio de debida diligencia, resaltando su importancia para la preservación de la seguridad internacional por el alto nivel de interconexión de las infraestructuras y sistemas digitales en la sociedad actual, que claramente trascienden fronteras.

Dinamarca considera que un Estado es responsable internacionalmente cuando no adopta todas las medidas de que es capaz para evitar que un actor, sea cual sea su naturaleza, lleve a cabo una OCM desde su territorio o utilizando las infraestructuras o sistemas en él instalados. Es obligación del Estado no permitir conscientemente este tipo de actuaciones desde el ciberespacio, lo que supone implementar todas las medidas

[1083] "Un Estado debe ejercer la debida diligencia para no permitir que su territorio, o la infraestructura cibernética en su territorio o bajo su control gubernamental, se utilice para operaciones cibernéticas que afecten los derechos de otros Estados y produzcan consecuencias adversas graves para ellos" (Traducción propia).

[1084] "El principio de diligencia debida exige que un Estado adopte todas las medidas que sean factibles, dadas las circunstancias, para poner fin a las operaciones cibernéticas que afecten al derecho de otros Estados, y produzcan consecuencias adversas graves para ellos" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

razonables para prevenir, eliminar y mitigar los daños que puedan perjudicar los intereses o derechos de otros Estados o, en general, de la comunidad internacional. En este sentido, el daño debe ser potencialmente significativo y no limitarse a simples inconvenientes o perturbaciones menores, las cuales no activan esta responsabilidad del Estado. Por otra parte, la postura de Dinamarca coincide con la de Irlanda en cuanto que entiende que la debida diligencia es una obligación que impone una conducta y cuyo incumplimiento genera, en el Estado afectado, el derecho a la adopción de contramedidas si se cumplen las condiciones que implican esa responsabilidad.

Tampoco sobre este principio de debida diligencia se pronuncia la Federación de Rusia en su posicionamiento ante el CCDCOE.

E) El Derecho Internacional humanitario

Partiendo del hecho de que la Carta de las NNUU y el Derecho Internacional consuetudinario -*ius ad bellum*- rigen todo uso de la fuerza por parte de los Estados, ya sea ésta de naturaleza cinética o cibernética, podemos justificar la aplicabilidad del DIH, que conforma el *ius in bello* de los conflictos armados entre Estados, a las ciberoperaciones que los contendientes lleven a cabo como acciones ofensivas o defensivas propias de la guerra, en la que se emplean junto con -o en apoyo de- las demás armas convencionales y del resto de avances tecnológicos orientados a la obtención de alguna ventaja frente al enemigo.

Sin embargo, la naturaleza digital del quinto dominio y la interconexión global de las infraestructuras y sistemas que lo soportan, conllevan una serie de dificultades a la hora de aplicar en este ámbito las normas y principios que protegen a los civiles y a los bienes no afectos a un uso militar.

La primera de las cuestiones a resolver para considerar la adaptación del DIH a las ciberoperaciones es la noción de *ataque*, por cuanto algunas normas basadas en los principios de distinción, proporcionalidad y precaución[1085] solo serán de aplicación en este contexto. En este sentido, el artículo 49 del Protocolo Adicional I a los Convenios de Ginebra (PAICG) entiende por ataques "los actos de violencia contra el adversario, sean ofensivos o defensivos" [1086].

Sobre esta misma base normativa define el Manual Tallinn 2.0, en su Regla 92, el ciberataque:

[1085] Los artículos 51 y 52 del Protocolo Adicional I a los Convenios de Ginebra de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales, de 1977, establecen la protección de la población civil y de los bienes de carácter civil, respectivamente, prohibiendo los ataques indiscriminados y los que tengan como objetivo a la población o bienes civiles, entre otros. Complementariamente, se obliga a las partes en conflicto a limitar los ataques estrictamente a objetivos militares, a tomar las precauciones factibles para evitar o reducir lo máximo posible los daños civiles y a la proporcionalidad entre la ventaja militar conseguida y los daños causados. Disponible en: https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977 (14/04/2024).

[1086] IBIDEM artículo 49, donde se definen los ataques y su ámbito de aplicación en cuanto a territorio, dominios, personas y bienes.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[1087] (SCHMITT, 2017, p. 415).

Otra de las cuestiones debatidas respecto a las ciberoperaciones, como ya analizamos anteriormente, es la de la *naturaleza violenta* del ataque y el alcance de sus efectos para los civiles[1088], por cuanto pueden afectar considerablemente a infraestructuras críticas y servicios esenciales, con el consiguiente alcance a la vida de las personas, incluso sin causar daño físico alguno. Dado que el DIH a través del artículo 54 del PAICG[1089] protege los bienes indispensables para la supervivencia de la población civil, entran aquí en consideración aquellas infraestructuras críticas que permiten el funcionamiento de las centrales eléctricas y, con ellas, los hospitales o las potabilizadoras de agua, por ejemplo. En este mismo sentido, sobre la base del referido artículo, se pronuncia la Regla 141 del Manual Tallinn 2.0 respecto a las ciberoperaciones:

> "Attacking, destroying, removing, or rendering useless objects indispensable to the survival of the civilian population by means of cyber operations is prohibited"[1090] (SCHMITT, 2017, p. 531).

A este respecto, en el apartado 5 de esta Regla se puntualiza que Internet no es un bien indispensable para la supervivencia de los civiles, no así otro tipo de infraestructuras digitales:

> "The Internet (or other communications network) does not, in and of itself, qualify as an object indispensable to the survival of the civilian population. In the context of cyber operations, however, cyber infrastructure indispensable to the functioning of electrical generators, irrigation works and installations, drinking water installations, and food production facilities could, depending on the circumstances, qualify" [1091] (SCHMITT, 2017, p. 533).

[1087] "Un ciberataque es una operación cibernética, ya sea ofensiva o defensiva, de la que se espera razonablemente que cause lesiones o la muerte a personas o daños o destrucción de objetos" (Traducción propia).

[1088] Vid. Supra. Apartado 5.3.1.

[1089] El artículo 54 del Protocolo Adicional I a los Convenios de Ginebra de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales, de 1977, prohíbe expresamente utilizar como método de guerra el hacer pasar hambre a la población civil, así como atacar, destruir o inutilizar los bienes indispensables para su supervivencia -alimentos, zonas agrícolas, cosechas, ganado, instalaciones de agua potable, etc.-.

[1090] "Está prohibido atacar, destruir, sustraer o inutilizar objetos indispensables para la supervivencia de la población civil mediante operaciones cibernéticas" (Traducción propia).

[1091] "Internet (u otra red de comunicaciones) no es, en sí misma, un objeto indispensable para la supervivencia de la población civil. Sin embargo, en el contexto de las operaciones cibernéticas, la infraestructura cibernética indispensable para el funcionamiento de generadores eléctricos, obras e instalaciones de riego, instalaciones de agua potable e instalaciones de producción de alimentos podría serlo, según las circunstancias" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

También es asunto primordial para el *ius in bello* la protección de las unidades y el personal médico[1092], que no pueden ser objeto de ataque. La consiguiente obligación de respetar y no causar ningún tipo de daño a las unidades sanitarias, en el marco de un conflicto armado, incluye no interferir en su labor ni destruir sus equipos o medios de transporte, ya sea con un ataque convencional o digital, tal y como recoge la Regla 131 del Manual Tallinn 2.0:

> "Medical and religious personnel, medical units, and medical transports must be respected and protected and, in particular, may not be made the object of cyber attack"[1093] (SCHMITT, 2017, p. 513).

Pero esta misma obligación se extiende también a las comunicaciones, los equipos informáticos, los sistemas y redes de soporte de esas unidades sanitarias y, también, a los datos médicos que alojan, todo lo cual tiene una vinculación directa e inmediata con las ciberoperaciones, que quedan proscritas en el DIH tal como indica la Regla 132 del Manual Tallinn 2.0:

> "Computers, computer network, and data that form an integral part of the operations and administration of medical units and transports must be respected and protected, and in particular not be made the object of attack"[1094] (SCHMITT, 2017, p. 515).

Todo lo anterior nos lleva a sostener que la protección de la población civil y las infraestructuras de igual carácter esenciales para su supervivencia durante un conflicto armado, así como las obligaciones derivadas, conciernen al uso de las ciberoperaciones por parte de los contendientes y que, por ello, no quedan en un vacío jurídico, sino que están reguladas por el Derecho Internacional y, especialmente, por el DIH (GISEL, RODENHÄUSER, & DÖRMANN, 2021, pág. 52).

Las opiniones de los Estados que han expresado públicamente su posición varían en la interpretación de algunas de las cuestiones referidas. Irlanda entiende que el DIH es aplicable a las ciberoperaciones que tienen lugar en el contexto de una guerra y que causen lesiones o la muerte de personas, daños físicos a bienes, o la pérdida de funcionalidad en redes o sistemas informáticos. Asimismo, considera que las OCM con efectos similares a operaciones cinéticas convencionales pueden ser la causa de un conflicto armado en relación al nivel de intensidad del ataque. Finalmente, concluye que la aplicabilidad del DIH al ciberespacio no alienta ni legitima su militarización.

[1092] A este respecto véase, por ejemplo, el Capítulo III, artículos 19 y 20 del I Convenio de Ginebra de 1949, el Capítulo II, artículos 12 y 13 del II Convenio, o el Título II, articulo 18 del IV Convenio. También en el mismo sentido, el artículo 12 del PACG I y el artículo 11 del PACG II. Este conjunto de normas protege a los hospitales y barcos con esta consideración, a las unidades y los medios de transporte sanitarios, a los heridos, a los enfermos y a los náufragos, entre otros.

[1093] "El personal médico y religioso, las unidades sanitarias y los transportes sanitarios deben ser respetados y protegidos y, en particular, no pueden ser objeto de ciberataques" (Traducción propia).

[1094] "Los ordenadores, las redes informáticas y los datos que forman parte integrante de las operaciones y la administración de las unidades y transportes sanitarios deben ser respetados y protegidos y, en particular, no ser objeto de ataques" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Alemania interpreta que un ciberataque es un acto iniciado en o a través del ciberespacio para causar efectos nocivos en las comunicaciones, en los sistemas informáticos o en la información alojada o transmitida a través de ellos, pero también en los objetos y las personas. En este sentido, la mera intrusión en redes extranjeras o la copia de sus datos no constituye un ataque. No obstante, no es necesario que se produzcan daños físicos en bienes o la muerte o lesión de personas comparables a los causados por una acción convencional, para considerar que una OCM constituye un ataque conforme al DIH. Éste será aplicable siempre que esas ciberoperaciones tengan un nexo causal con el esfuerzo militar empleado en el conflicto armado, independientemente de su calificación como lícitas o ilícitas desde la perspectiva del *ius ad bellum*. Igualmente, los ciberataques de suficiente entidad e impacto lanzados por un grupo armado[1095] contra un Estado, pueden considerarse como un conflicto armado no internacional y, por lo tanto, es de aplicación el DIH.

Dinamarca entiende que una ciberoperación se considera ataque en el contexto de guerra declarada, cuando produzca efectos similares a los causados por un ataque cinético convencional. De esta manera, el DIH aplicará en el caso de un ciberataque cuando sea razonable esperar que éste cause muerte o lesiones a personas y daños físicos a bienes, directa o indirectamente.

La Federación de Rusia tampoco se pronuncia sobre estos extremos en su posicionamiento publicado en la página del CCDCOE.

5.3.2.3. Medidas de respuesta ante un ataque: legítima defensa y contramedidas

El Derecho Internacional prevé medidas de respuesta que el Estado puede adoptar frente al ataque de otro Estado, centrándonos en nuestro análisis en las dos principales para el objeto de nuestro estudio: la legítima defensa y las contramedidas.

A) La legítima defensa

El artículo 21 de la Resolución de las NNUU sobre la responsabilidad de los Estados por HII[1096] se refiere a la legítima defensa como una medida que habilita para utilizar de manera lícita recursos que, de otra forma, constituirían una violación del Derecho Internacional:

> "La ilicitud del hecho de un Estado queda excluida si ese hecho constituye una medida lícita de legítima defensa tomada de conformidad con la Carta de las Naciones Unidas".

[1095] En este caso Alemania se refiere indirectamente a grupos terroristas con suficiente capacidad ofensiva para lanzar ciberataques, como Al Qaeda o DAESH.

[1096] Resolución aprobada por la Asamblea General -sobre la base del informe de la Sexta Comisión (A/56/589 y Corr.1)-. Responsabilidad del Estado por hechos internacionalmente ilícitos. A/RES/56/83, de 28 de enero de 2002. Disponible en: https://international.vlex.com/vid/resolucion-aprobada-asamblea-general-248406 (15/04/2024)

Ediciones Universidad de Salamanca | CC BY-NC-ND

Éste, a su vez, se vincula con el artículo 51 de la Carta de las Naciones Unidas, el cual determina que, solo ante un ataque armado, el Estado tiene el derecho a la legítima defensa:

> "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales".

Una vez convenido que el DIH se aplica tan pronto como existe un conflicto armado entre Estados a consecuencia del uso de la fuerza, en cuyo ámbito de interpretación entran las OCM como ya hemos estudiado, y existiendo distintas interpretaciones en cuanto al nivel de intensidad necesario para que esa fuerza adquiera la consideración de ataque armado, debemos centrarnos en su aplicación a las ciberoperaciones como HII legitimadores del recurso a la legítima defensa.

El Manual Tallinn 2.0, en su Regla 71, atiende a la legítima defensa frente a ataques armados y considera que una operación cibernética puede ser motivo de ella en base a su escala y efectos:

> "A State that is the target of a cyber operation thar rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects" [1097] (SCHMITT, 2017, p. 339).

En la Regla 72, por su parte, considera que el recurso a las ciberoperaciones en virtud del derecho de legítima defensa debe ser necesario y proporcionado:

> "A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate"[1098].

A este respecto, Irlanda entiende que no todo uso de la fuerza supone un ataque armado que justifique la legítima defensa, teniendo que acudir a su escala y efectos caso por caso para analizarlo. Esto mismo aplica a las ciberoperaciones y el umbral de violencia que permita el ejercicio de la legítima defensa, que solo en circunstancias excepcionales alcanzan la escala y los efectos que permitan asimilarlos a un ataque armado convencional.

[1097] "Un Estado que sea objetivo de una operación cibernética que alcance el nivel de un ataque armado puede ejercer su derecho inherente a la legítima defensa. Que una operación cibernética constituya un ataque armado depende de su escala y efectos" (Traducción propia).
[1098] "El uso de la fuerza que implique operaciones cibernéticas realizadas por un Estado en el ejercicio de su derecho de legítima defensa, debe ser necesario y proporcionado" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Alemania también considera que para que una ciberoperación pueda constituir un ataque armado, sus efectos y escala deben ser comparables a los de un ataque cinético, para lo cual hay que valorar parámetros como la destrucción física de bienes producida, la causación de muerte o lesiones a personas, si ha supuesto una incursión territorial grave, el contexto estratégico en el que se genera y los efectos causados fuera del ciberespacio por dicha OCM. Si aún así el Estado agraviado considera que la OCM es equiparable a un ataque armado, debe comunicarlo al Consejo de Seguridad de NNUU conforme a lo establecido en el artículo 51 de la Carta, para que se active el recurso de la legítima defensa. Una vez hecho esto, la respuesta a una OCM puede articularse a través de todos los medios necesarios siempre que sean proporcionales, puesto que la legítima defensa no requiere responder con los mismos medios del ataque. En este sentido, también los actos cibernéticos consumados de agentes no estatales[1099] pueden asimilarse a un ataque armado y justificar el recurso a la legítima defensa.

En cuanto a la postura de Dinamarca, no todo uso ilegal de la fuerza equivale a un ataque armado, de forma que una OCM podrá considerarse como tal si sus efectos son asimilables a los de una acción cinética convencional que sí tenga esa consideración. Coincide con Alemania en que una ciberoperación de un actor no estatal puede justificar una respuesta de legítima defensa.

Una vez más, la Federación de Rusia no se manifiesta sobre este asunto en su posicionamiento ante el CCDCOE.

B) Las contramedidas

En cuanto a las contramedidas, el artículo 22 de la Resolución de las NNUU sobre la responsabilidad de los Estados por HII[1100] señala que:

> "La ilicitud del hecho de un Estado que no esté en conformidad con una obligación internacional suya para con otro Estado queda excluida en el caso y en la medida en que ese hecho constituya una contramedida tomada contra ese otro Estado de acuerdo con lo dispuesto en el capítulo II [contramedidas] de la tercera parte [modos de hacer efectiva la responsabilidad internacional del Estado]".

Por su parte, el artículo 49 define el objeto y los límites de las contramedidas[1101], disponiendo que el fin último es inducir al Estado atacante a que cumpla sus obligaciones internacionales, para lo que se permite el incumplimiento temporal por

[1099] Nuevamente Alemania se refiere indirectamente a grupos terroristas con suficiente capacidad ofensiva para lanzar ciberataques, como Al Qaeda o DAESH.

[1100] Resolución aprobada por la Asamblea General -sobre la base del informe de la Sexta Comisión (A/56/589 y Corr.1)-. Responsabilidad del Estado por hechos internacionalmente ilícitos. A/RES/56/83, de 28 de enero de 2002.

[1101] El artículo 49 estipula que: "1) El Estado lesionado solamente podrá tomar contramedidas contra el Estado responsable del hecho internacionalmente ilícito con el objeto de inducirlo a cumplir las obligaciones que le incumban en virtud de lo dispuesto en la segunda parte. 2) Las contramedidas se limitarán al incumplimiento temporario de obligaciones internacionales que el Estado que toma tales medidas tiene con el Estado responsable. 3) En lo posible, las contramedidas serán tomadas en forma que permitan la reanudación del cumplimiento de dichas obligaciones".

Ediciones Universidad de Salamanca | CC BY-NC-ND

parte del agraviado de las que le vinculen respeto a aquel. Esta respuesta debe ser proporcional y notificada -salvo casos de urgencia- al Estado agresor. Igualmente, las contramedidas no pueden afectar a la prohibición del uso de la fuerza y al resto de normas del DIH.

En cuanto a su aplicación al ámbito del ciberespacio, existen dos particularidades derivadas de su propia naturaleza. Primeramente, la dificultad en la atribución de las OCM supone un problema para poder justificar una contramedida, tal y como señala la doctora Salazar Albornoz:

> "Ante las dificultades en materia de atribución y a que las contramedidas presuponen la existencia de un HII, a la fecha, ningún Estado ha enmarcado su respuesta a una ciberoperación maliciosa como una contramedida" (SALAZAR ALBORNOZ, 2022, pág. 23).

En segundo lugar, la obligación de notificar la adopción de contramedidas al Estado agresor cabría entenderla excepcionada en el ciberespacio, en atención a la naturaleza lógicamente encubierta de las intromisiones cibernéticas en las redes y sistemas de otro Estado, por la misma necesidad de dar una cobertura adecuada a la contramedida si se articula a través de una ciberoperación, y por el breve espacio de tiempo que se dispone para poder responder de manera efectiva a una OCM.

Conforme a este planteamiento, Irlanda entiende que las contramedidas en el ámbito del ciberespacio deben ser igualmente proporcionadas y de carácter temporal, y en ningún caso pueden suponer el uso de la fuerza. Por otra parte, no es necesario que sean las mismas que las utilizadas en el ataque, por lo que a una OCM ofensiva se puede responder con una contramedida convencional, no digital.

Alemania, por su parte, considera que tanto las violaciones convencionales como cibernéticas de las obligaciones internacionales de un Estado pueden ser respondidas, igualmente, mediante contramedidas de cualquier naturaleza -físicas o digitales-. En cuanto a las contramedidas cibernéticas, están sujetas a las mismas limitaciones que las convencionales y, además, requieren un uso ponderado y meticuloso por los posibles efectos secundarios no deseados, derivados de la interconectividad característica de las infraestructuras TIC. Asimismo, Alemania defiende que un Estado atacado puede llevar a cabo ciberoperaciones de reconocimiento en las redes y sistemas del atacante, para explorar posibles opciones de respuesta y evaluar el riesgo potencial de los efectos secundarios.

La postura de Dinamarca se construye desde la consideración de que un Estado puede verse afectado por una OCM que no alcance el nivel mínimo de catalogación como ataque para suponer un HII, frente a la cual se pueden adoptar medidas de naturaleza diplomática, económica o política, perfectamente encuadrables en la Zona Gris. Las violaciones, de cualquier naturaleza, de obligaciones internacionales por parte de un Estado pueden responderse con contramedidas convencionales o cibernéticas del agredido, siendo deseable que, si son de estas últimas, sus efectos sean reversibles. Dinamarca plantea la cuestión de si es viable que un Estado responda con una contramedida frente a un ciberataque que aún no se ha llegado a consumar, pero del

Ediciones Universidad de Salamanca | CC BY-NC-ND

que se tiene plena certeza que va a producirse. Su postura es afirmativa en el sentido de entender que sí cabe adoptar contramedidas contra una OCM aún no lanzada, porque un Estado no tiene obligación de sufrir un daño real para poder adoptar una contramedida preventiva, que es temporal y orientada a inducir al atacante a que cumpla sus obligaciones internacionales.

La Federación de Rusia considera que las contramedidas no pueden afectar a la obligación de los Estados de abstenerse del uso de la fuerza, de la obligación de proteger los derechos humanos fundamentales, las obligaciones del DIH y otras obligaciones que derivan del Derecho Internacional general, tal y como recoge el artículo 50 de la Resolución de las NNUU sobre la responsabilidad de los Estados por HII[1102].

5.3.3. Reflexiones sobre la aplicabilidad del Derecho Internacional al ciberespacio

Las operaciones cibernéticas son una manifestación más de la forma en que los Estados, actualmente, pueden relacionarse y entrar en conflicto para tratar de influir en otros actores, defender sus posicionamientos, responder ante una agresión o complementar a las acciones cinéticas convencionales en una guerra.

Todo ello en el marco del Derecho Internacional que, a través de sus normas generales y especiales, trata de dar respuesta a las nuevas situaciones que derivan de la naturaleza digital del quinto dominio. A este respecto, sin embargo, hay dos posturas en la comunidad internacional. Por un lado, la de aquellos países que entienden que el Derecho Internacional puede aplicarse al ciberespacio mediante la interpretación de sus normas –EE.UU. y la mayoría de los países de la Unión Europea-. Y por otro, la de aquellos que, como Rusia, Reino Unido o Brasil, consideran que ese cuerpo normativo internacional no puede aplicarse tal cual, por analogía o interpretación, al espacio de la información, y que propugnan el acuerdo entre los Estados de la comunidad internacional para, por consenso, definir la interpretación de esos conceptos jurídicos elaborados en otros tiempos para otras problemáticas distintas y, en caso de que esto no sea suficiente para atender al caso concreto planteado, elaborar nuevas normas vinculantes que ayuden a regular los conflictos en el contexto actual.

En este sentido, Moynihan señala que el Derecho Internacional es aplicable a las actividades de los Estados en el ciberespacio conforme a los tratados pertinentes y, en caso de ausencia de estos, debe recurrirse al Derecho Internacional consuetudinario vigente, pues sus principios y normas son aplicables en el nuevo dominio "unless there

[1102] La Resolución aprobada por la Asamblea General sobre la responsabilidad del Estado por hechos internacionalmente ilícitos (A/RES/56/83), en su artículo 50 determina las obligaciones que no pueden ser afectadas por las contramedidas: "1) Las contramedidas no afectarán: a) La obligación de abstenerse de recurrir a la amenaza o al uso de la fuerza, como está enunciada en la Carta de las Naciones Unidas; b) Las obligaciones establecidas para la protección de los derechos humanos fundamentales; c) Las obligaciones de carácter humanitario que prohíben las represalias; d) Otras obligaciones que emanan de normas imperativas del Derecho Internacional general. 2) El Estado que tome contramedidas no quedará exento del cumplimiento de las obligaciones que le incumban: a) En virtud de cualquier procedimiento de solución de controversias aplicable entre dicho Estado y el Estado responsable; b) De respetar la inviolabilidad de los agentes, locales, archivos y documentos diplomáticos o consulares".

Ediciones Universidad de Salamanca | CC BY-NC-ND

is state practice with *opinio iuris* to indicate that a relevant principle or rule is not applicalbe"[1103] (MOYNIHAN, 2020, pág. 56).

En otro orden de cosas, el Derecho Internacional resulta aplicable al ciberespacio independientemente de las mayores o menores capacidades técnicas de un Estado para ejercer efectivamente su jurisdicción en él y poder manifestar, mediante su ejercicio, su soberanía digital, por cuanto que, haciendo analogía de lo establecido para el ámbito físico:

> "El hecho de que un Estado no pueda probar el ejercicio de soberanía sobre dichas partes del territorio no puede interpretarse precipitadamente en el sentido de que dicha soberanía no existe. Cada caso debe considerarse según las circunstancias propias del mismo" (CASANOVAS Y LA ROSA & RODRIGO HERNÁNDEZ, 2016, pág. 385).

En este mismo sentido, la Regla 4.1 del Manual Tallinn 2.0 señala que las ciberoperaciones que violan la soberanía de otro Estado constituyen un hecho internacionalmente ilícito:

> "Cyber operations that prevent or disregard another State´s exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law. Of course, in certain situations international law permits or envisages exceptions to the obligation to respect another State´s sovereignty. The paradigmatic examples are when an action that would otherwise violate the latter´s sovereign is authorised by the Security Council (Rule 76) or is engaged in pursuant to the exercise of the right of self-defence (Rule 71)"[1104].

Para concluir, indicar que el hecho de la aplicabilidad del Derecho Internacional al ciberespacio, a través de su interpretación y analogía, no impide que el cuerpo normativo que lo conforma deba continuar siendo desarrollado por los Estados, mediante el debate en foros y grupos de trabajo liderados por NNUU como vía para llegar al consenso sobre la forma de interpretar dichos preceptos o, también, para definir nuevas normas de carácter voluntario con las que regular esas nuevas situaciones de difícil encaje en el Derecho Internacional preexistente. Y ello habrá de hacerse sobre la base de la valoración y el conocimiento actualizado del desarrollo de las nuevas capacidades militares en el ciberespacio, sus posibles repercusiones para las personas y el espíritu de protección hacia estas que, desde su origen, han alimentado al Derecho Internacional.

[1103] "Salvo que exista una práctica estatal con *opinio iuris* que indique que un principio o norma pertinente no es aplicable" (Traducción propia).

[1104] "Las operaciones cibernéticas que impiden o ignoran el ejercicio de sus prerrogativas soberanas por parte de otro Estado constituyen una violación de dicha soberanía y están prohibidas por el Derecho Internacional. Por supuesto, en determinadas situaciones el Derecho Internacional permite o prevé excepciones a la obligación de respetar la soberanía de otro Estado. Los ejemplos paradigmáticos son cuando una acción que de otro modo violaría la soberanía de este último es autorizada por el Consejo de Seguridad (Regla 76) o se lleva a cabo en virtud del ejercicio del derecho de legítima defensa (Regla 71)" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

5.4. Conclusiones: el impulso de la amenaza con el salto del mundo físico al plano digital

La amenaza evoluciona conforme lo hace la sociedad a la que afecta. Así, la guerra, como conflicto armado entre Estados, se ha ido transformando de la mano de la política y la evolución tecnológica para adaptarse al escenario internacional de cada momento.

Si hasta el siglo XX la guerra clásica se libraba en un campo de batalla físico y delimitado, entre ejércitos nacionales, regulares y simétricos en cuanto a sus capacidades, a partir de la llegada de la era digital, en un contexto de globalización, ambigüedad e interdependencia tecnológica, el conflicto armado evoluciona en sus medios y técnicas de combate para adaptarse a un nuevo campo de batalla extendido, propio de la guerra híbrida.

En la guerra híbrida se combinan de manera simultánea todas las capacidades militares, políticas y civiles en los dominios terrestre, marítimo, aéreo, espacial y cibernético para alcanzar los mayores efectos en las tres dimensiones en que tiene lugar el enfrentamiento: la física, la virtual y la cognitiva. Se tratan de ejecutar de esta forma las operaciones multidominio para aprovechar cualquier tipo de ventaja frente al enemigo.

Es en este contexto donde adquieren relevancia el ciberespacio y las acciones ofensivas y defensivas que en él se llevan a cabo, a tenor de lo cual se plantea la cuestión de si, en las guerras actuales, como por ejemplo la de Rusia y Ucrania, la clave que puede determinar la inclinación de la balanza a favor de uno u otro de los contendientes es la capacidad ofensiva en el quinto dominio, en detrimento de las acciones cinéticas convencionales.

La contestación a esta pregunta divide a los teóricos de la guerra, que se dividen entre los que ven la ciberguerra como sustitutiva del clásico enfrentamiento parametrizado por Clausewitz, los que entienden las ciberoperaciones como una herramienta más que complementa a las armas convencionales y, finalmente, los que consideran que las operaciones en el ciberespacio evolucionan de manera autónoma e independiente a las acciones de guerra que se desarrollan en el resto de dominios físicos.

En cualquier caso, el ciberespacio es interpretado de distinta forma e integrado de diferente manera en la estrategia geopolítica de los Estados, lo que unido a la alta dependencia tecnológica de las sociedades actuales nos lleva a pensar que los conflictos armados del futuro tendrán un elevado nivel de confrontación cibernética, pero ello no parece indicar que las operaciones cinéticas convencionales, también cada vez más tecnificadas y digitales, vayan a desaparecer. La clave parece estar en las operaciones multidominio y la habilidad de cada contendiente para integrar todas sus capacidades ofensivas bajo una misma dirección.

La segunda gran amenaza examinada por orden cronológico, el terrorismo, se distingue por la dificultad de su conceptualización jurídica, dado su carácter eminentemente político y la instrumentalización de la violencia que ejerce bajo cualquier ideología política, social o religiosa, de forma que los mismos hechos, dependiendo de por quién

Ediciones Universidad de Salamanca | CC BY-NC-ND

sean interpretados, pueden ser calificados de diferente manera. Ello no ha impedido los esfuerzos por acordar, a nivel internacional, unas características mínimas que permitan definir una acción violenta como terrorista. A esta tarea se han aplicado las NNUU, la OTAN, la UE, e incluso los Estados individualmente, como España a través de su Código Penal, sin alcanzar la pretendida definición jurídica de terrorismo, quedándose en el acuerdo de la comunidad internacional sobre determinados actos violentos que se catalogan como tal.

La nueva amenaza terrorista golpea brutalmente los valores occidentales el 11 de septiembre de 2001 y demuestra que, con su evolución, se ha adaptado perfectamente al mundo interconectado y global, consiguiendo con ello elevar su estatus a nivel internacional. Este escenario de violencia trasciende con mucho el enfoque de la respuesta individual de carácter nacional, siendo necesario a partir de entonces un compromiso conjunto y complementario para unir fuerzas frente a la yihad internacional radical.

En lo que concierne a España, ésta ha sufrido los envites del terrorismo desde finales del siglo XIX con el anarquismo, pasando posteriormente por la lucha contra el terrorismo autóctono de ETA y los GRAPO, hasta sufrir el terrible atentado de Atocha, en Madrid, el 11 de marzo de 2004, que abre una serie de atentados en suelo europeo que continúan produciéndose y sumando víctimas a fecha de hoy.

El primer exponente de esta amenaza terrorista internacional fue Al Qaeda que, con sus atentados de septiembre de 2001, no solo desafió a la primera potencia mundial sino que consiguió lanzar una llamada a todos los islamistas radicales del mundo para que se sumaran a su causa: la yihad. Su relevo lo toma DAESH, que va un paso más allá con la instauración del Califato Islámico, asentado en un área territorial muy amplio sobre el que ejerce potestades cuasi soberanas, y que elabora una estrategia comunicativa centralizada, profesionalizada y bien planificada con la que vertebrar su mensaje propagandístico y proselitista.

La yihad violenta se complementa con otros modelos evolucionados de yihad, como la judicial, que se basa en el permanente recurso a los tribunales occidentales para judicializar todo tipo de causas, con el objetivo principal de desgastar a quienes les critican o contradicen, al tiempo que mantienen la narrativa del victimismo como grupo señalado en las sociedades libres y democráticas. En esta misma línea, la yihad digital aprovecha todo el potencial de Internet para la expansión de su mensaje de terror y, también, para el envío de instrucciones operativas y los procesos de captación y radicalización de seguidores. DAESH ha demostrado su adaptación al ciberespacio y ha abierto un nuevo frente de batalla virtual que complementa al militar, sobre la idea de una yihad poliédrica que ofrece al musulmán fiel y comprometido dos caminos para su recorrido: el activismo digital y el activismo operativo. De esta forma, quien no quiera o no pueda empuñar las armas puede hacer la yihad desde el ciberespacio, con labores tan importantes como la propaganda, la captación, la difusión de mensajes y consignas o la elaboración de material de adoctrinamiento y especialización en técnicas de combate o de preparación de explosivos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

La tercera amenaza es la proveniente de las operaciones maliciosas en el ciberespacio, que requiere atender previamente a la cuestión de si las actividades que en él se llevan a cabo entran en el ámbito de aplicación del Derecho Internacional, dado que su naturaleza digital y tecnológica no parece casar bien con un conjunto normativo desarrollado para responder a una realidad física y analógica muy distinta a la actual.

Los desafíos que comporta interpretar el Derecho Internacional para adaptarlo a las ciberoperaciones que involucran a los Estados son fuente de discusión doctrinal, pues hay que recurrir en no pocas ocasiones a la adaptación, caso por caso, de conceptos y principios cruciales como el de ataque, soberanía, uso de la fuerza o la debida diligencia, para ver cómo, desde el ciberespacio, interactúan en las relaciones entre los Estados.

De esta manera, cabe concluir que la aplicabilidad del Derecho Internacional a las ciberoperaciones a través del recurso a la analogía y la interpretación no es óbice para que, en paralelo, se siga avanzando por la comunidad internacional en una doble vía. Por un lado, llegar a consensos sobre la forma de interpretar esos principios y conceptos nucleares que contienen la esencia del espíritu de la ley para, desde acuerdos en grupos de trabajo *ad hoc* liderados por NNUU, determinar esas bases que permitan la adaptación del Derecho Internacional a las nuevas situaciones que demanda el ciberespacio. Y por otro, la redacción de nuevos preceptos de carácter voluntario que solventen esos casos de difícil encaje en el cuerpo normativo preexistente, de forma que el Derecho Internacional siga evolucionando para mantenerse activo y aplicable a la realidad global, digital y tecnológica actual. En cualquier caso, el progreso, los conflictos y las relaciones humanas son inseparables, y el Derecho Internacional debe avanzar con ellos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 6. EL DESAFÍO DE SEGURIDAD EN LA ZONA GRIS

Una vez estudiada la evolución de la amenaza y su ágil adaptación a los nuevos dominios que incorporan las relaciones internacionales, debemos referirnos al espacio que ocupa la denominada *Zona Gris*. Para ello, antes incluso de definirla, es menester precisar que el uso de la Zona Gris, como todo entorno de conflicto, es consustancial a las relaciones de poder entre Estados y, nos atreveríamos a decir, entre humanos por cuanto que, desde siempre, ha existido una amplia órbita de actuación entre las relaciones de paz y armonía sustentadas en la buena fe de las partes, y el exasperado encono que enciende la peor y más destructiva de las manifestaciones humanas: la guerra.

Queda de esta forma respaldado que, en las relaciones políticas ordinarias entre Estados, de amistad, de colaboración, de competencia, de supervivencia o de cualquier otra clase, entre el blanco fulgúreo de la paz y el lóbrego negro de la guerra invariablemente ha venido existiendo una amplia gama de grises que definen esa zona de estar y conducirse en la política internacional que, actualmente, conocemos como *Zona Gris*.

6.1. La ambigüedad entre la paz y la guerra: la Zona Gris

Habiendo concurrido desde siempre ese amplio espectro de actuación para la gestión de intereses en la actividad política, es con la globalización y el crecimiento exponencial de la interdependencia entre los actores internacionales cuando estos adquieren un perfil poliédrico el cual, a su vez, determina la insuficiencia de las categorías clásicas -aliado, amigo, enemigo, ataque, paz, guerra- para anclar las referencias que, antes, permitían ubicar exactamente en qué nivel de ese continuo se encontraban dichas relaciones (AZNAR FERNÁNDEZ-MONTESINOS, 2024, págs. 324-330). Cuando los extremos son antagónicos y las acotaciones entre ellos equidistantes y nítidas, es muy fácil conocer el punto exacto en el que nos encontramos y tomar las decisiones que correspondan para continuar el trayecto. El problema radica cuando el camino que conecta los opuestos se desdibuja por la niebla y se pierden las guías que sirven para fijar dónde estamos y cuánto queda para llegar a nuestro destino, surgiendo la duda, la indecisión e, incluso, la paralización ante la falta de perspectiva. Esta es la Zona Gris (en adelante ZG).

De esta manera, podemos convenir que la ZG conforma ese espacio impreciso en el que la guerra y la política comparten objetivos, cuya estrategia "aúna a un tiempo y de modo casi indiferenciado, actuaciones pacíficas y cuasi hostiles entre Estados que mantienen relaciones pacíficas" (AZNAR FERNÁNDEZ-MONTESINOS, 2024, pág. 327).

Y es esta, precisamente, la primera característica que nos va a servir para definir la ZG: *la paz como marco de referencia*. No obstante, como señala Baqués, hay que precisar que se trata de una paz:

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] polemológica, es decir, una paz en la que se rompe de modo intencionado el principio de *bona fides* que debería regir en las relaciones entre Estados. Se puede decir con más contundencia planteándolo al revés: se trata de una paz presidida por la *mala fe*" (BAQUÉS QUESADA, 2021, pág. 115).

Este planteamiento hobbesiano, en el que la mala fe descabalga a la *bona fides* en las relaciones entre Estados, nos conduce inexorablemente al escepticismo y a la duda, a la dificultad a la hora de identificar los autores e interpretar sus acciones hostiles y, con ello, a *la ambigüedad* como otro rasgo típico de la ZG que, lógicamente, complica la adopción de una respuesta adecuada, acertada y, sobre todo, en tiempo oportuno. La auténtica complejidad en la ZG reside en saber -o poder- diferenciar una agresión que trata de pasar desapercibida, bajo el umbral de respuesta, de lo que se podría entender como competencia dentro de los parámetros usuales de la política entre Estados. Como señala Jordán:

> "[…] resulta sencillo determinar el límite entre Zona Gris y el conflicto armado, pero la frontera se desdibuja en el extremo opuesto al diferenciarla de la competencia pacífica. […] En la práctica, esto no siempre es fácil de demostrar, ya que el actor hostil puede recurrir a medios propios tanto de la competencia pacífica como de la Zona Gris con justificaciones plausibles de carácter legal, económico, humanitario, de seguridad, etc. La ambigüedad resultante dificulta la detección, la disuasión y la respuesta, a la que fácilmente se calificará de sobrerreacción" (JORDÁN ENAMORADO, 2022, pág. 75).

Se incorpora de este modo a la ZG otra de sus peculiaridades: *el componente híbrido y, a la vez, asimétrico*. En base a éste, el agresor va a tratar de alcanzar sus objetivos estratégicos utilizando de manera coordinada instrumentos de poder multidimensionales -diplomáticos, informacionales, militares, económicos- pero sin sobrepasar las líneas rojas que delimitan el *statu quo* en el que se encuentra cómodo el adversario, y que supondrían llegar al enfrentamiento militar abierto. Es por ello que sean las potencias iliberales revisionistas, en las que se legitiman acciones formalmente democráticas "pero teleológicamente contrarias a ella" (SÁNCHEZ BARRILAO, 2020, pág. 117) las que, principalmente, tratan de ganar ventaja en este terreno con el objetivo de alterar ese orden internacional con el que discrepan, mientras garantizan su propia seguridad prevaliéndose del marco normativo que, paradójicamente, les protege (VILLENA SÁNCHEZ & AZNAR FERNÁNDEZ MONTESINOS, 2022, págs. 21-22).

También *el gradualismo* constituye un atributo esencial de la ZG, en cuanto método empleado por el agresor para ir logrando paulatina y lentamente avances parciales sin obtener respuesta de la contraparte. El Estado que se instala en la ZG suele ser revisionista y disconforme, pero aún mantiene su capacidad de maniobra en el tablero de juego del orden internacional para, sin comprometer su seguridad ni su supervivencia, tratar de obtener alguna ventaja en la competencia por el poder. Para ello planifica a largo plazo su estratagema de erosión y desgaste del contrario, en la conocida como *salami tactics*, consciente de que la consolidación del auténtico objetivo final que pretende -la desestabilización del adversario- será en base a la suma de efectos progresivamente alcanzados a lo largo del tiempo y que hayan conseguido pasar por debajo del umbral de respuesta (BAQUÉS QUESADA, 2021, págs. 124-126).

Ediciones Universidad de Salamanca | CC BY-NC-ND

En este sentido, el actor instalado en la ZG pretende que sus operaciones pasen inadvertidas para el agredido y, si son detectadas por éste, que queden por debajo del umbral del entendimiento. Caso de que sean entendidas, que permanezcan por debajo del umbral de decisión y, si se llega a tomar una decisión por el adversario, que esté por debajo del umbral de respuesta, es decir, "que no merezca la pena una respuesta por la dinámica en la que se puede entrar" (GUTIÉRREZ DE LEÓN, 2021)

Finalmente hay que citar como rasgo distintivo de la ZG, como señala la nota conceptual[1105] *El papel de las FAS en la Zona Gris (ZG) – (NCZG)*, del Estado Mayor de la Defensa (EMAD)[1106], el hecho de que la población civil desempeña un papel central en la operativización de la estrategia híbrida, ya sea como *objetivo de las narrativas* propagandísticas o desinformadoras que buscan sustentar el rol asumido por el agresor, o bien como *instrumento ofensivo* a través del cual canalizar las movilizaciones sociales que tratan de desacreditar las instituciones o desestabilizar el orden interno del Estado atacado.

De esta forma, una vez determinada la existencia de ese espacio entre la paz y la guerra, de naturaleza ambigua, híbrida, asimétrica, gradual y ampliamente enfocada en la población civil, podemos afirmar que la ZG no es la mera constatación de un marco relacional de transición del blanco al negro, de un polo al otro, sino que goza de entidad propia en base a sus objetivos, sus herramientas y sus efectos (BAQUÉS QUESADA, 2021, págs. 119-120), por lo que trataremos ahora de definirla.

6.1.1. Definición de Zona Gris

En base a los elementos que se prioricen al delimitar la ZG pueden concluirse diversas definiciones de la misma. Pero primeramente conviene hacer una precisión terminológica por cuanto, en ocasiones, parte de la doctrina asimila la ZG con la *guerra hibrida*, como ocurre en el informe *Countering Hybrid Warfare*, del Multinational Capability Development Campaign (MCDC)[1107], que define las campañas en ZG en base a la criticidad de las vulnerabilidades atacadas, la sincronización de medios utilizados y los consecuentes efectos para el Estado agredido, fijando que:

> "Hybrid warfare is the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects. The challenge presented by revisionist actors who exploit

[1105] Una nota conceptual es un "documento de reflexión con carácter prospectivo, de menor entidad que un concepto, que investiga sobre elementos de referencia con vistas a un posterior desarrollo conceptual. Su oportunidad vendrá derivada, normalmente, de evoluciones en el entorno operativo, posibilidades de mejorar capacidades con nuevas tecnologías, cambios orgánicos, nuevos procedimientos, u otras causas" (JEMAD, Instrucción Comunicada 10/21, «Instrucción de Conceptos Conjuntos». Noviembre de 2021).
[1106] Nota Conceptual *El papel de las FAS en la zona gris (ZG) – (NCZG)*. Centro Conjunto de Desarrollo de Conceptos del Estado Mayor de la Defensa. 14 de marzo de 2022. Página 3.
[1107] MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. March 2019. Disponible en: https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf (02/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> hybrid warfare has a broad impact across societies, national government and multinational institutions"[1108] (MONAGHAN & et al., 2019, pág. 3).

El mismo documento especifica que el uso del término *guerra* en el ámbito de la amenaza híbrida no implica una equiparación, por cuanto se hace con la intención de significar la naturaleza grave del desafío, poner de manifiesto la posibilidad de generar efectos cinéticos usando medios no militares y, en tercer lugar, resaltar la distinta forma de entender la guerra y la política entre los Estados:

> "The use of the term 'warfare' in this handbook is simply intended to signify the serious, adversarial, hostile and enduring nature of the challenge. It also denotes the ability of a hybrid aggressor to create warlike effects and outcomes (such as disrupting critical infrastructure or even territorial expansion) by 'weaponizing' non-military means, and the possibility that hybrid warfare may be employed to set the conditions to make future conventional aggression more effective. More broadly, it also suggests competitors and adversaries may take a less restricted view of what constitutes 'warfare' and the ways and means deployed to achieve political goals"[1109] (MONAGHAN & et al., 2019, pág. 17).

Por ello conviene aclarar, en línea con lo que advierte Jordán, uno de los autores del citado informe, que "llamar metafóricamente Hybrid Warfare a algo que no es guerra y que encaja mejor en el concepto de Zona Gris acaba generando confusión" (JORDÁN ENAMORADO, 2019). Como señala Jordán, se trata de una cuestión terminológica arrastrada desde el anterior informe de la MCDC, de 2017, titulado *Understanding Hybrid Warfare*[1110], en el que no participó ningún autor español. En este mismo sentido, Carment y Belo advierten que ZG y *guerra híbrida* no son sinónimos:

> "[…] we distinguish between the strategic goals of grey-zone conflict and the tactical operations of hybrid warfare. The two are not synonymous. Unlike hybrid warfare, grey-zone conflict participants rely on unconventional tactics that do not cross the threshold of formalized state-level aggression. Put another way, hybrid warfare can be a tactical subset of grey-zone conflict deployed under certain conditions and in varying degrees"[1111] (CARMENT & BELO, 2018, pág. 2).

[1108] "La guerra híbrida es el uso sincronizado de múltiples instrumentos de poder adaptados a vulnerabilidades específicas en todo el espectro de funciones sociales para lograr efectos sinérgicos. El desafío que representan los actores revisionistas que explotan la guerra híbrida tiene un amplio impacto en todas las sociedades, los gobiernos nacionales y las instituciones multinacionales" (Traducción propia).

[1109] "El uso del término *guerra* en este manual simplemente tiene la intención de significar la naturaleza seria, adversaria, hostil y duradera del desafío. También denota la capacidad de un agresor híbrido para crear efectos y resultados bélicos (como la interrupción de la infraestructura crítica o incluso la expansión territorial) mediante la *militarización* de medios no militares, y la posibilidad de que la guerra híbrida pueda emplearse para establecer las condiciones para hacer que la agresión convencional futura sea más efectiva. En términos generales, también sugiere que los competidores y adversarios pueden tener una visión menos restringida de lo que constituye una *guerra* y de las formas y medios desplegados para lograr objetivos políticos" (Traducción propia).

[1110] MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. January 2017. Disponible en:https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf (02/05/2024).

[1111] "Distinguimos entre los objetivos estratégicos del conflicto de la Zona Gris y las operaciones tácticas de la guerra híbrida. Los dos no son sinónimos. A diferencia de la guerra híbrida, los participantes en los conflictos de la Zona Gris dependen de tácticas no convencionales que no cruzan el umbral de una

Ediciones Universidad de Salamanca | CC BY-NC-ND

También se pronuncia al respecto la nota conceptual *El papel de las FAS en la Zona Gris (ZG) – (NCZG)*, del Estado Mayor de la Defensa (EMAD), que considera que, siendo conceptos que definen realidades vinculadas, su alcance es distinto:

> "La ZG se encuentra íntimamente ligada a otros conceptos de uso habitual en el vocabulario estratégico contemporáneo, como el que se refiere al "modo híbrido de hacer la guerra" (*hybrid warfare*), traducido habitualmente como "guerra híbrida", o el de "amenaza híbrida" (*hybrid threat*), muy relacionado con el anterior, en un intento de aumentar su alcance, desde el ámbito de lo estrictamente militar y de la Defensa, al más amplio de la Seguridad"[1112].

Por ello, siguiendo la doctrina mayoritaria, nosotros nos referiremos a la ZG como el espacio de competencia en el que operan las estrategias híbridas, acciones de manipulación encubierta con fines desestabilizadores y hostiles, que materializan la amenaza en dicho entorno por parte de un agresor que trata de pasar desapercibido en su ataque.

Aclarada la cuestión, recurrimos de nuevo a Jordán para aproximarnos a una definición de ZG en la que se incide en su disposición como espacio equidistante entre la política convencional y el conflicto armado donde, al menos por parte de uno de los actores, no hay conformidad con el orden establecido:

> "La zona gris es un espacio intermedio en el espectro de conflicto político que separa la competición acorde con las pautas convencionales de hacer política, del enfrentamiento armado directo y continuado. El conflicto en la zona gris gira en torno a una incompatibilidad relevante para al menos uno de los actores. Las estrategias utilizadas son multidimensionales, de implementación gradual y con objetivos a largo plazo" (JORDÁN ENAMORADO, 2018, pág. 133).

Para Baqués, en total desacuerdo con la visión de Cicerón reflejada en la máxima *inter pacem et bellum nihil est medium*[1113], la ZG se entiende como amenaza, estrategia o conflicto híbrido entre Estados por debajo del umbral de la guerra:

> "La zona gris es un tipo de amenaza, estrategia o conflicto híbrido, generada por actores moderadamente revisionistas (normalmente Estados) cuando persiguen fines similares a los de una guerra (pero evitando que llegue a estallar), amparándose en la ambigüedad de sus acciones (o empleando proxies), contando para ello con la difusión de una narrativa orientada a la movilización de civiles y la guerrilla económica, así como con el apoyo de las fuerzas armadas en aras a estimular o reforzar esas movilizaciones (inteligencia y operaciones especiales) y para disuadir a los defensores del status quo de intervenir contra la misma (fuerzas regulares)" (BAQUÉS QUESADA, 2021, pág. 173).

---

agresión formalizada a nivel estatal. Dicho de otra manera, la guerra híbrida puede ser un subconjunto táctico de un conflicto de Zona Gris desplegado bajo ciertas condiciones y en diversos grados" (Traducción propia).

[1112] Nota Conceptual *El papel de las FAS en la zona gris (ZG) – (NCZG)*. Centro Conjunto de Desarrollo de Conceptos del Estado Mayor de la Defensa. 14 de marzo de 2022. Página 1.

[1113] "Entre la paz y la guerra nada hay en el medio" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Un enfoque sistémico y centrado en la naturaleza híbrida de la amenaza en la ZG es el que presenta el informe *Campaigning in the Grey Zone. Towards a Systems Approach to Countering Hybrid Threats*[1114], que interpreta la competición en la ZG como parte de un sistema complejo y adaptativo, esencial para la estrategia de seguridad y defensa del Estado, en el que las amenazas híbridas requieren un tratamiento integral por cuanto:

> "Hybrid threats combine modern tools of statecraft to seek gains while avoiding reprisal. Trends in power, interdependence and technology suggest more motivated revisionist actors will exploit new levers across the full spectrum of moder domestic and international life. If such revisionist remain incentivized by deterrence, entanglement and norms to keep aggression short of war, hybrid challenges will proliferate"[1115] (MONAGHAN & McDONALD, 2023, pág. 2).

Finalmente, por la claridad y sencillez de exposición, nos parece muy apropiado el significado de ZG que ofrece el Centro Conjunto de Desarrollo de Conceptos del EMAD, en su nota conceptual de 2022, titulada *El papel de las FAS en la Zona Gris (ZG) – (NCZG):*

> "El término Zona Gris (ZG) se refiere a "la zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre Estados (*bona fide*) que pese a alterar notablemente la paz no cruzan los umbrales que permitirían o exigirían una respuesta armada. En este tipo de conflictos, a pesar de desarrollarse en tiempo de Paz, las FAS juegan un papel determinante, aunque complementario en el marco de la actuación global del Estado"[1116].

En todo caso, y volviendo a lo que ya señalábamos al inicio de este capítulo, debemos estudiar la actuación de los Estados en la ZG como un recurso más para arbitrar la consecución de sus objetivos en el plano internacional, que trasciende el marco temporal contemporáneo:

> "Se ha venido operando en esta región del espectro de los conflictos desde hace mucho tiempo y, de hecho, fue en la Guerra Fría cuando este tipo de enfrentamientos alcanzaron su apogeo como consecuencia de las dinámicas propias de la política de bloques y el efecto paralizador de las armas nucleares, factores que obligaban a utilizar vías alternativas a través de las cuales canalizar la competición entre superpotencias sin provocar con ello una escalada de consecuencias potencialmente devastadoras" (VILLANUEVA LÓPEZ, 2019).

[1114] Campaigning in the Grey Zone. Towards a Systems Approach to Countering Hybrid Threats. The Hague Centre for Strategic Studies. Octubre 2023. Disponible en: https://hcss.nl/report/campaigning-grey-zone-towards-systems-approach-countering-hybrid-threats/ (30/04/2024).

[1115] "Las amenazas híbridas combinan herramientas modernas del arte de gobernar para buscar ganancias y evitar represalias. Las tendencias en el poder, la interdependencia y la tecnología sugieren que los actores revisionistas más motivados explotarán nuevas formas en todo el abanico que ofrece la vida moderna nacional e internacional. Si dichos estados revisionistas continúan incentivados por la disuasión, la confusión y las normas para evitar que la agresión llegue a la guerra, proliferarán los desafíos híbridos" (Traducción propia).

[1116] Nota Conceptual *El papel de las FAS en la zona gris (ZG) – (NCZG)*. Centro Conjunto de Desarrollo de Conceptos del Estado Mayor de la Defensa. 14 de marzo de 2022. Página 1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

6.1.2. Actores, escalada y estrategias en la Zona Gris

Son principalmente los actores estatales quienes, mediante el uso de todos los instrumentos de poder a su alcance para confrontar al rival, aprovechan el terreno de conflicto solapado que ofrece la ZG para tratar de optimizar su estatus a costa del desgate de los rivales, sin llegar a provocar una respuesta armada. Por ello, son las potencias iliberales revisionistas las que mejor compensan la amenaza en la ZG por cuanto:

> "[…] aspiran a modificar el orden internacional, y a garantizar su propia seguridad interna, ya que sienten dicho orden como una amenaza para la supervivencia de su régimen político, pues aquel propugna principios como la democracia, el Estado de derecho o la libertad individual, los cuales cuestionan las bases de sus regímenes. Estos regímenes necesitarán, por un lado crear nuevos muros (físicos, digitales, informativos, económicos, diplomáticos) que los aíslen política y socialmente de la influencia y el atractivo de la fórmula política democrática; y por otro, reaccionar contra la fuerza expansiva del orden democrático en el ámbito internacional" (VILLENA SÁNCHEZ & AZNAR FERNÁNDEZ MONTESINOS, 2022, pág. 22).

Conviene sin embargo recordar lo dicho en el capítulo anterior[1117] en cuanto a la distinta forma de entender cada Estado, condicionado por su propia cultura o sensibilidad política, los entornos en los que opera la *confrontación informativa* o, en este caso, la amenaza híbrida. Mientras Occidente trata de superar con el bosquejo de la ZG la perspectiva binaria de Clausewitz, en la que los Estados se encuentran en situación de guerra o de paz[1118], sin áreas intermedias, otros competidores sistémicos entienden la ecuación de distinta forma (MARTÍNEZ VALERA, 2021).

En el caso de Rusia, su estrategia de operaciones híbridas se basa en tres pilares: el pilar de la *población*, a la que se dirige la propaganda -público interno- y la desinformación -público externo-; el pilar de la *acción*, conformado por el conjunto de medidas aplicadas para desgastar al adversario aprovechando sus debilidades -corrupción de instituciones, presión económica, coacción energética, fomento de la subversión, etc-; y el pilar de la *maskirovka*[1119], para desconcertar al rival de manera que no pueda interpretar las acciones que se están desarrollando contra él y no sepa ver lo que realmente está aconteciendo (CALVO ALBERO, 2022). De este modo, Rusia integra de manera proactiva en su forma de relacionarse con el resto de actores internacionales la *confrontación informativa* para, continuamente, tratar de sacar ventaja y mejorar su posición relativa frente a sus adversarios. En esta línea, en 2013 el General ruso Valery Gerasimov ya concluía que:

> "La guerra de la información abre amplias posibilidades asimétricas para reducir el potencial de combate del enemigo. En el norte de África hemos sido testigos de

[1117] Epígrafe 5.1.3. Ucrania: ¿guerra o ciberguerra?

[1118] Para Clausewitz, recordemos, la guerra es una extensión de la política y, por ello, tanto la política como la lucha por el poder son parte de la guerra, de forma que los Estados o están en guerra o están en paz.

[1119] Engaño, farol, ocultación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> la implantación de tecnologías de influencia sobre las estructuras estatales y la población con la ayuda de las redes de información. Es necesario mejorar las acciones en el espacio de la información, incluida la defensa de nuestras propias instalaciones" (GERASIMOV, 2013).

Para China, por su parte, la competencia por debajo del umbral de la guerra también representa su *modus operandi* habitual, por cuanto los límites del conflicto se amplían para dar cabida al uso de todos los medios disponibles por el Estado, de cualquier naturaleza y condición, incluidas las fuerzas armadas, para doblegar al rival ante sus intereses (GARCÍA CANTALAPIEDRA, 2023, pág. 69). Su sistema político autoritario dirige esta línea de acción en la ZG bajo tres premisas:

1. Un *planeamiento centralizado*, que se acompaña de una escrupulosa ejecución coordinada a través de la que se despliegan todas las capacidades ofrecidas por el propio Estado, la sociedad civil, el sector privado, las organizaciones no gubernamentales e, incluso, las alianzas internacionales.
2. La interpretación posesiva y excluyente del *dominio de la información* en cuanto a la capacidad de recopilar, tratar, analizar y explotar la información y, además, negársela al adversario (MARTÍNEZ VALERA, 2021).
3. Y la extrema habilidad para endosar al rival la *carga de la escalada en la ZG*, de manera que si se trata de Estados con capacidad de respuesta, les coloca ante el dilema de aceptar los hechos consumados -perjudicando así su posición-, o responder iniciando un conflicto -lo que hará que sea visto como agresor al utilizar la violencia frente a una acción no cinética por parte de China-. En el caso de Estados sin capacidad militar efectiva, las acciones chinas en ZG quedarán mayormente sin respuesta, pues estos son conscientes de que plantar cara a Pekín escalaría el conflicto, conllevando un coste que no pueden asumir (VILLANUEVA LÓPEZ, 2019).

Por consiguiente, podemos decir que, al igual que Rusia, China integra en su política internacional, de manera habitual y sin restricciones, el uso de todos los recursos a su alcance para ganar en el enfrentamiento en ZG a sus contendientes[1120].

Visto ya que el conflicto en ZG suele acontecer principalmente entre Estados, que se desenvuelven en ella de distinta manera conforme a cómo la interpretan e integran en su política de relaciones internacionales, debemos decir que ello no es óbice para que puedan concurrir otros actores no estatales que, con distintas formas y nivel de implicación, actúen por delegación frente al adversario señalado por el Estado que los ampara. Son estos los conocidos como *proxies*[1121], cuya virtualidad es diferir el enfrentamiento directo entre ambos Estados competidores.

[1120] En este sentido, en mayo de 2024 se detecta un grupo de ciberespionaje vinculado a China, conocido como Mustang Panda, centrado en varias de las compañías navieras de transporte marítimo comercial con sede en Noruega, Grecia y Países Bajos. Disponible en: https://www.escudodigital.com/ciberseguridad/china-malware-espiar-envios-comerciales-barcos_59045_102.html (19/05/2024).

[1121] El diccionario de la Real Academia Española no recoge este anglicismo, por lo que recurrimos al diccionario inglés Britannica que, en su página web, ofrece dos acepciones del término *proxy*: "1 (count): a person who is given the power or authority to do something (such as to vote) for someone else; 2 (noncount): power or authority that is given to allow a person to act for someone else — usually used in

Ediciones Universidad de Salamanca | CC BY-NC-ND

La gradación del compromiso del *proxy* varía en atención a los intereses compartidos con su mentor -ideológicos, políticos, económicos, tácticos, etc.-, pudiendo señalar como ejemplos los grupos insurgentes o bandas terroristas como Hezbollah, elemento clave para la estrategia disuasora de Irán frente a Israel (BAQUÉS QUESADA, 2021, págs. 138-143); el uso de ejércitos de mercenarios como el Grupo Wagner para consolidar pretendidas acciones humanitarias, de seguridad y apoyo a la población que, verdaderamente, sustentan la penetración rusa en el Sahel frente a los intereses estratégicos europeos en la zona[1122]; o el empleo de grupos hacktivistas como NoName057(16) para atacar la infraestructura electoral del Estado español durante las elecciones generales de julio de 2023[1123].

También pueden operar como *proxy* todo tipo de organizaciones civiles y no gubernamentales, en el papel de multiplicadores de efectos de aquellas medidas de perfil económico, mediático, político o cultural, que formen parte de la estrategia híbrida definida por el Estado actor para alcanzar, a largo plazo, los objetivos buscados frente al Estado rival. Claro ejemplo de esto es la línea de actuación de la cadena de televisión internacional *Russia Today* (RT), señalada en la UE como medio de propaganda del Kremlin, tal y como quedó patente en la sentencia del Tribunal General de la Unión de 27 de julio de 2022[1124], o la red de desinformación pro-Kremlin denominada *Portal Kombat*[1125], desenmascarada en febrero de 2024 por el servicio

---

the phrase *by proxy*". De esta manera, en la primera entrada (contable) se define como una persona a la que se le da el poder o la autoridad para hacer algo -como votar- por otra persona, y en la segunda (incontable) como poder o autoridad que se otorga para permitir que una persona actúe en nombre de otra, y generalmente se usa en la frase *por poder* (Traducción propia). Disponible en: https://www.britannica.com/dictionary/proxy (20/05/2024).

[1122] El Kremlin ha reconfigurado el grupo paramilitar Wagner a partir de la muerte en 2023 de su díscolo líder, Yevgeny Prigozhin, pasando a considerarlo *Cuerpos Expedicionarios*. A través de estos grupos de mercenarios Rusia ofrece formación militar a los oficiales de los ejércitos de Mali, Níger y Chad, así como respaldo a los regímenes políticos que los gobiernan, a cambio del acceso a recursos naturales -madera, oro, uranio, litio- y la consecuente capacidad de influencia política. Disponible en: https://www.bbc.com/mundo/articles/c514zz52gwvo (03/05/2024).

[1123] El grupo hacktivista prorruso NoName057(16) llevó a cabo una serie de ciberataques contra diversas instituciones españolas vinculadas con la seguridad y transparencia del proceso de elecciones generales de 2023, incidiendo especialmente en la jornada del 23 de julio en la propia página web del Ministerio del Interior, responsable de la seguridad del proceso. Disponible en: https://www.elconfidencial.com/espana/2023-07-23/elecciones-23j-hackers-prorrusos-atacan-interior-votacion_3706141/ (03/05/2024).

[1124] Sentencia del Tribunal General de 27 de julio de 2022 — RT France/Consejo (Asunto T-125/22) [«Política exterior y de seguridad común — Medidas restrictivas motivadas por acciones de Rusia que desestabilizan la situación de Ucrania — Prohibición temporal de emisión y suspensión de autorizaciones de radiodifusión respecto de los contenidos de determinados medios de comunicación — Inclusión en la lista de entidades a las que se aplican medidas restrictivas — Competencia del Consejo — Derecho de defensa — Derecho a ser oído — Libertad de expresión e información — Proporcionalidad — Libertad de empresa — Principio de no discriminación por razón de nacionalidad»]. DOUE C 340/40, de 5.9.2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022TA0125 (03/05/2024).

[1125] Este ecosistema de desinformación del Kremlin busca amplificar el alcance mediático de las piezas de información que, en cada momento y conforme a las peculiaridades del destinatario, se consideren necesarias para apoyar las narrativas rusas, tanto para favorecer su propia línea de acción política, como para desprestigiar a los Estados occidentales y sus instituciones democráticas. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

francés Viginum[1126], dedicada a amplificar masivamente fuentes de propaganda rusas en Europa y EE.UU.

En cuanto a los fines perseguidos en la ZG, serán estos de alta relevancia estratégica para el Estado actor y, por ello, los beneficios esperados a largo plazo deben superar los costes de adentrarse en ese camino ambiguo, de procedimientos no convencionales y *pseudopacíficos*, que busca explotar al máximo las vulnerabilidades específicas del rival para incrementar el poder relativo del agresor frente a aquel (JORDÁN ENAMORADO, 2018, pág. 137). Por esta razón, la clave será encontrar el equilibrio entre los fines pretendidos y los medios empleados que, en todo caso, conforme a lo dicho en el primer epígrafe respecto al componente híbrido y asimétrico, supondrá el empleo coordinado, integral y simultáneo de todos los instrumentos de poder multidimensionales al alcance del Estado -diplomáticos, informacionales, militares, económicos-.

Como venimos señalando, este escenario de ZG es especialmente ventajoso para Estados con objetivos revisionistas y estructuras de gobierno autocráticas, que buscan por encima de todo su perpetuación en el poder y, junto a esto, la reordenación a su favor del *statu quo* geopolítico -regional o internacional- para aumentar su *cuota de poder relativo*, esto es, desplegar más poder que sus rivales para configurar el entorno de manera más favorable a sus intereses (JORDÁN ENAMORADO, 2020). Dicha ganancia puede representar un fin en sí misma[1127] o ser el prólogo de un conflicto armado, puesto que conforme el agresor vaya acumulando poder irá adaptando su estrategia que, en un momento determinado, puede llevarle a considerar que una agresión convencional le resulta más beneficiosa para alcanzar sus propósitos[1128]. No obstante, el conflicto

https://www.rfi.fr/es/europa/20240213-portal-kombat-francia-revela-una-red-que-difunde-propaganda-rusa-en-europa-y-ee-uu
https://euvsdisinfo.eu/es/las-manipulaciones-del-kremlin-a-nivel-mundial/ (03/05/2024).

[1126] Viginum es el Servicio de Vigilancia y Protección Contra las Injerencias Digitales Extranjeras, dependiente de la Secretaría General de Defensa y de la Seguridad Nacional del gobierno francés. Se trata de un servicio técnico y operativo de naturaleza judicial (no es un servicio de inteligencia) que fue creado el 14 de julio de 2021 por el Decreto 2021-922, de 13 de julio. Disponible en: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361 (04/05/2024).
Viginum es el responsable de la vigilancia y detección de las injerencias digitales extranjeras, debiendo identificar aquellas operaciones que impliquen, de manera directa o indirecta, a un Estado o a un organismo no estatal extranjero, que tengan por objetivo la difusión, masiva y deliberada, por medio de un servicio de comunicación público en línea, de alegaciones o imputaciones de hechos manifiestamente inexactos o falsos, de tal modo que potencialmente puedan afectar a los intereses fundamentales de Francia. Su objetivo como proyecto de inteligencia estratégica es, básicamente, demostrar a partir del trabajo en fuentes abiertas, que determinadas noticias, narrativas o relatos compartidos y difundidos por los ciudadanos franceses pueden basarse en informaciones interesadas creadas por terceros países con el fin de inducirles a error y provocar un estado de opinión que perturbe la libre formación de criterio y, con ello, afectar al debate democrático y pacífico. Es importante señalar que Viginum trabaja únicamente en la detección e identificación de la amenaza desinformativa, pero no participa en la respuesta que desde el ámbito político se determine para la misma.

[1127] Por ejemplo, para Rusia impedir que Moldavia y Albania ingresen en la UE.

[1128] Por ejemplo, la estrategia que, a todas vistas, parece haber seguido Rusia con Ucrania desde la invasión y anexión unilateral de Crimea en 2014 que, finalmente, ha devenido en la guerra iniciada el 24 de febrero de 2022. Este paso de la ZG a la confrontación armada se escenificó a través de las maniobras militares ZAPAD 21, iniciadas en septiembre de 2021 y que se mantuvieron en la frontera de Bielorrusia con Ucrania para, meses después, favorecer la invasión. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

armado también puede estallar como respuesta del Estado agredido, pues el control de la escalada se convierte en cuestión delicada en la ZG por la sucesión de altibajos en la intensidad de las acciones de confrontación.

Por esta razón, la configuración y el control de la escalada merece ser estudiada como pieza determinante de la estrategia híbrida aplicada por los competidores para alcanzar sus objetivos en la ZG. La clave en el desarrollo de esta estrategia será el gradualismo en la implementación de las herramientas e instrumentos de poder que, utilizados de manera simultánea y aprovechando las vulnerabilidades del agredido, permitan llegar a su desestabilización y desgaste interno. Para ello seguiremos la propuesta teórica del profesor Jordán[1129], que distingue cuatro niveles de intensidad de estas acciones híbridas orientadas a degradar el proceso de toma de decisiones del oponente, tal y como se representa en el gráfico 6.1.



Gráfico 6.1.
Fuente: Javier Jordán, 2020

El primero de ellos es el de *configuración del entorno*, nivel inferior de la escalada y, a la vez, el más ambiguo por su proximidad al ámbito de la competencia pacífica entre Estados conforme a los parámetros comúnmente aceptados en la política internacional. El agresor comienza en esta fase a traspasar con sus acciones -en modo alguno inocentes

https://es.euronews.com/2022/02/20/rusia-y-bielorrusia-prolongan-sus-maniobras-a-las-puertas-de-ucrania
https://informnapalm.org/es/comienzo-de-las-maniobras-oeste-2021-y-el-traslado-de-los-cazas-rusos-su-30sm-a-belarus/ (04/05/2024).

[1129] El marco teórico sobre el que el Profesor Jordán estructura su análisis de los niveles de escalada en el conflicto en la Zona Gris, que va a guiar nuestro estudio, es también seguido por el modelo que define la nota conceptual *El papel de las FAS en la Zona Gris*, del Centro Conjunto de Desarrollo de Conceptos, del EMAD, de marzo de 2022.

Ediciones Universidad de Salamanca | CC BY-NC-ND

e inofensivas- las líneas de lo que se considera aceptable en las relaciones normales entre Estados. La baja intensidad de los actos y el reducido alcance de sus efectos los camuflan y los hacen muy difíciles de identificar como amenaza por parte del adversario atacado, cuyo umbral de respuesta no se inmuta -es la conocida como *salami tactics*-. Sin embargo, su poder destructivo radica en la persistencia en el tiempo "que genera efectos acumulativos y prepara el terreno a acciones decisivas en una escalada posterior" (JORDÁN ENAMORADO, 2020).

En esta etapa cobra especial sentido para el agresor la elaboración de narrativas que, por un lado, a través de la propaganda, doten internamente de sentido a su maniobra y sirvan para cohesionar a la población y, por otro, mediante la desinformación, deslegitimen institucionalmente y deterioren la cohesión social del Estado adversario, generando polarización[1130] y crispación política que acaben sacando al debate público cuestiones domésticas que favorezcan al atacante[1131]. También son relevantes en este nivel el fomento de la corrupción de funcionarios públicos[1132], la diplomacia asertiva[1133],

[1130] Como muestra de la construcción de narrativas que aprovechan las divisiones internas del Estado agredido podemos mencionar la operación de influencia iraní que, durante tres años, a través de IA generativa y redes sociales, gestionó una red de comportamiento inauténtico coordinado para influir en la sociedad israelí y, de esta forma, sembrar la desconfianza en su gobierno utilizando a las comunidades ortodoxa y LGBTQ+, el discurso político de la izquierda y la derecha, o la guerra de Israel contra Hamás. Disponible en: https://www.darkreading.com/threat-intelligence/three-year-iranian-influence-op-preys-divides-israeli-society (09/05/2024).

[1131] Ejemplo de ello es la gestión de la ayuda económica y el envío de armas a Ucrania para enfrentar al ejército ruso, o la expansión de la OTAN y la UE hacia los antiguos países del Telón de Acero, ambas cuestiones manejadas por el Kremlin para alimentar su narrativa victimista frente a Occidente, a través de la cual presenta la invasión de Ucrania como una respuesta de defensa e, incluso, de supervivencia. Disponible en: https://actualidad.rt.com/actualidad/422597-expertos-culpan-expansion-otan-conflicto (08/05/2024).

[1132] En este sentido podemos citar el caso de diputados del Parlamento Europeo investigados por blanqueo de capitales, corrupción y participación en organización delictiva, en base a supuestas transferencias de información y actuaciones que beneficiaban a Qatar. Puede consultarse la Resolución del Parlamento Europeo, de 15 de diciembre de 2022, sobre las sospechas de corrupción en relación con Qatar y la necesidad de aumentar la transparencia y la rendición de cuentas en las instituciones europeas (2022/3012(RSP)), así como su seguimiento en prensa. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0448_ES.html
https://elpais.com/internacional/2023-03-06/qatargate-la-defensora-del-pueblo-europea-pide-explicaciones-por-los-viajes-pagados-por-qatar-a-un-alto-funcionario-de-la-comision.html
https://valenciaplaza.com/qatargate-salpica-corrupcion-gobierno-union-europea (04/05/2024).
Posteriormente, otros eurodiputados alemanes fueron acusados de espiar para los servicios secretos chinos. Disponible en: https://elpais.com/internacional/2024-04-23/detenido-en-alemania-el-asistente-de-un-eurodiputado-del-partido-ultra-afd-por-espiar-para-china.html
https://es.euronews.com/my-europe/2024/04/23/tras-el-rusiagate-los-eurodiputados-se-apresuran-a-denunciar-el-emergente-chinagate (04/05/2024).

[1133] El envío de mensajes derivados de la retirada o *llamamiento a consultas* de un embajador es algo usual en el marco de las relaciones diplomáticas entre Estados pero, también es cierto, normalmente supone una reacción inmediata a un determinado acto de política internacional por lo que, sumado al resto de movimientos sincronizados, conlleva un desgaste interno para el adversario. En el caso de la relación entre España y Marruecos esta situación se produjo cuando, con ocasión de la pandemia del COVID 19, se aceptó a finales de abril de 2021 el ingreso en un hospital de Logroño del líder del Frente Polisario, Brahim Ghali. Posteriormente, y a consecuencia de ello, entre el 17 y el 18 de mayo Marruecos llamó a consultas a su embajadora en Madrid y, al mismo tiempo, relajó el control de sus fronteras con Ceuta para que cerca de 8.000 migrantes saltaran la valla de la ciudad autónoma española, en una crisis

Ediciones Universidad de Salamanca | CC BY-NC-ND

la exfiltración de datos de servidores públicos o altos cargos[1134], las campañas de daños informáticos a la población a gran escala[1135] y, finalmente, la creación de dinámicas de *lawfare*[1136] sobre las que construir un relato que, desde la interpretación parcial e interesada de la norma jurídica -nacional o internacional-, legitime ante la opinión pública la reivindicación[1137] del agresor en la ZG (BAQUÉS QUESADA, 2021, págs. 148-149).

La segunda fase del nivel de agresividad de las estrategias híbridas es la de *interferencia*, en la que ya comienza a ser patente que existe una instrumentalización de la ZG para administrar el conflicto. Ello obliga al Estado agresor a enmascarar sus acciones para que no sean tan evidentes y tratar de dificultar la atribución, la disuasión y la respuesta del rival (JORDÁN ENAMORADO, 2020). En este estadio las estrategias híbridas puestas en marcha por el agresor para desestabilizar y perjudicar a su adversario ya son sensiblemente más intrusivas y decididas, a través de campañas de injerencia para afectar a procesos electorales[1138], o de apoyo encubierto a conflictos internos -

sin precedente. Disponible en: https://www.europapress.es/nacional/noticia-marruecos-llama-consultas-embajadora-madrid-20210518182948.html
https://elpais.com/espana/2021-05-18/espana-convoca-a-la-embajadora-de-marruecos.html
https://www.elsaltodiario.com/control-fronteras/acuerdo-ue-pesca-externalizacion-fronteras-que-hay-detras-ultima-crisis-migratoria-marruecos-ceuta
https://elpais.com/espana/2021-05-18/el-ejercito-se-despliega-para-controlar-las-calles-de-ceuta-tras-la-entrada-de-5000-inmigrantes.html
https://elpais.com/espana/2021-05-19/que-esta-pasando-en-ceuta-claves-de-la-crisis-entre-espana-y-marruecos.html (04/05/2024).

[1134] China aparece como la principal sospechosa de una gran exfiltración de información personal y confidencial de personal militar de UK, entre los que se hallarían datos relacionados con las nóminas y el procedimiento de pago, vulnerabilidad que abriría la puerta a posteriores actos de chantaje a las personas afectadas. Disponible en: https://osintcorp.net/china-suspected-after-major-mod-payroll-breach/ (07/05/2024).

[1135] En mayo de 2024 las instituciones públicas polacas son objetivo de una campaña de malware a gran escala coordinada por el actor estatal APT28, vinculado a Rusia, mediante el envío de correos electrónicos que buscaban despertar el interés del destinatario para incitarlo a hacer clic en el enlace, el cual redirigía a un sitio web donde se accedía a los datos del usuario. Disponible en: https://thehackernews.com/2024/05/kremlin-backed-apt28-targets-polish.html (11/05/2024).

[1136] Sobre el término *lawfare,* neologismo que proviene de *law* (ley, derecho) y *warfare* (guerra) decir que, básicamente, hace referencia a un método de guerra no convencional en el que la ley se utiliza como medio para alcanzar objetivos militares que ayuden a vencer al enemigo. Puede consultarse al respecto el documento Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts. Colonel Charles J. Dunlap, Jr., USAF. Noviembre de 2021. Disponible en: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=6193&context=faculty_scholarship (16/11/2024).

[1137] Esta reivindicación, que el agresor presenta a la comunidad internacional sobre una base de presunta legalidad, puede ser la reclamación de un territorio al Estado agredido, la revisión de un tratado que les vincula y que ahora ya no interesa cumplir, la subsanación de algún tipo de agravio pasado -real o imaginario- o, simplemente, la reparación de una ofensa producida en sus relaciones ordinarias. En todo caso, el agresor trata de legitimar su reivindicación ante la comunidad internacional y el público objetivo mediante la construcción de su propia narrativa, que difunde a través de la adecuada propaganda.

[1138] Los servicios de inteligencia belgas confirman en abril de 2024 la existencia de una red de injerencia prorrusa en varios Estados europeos, incluida Bélgica, con pagos a eurodiputados de diversas nacionalidades, de cara a las elecciones europeas del 9 de junio de ese año. Disponible en: https://elpais.com/internacional/elecciones-europeas/2024-04-12/belgica-investiga-un-caso-de-injerencia-rusa-en-las-elecciones-europeas.html

Ediciones Universidad de Salamanca | CC BY-NC-ND

ideológicos, territoriales, identitarios-[1139], las operaciones encubiertas y sabotajes realizados por servicios de inteligencia[1140] o a través de terceros[1141], el apoyo encubierto a movimientos migratorios dirigidos[1142], los ciberataques intimidatorios contra infraestructuras críticas o servicios esenciales[1143], la coerción económica para condicionar la acción exterior del otro Estado o las demostraciones de fuerza en el contexto de tensión previa generada[1144].

https://www.larazon.es/internacional/injerencia-rusa-cierne-elecciones-europeas-mes-junio_20240429662ee3d28e66020001bd6533.html (04/05/2024).

[1139] Un ejemplo es la demostrada vinculación entre Rusia y el nacionalismo independentista catalán, con amplia repercusión y seguimiento en prensa. Disponible en: https://www.elmundo.es/cataluna/2021/11/09/61896962e4d4d840138b458a.html https://www.elmundo.es/cataluna/2024/02/08/65c5394221efa07f538b45a9.html https://www.infobae.com/america/agencias/2024/01/29/un-juez-en-espana-advierte-que-rusia-estaba-dispuesta-a-apoyar-al-independentismo-catalan/ (04/05/2024).

[1140] En mayo de 2024 el grupo de hackers patrocinado por el Estado iraní conocido como APT42 se hace pasar por conocidos medios de comunicación –The Washington Post, The Economist- y think tanks para atacar a periodistas, investigadores y activistas de países occidentales y Oriente Medio, redirigiéndoles a enlaces maliciosos y, posteriormente, tener acceso a las redes sociales de la víctima. Disponible en: https://news.hitb.org/content/iranian-state-backed-cyber-spies-continue-impersonate-media-brands-think-tanks (05/05/2024).

[1141] El 26 de septiembre de 2022 se producen varias explosiones que afectan a los gasoductos Nord Stream del mar Báltico, una infraestructura energética crítica para el abastecimiento a Alemania en un contexto marcado por la guerra de Ucrania, y con Europa decidiendo la aplicación de sanciones económicas al Kremlin mientras trata de gestionar su elevada dependencia del gas ruso. Para la comunidad internacional la principal sospechosa es Rusia que, lógicamente, niega su participación en el sabotaje y culpa a Occidente. Disponible en: https://elpais.com/internacional/2023-02-27/el-sabotaje-del-nord-stream-cinco-meses-de-sospechas-y-teorias-conspirativas.html (04/05/2024).

[1142] Un ejemplo de ello es la estrategia de presión por parte de Túnez -y Libia- hacia la UE para alcanzar acuerdos económicos ventajosos que se apoya, en gran medida, en la gestión de los flujos migratorios con destino a Lampedusa (Italia). Así, en septiembre de 2023 el presidente tunecino, Kais Said, niega la entrada al país de una delegación de la UE para la puesta en marcha de un acuerdo que fija la asistencia financiera europea de más de 1.000 millones de euros a Túnez a cambio de su ayuda en el control de la inmigración ilegal desde sus fronteras. Al mismo tiempo, el 12 de septiembre, 5.112 inmigrantes ilegales alcanzan la isla de Lampedusa en un aluvión de embarcaciones que se hacen a la mar desde el litoral tunecino, muchas de ellas remolcadas por pesqueros. Disponible en: https://elpais.com/internacional/2023-09-26/tunez-pone-en-entredicho-el-acuerdo-migratorio-con-la-ue-al-bloquear-otra-visita-europea-al-pais.html https://gaceta.es/europa/tunez-presiona-a-italia-con-mas-de-130-embarcaciones-en-un-solo-dia-que-dejan-en-lampedusa-a-mas-5-000-inmigrantes-ilegales-20230913-1559/ (04/05/2024).

[1143] En mayo de 2024 la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) y otros organismos nacionales e internacionales de ciberseguridad emiten un aviso alertando de que grupos hacktivistas rusos atacan cada vez más sistemas de tecnología operativa a pequeña escala en Norteamérica y Europa. Estos ataques, centrados principalmente en los sectores de sistemas de agua y aguas residuales, presas, energía y alimentación y agricultura, suponen amenazas significativas para las infraestructuras críticas occidentales. Disponible en: Russian Hackers Attacking Small-scale Infrastructure Sectors (gbhackers.com) (05/05/2024).

[1144] En marzo de 2024 las fuerzas navales de China, Rusia e Irán inician unas maniobras en el golfo de Omán, zona de alto interés estratégico por su conexión con el golfo Pérsico a través del estrecho de Ormuz, por donde transita la quinta parte del petróleo comercializado a nivel mundial y lugar de continuos enfrentamientos con los hutíes, que en apenas seis meses han atacado a más de media centena de buques en la zona. La cooperación militar entre los tres países se ha intensificado como respuesta a las crecientes tensiones con EE.UU. por el suministro, por parte de Irán a Rusia, de drones militares muy utilizados en la guerra de Ucrania, y por la vinculación de Irán con Hamás, a la que facilita misiles y otro material para su

Ediciones Universidad de Salamanca | CC BY-NC-ND

El tercer nivel de agresividad en la escalada es la *desestabilización*, que conlleva una intensificación de la estrategia híbrida que busca propiciar disfunciones graves en la estructura política, social y económica del adversario para ahondar en su inestabilidad y hacerlo más vulnerable a la coerción, en forma de sanciones económicas y bloqueos comerciales[1145], grandes movimientos de capital en Bolsa[1146], ciberataques coordinados de amplio alcance[1147], la degradación del espectro electromagnético[1148], el apoyo encubierto a grupos políticos antisistema, a movimientos sociales violentos o revolucionarios[1149] o, incluso, a milicias armadas y compañías privadas militares con control de territorio[1150]. Esta es la linde que marca el punto inmediatamente anterior al conflicto armado (JORDÁN ENAMORADO, 2020).

La cuarta y última fase del nivel de agresividad de las estrategias híbridas en la ZG es el *empleo directo, limitado y puntual de la fuerza*, momento de difícil equilibrio por cuanto los contendientes recurren al uso de la violencia para sostener acciones de hechos

guerra con Israel. Disponible en: https://es.euronews.com/2024/03/12/ejercicios-navales-conjuntos-de-china-iran-y-rusia-en-el-golfo-de-oman https://cnnespanol.cnn.com/2023/10/12/como-consigue-Hamás-armas-trax/#:~:text=No%20mencion%C3%B3%20ninguna%20participaci%C3%B3n%20exterior,nos%20da%20dinero%20y%20armas%22. (04/05/2024).

[1145] El más claro y reciente ejemplo de esta escalada del nivel de presión de la estrategia híbrida en la ZG, previa al conflicto armado, lo tenemos en las sanciones de la Unión Europea contra Rusia como consecuencia de la invasión de Ucrania, con el objetivo de disminuir la capacidad del Kremlin para financiar la guerra, imponer costes económicos y políticos a sus élites políticas, y dañar la base económica rusa con el bloqueo de movimientos de capital o la reducción de la dependencia energética europea del gas importado desde Rusia. Disponible en: https://eu-solidarity-ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine_es https://www.consilium.europa.eu/es/policies/sanctions-against-russia/ https://www.dw.com/es/la-ue-acuerda-nuevas-sanciones-a-rusia-con-motivo-de-los-dos-a%C3%B1os-de-guerra-en-ucrania/a-68314644 (04/05/2024).

[1146] El objetivo de estos movimientos en bolsa es conseguir la fluctuación de precios de las acciones de determinados grupos de empresas -tecnológicas, energéticas, de infraestructuras- como modo de chantaje económico para que el adversario ceda en su posición o, al contrario, se vea obligado a realizar determinado movimiento que, de otra manera, no llevaría a cabo. Es un ejemplo de ello el precio del crudo en los mercados internacionales y, a través de él, la cotización en bolsa de las empresas del sector.

[1147] Principalmente a través de ciberataques de denegación de servicios o de caída de sistemas de soporte de infraestructuras críticas y servicios esenciales -centrales de energía, hospitales, instituciones públicas- con el objetivo de dejar patente la debilidad del Estado agredido. Estos ciberataques también pueden estar enfocados a la recopilación de información sobre el rival, con la que posteriormente generar inteligencia que sea explotada operativamente en otras acciones híbridas complementarias.

[1148] Su finalidad principal es dificultar el normal funcionamiento de los servicios que sostienen la sociedad digital, tecnológica y ciberdependiente actual. El simple hecho de perturbar la señal de telefonía móvil en una gran ciudad puede generar pérdidas millonarias al día.

[1149] Estas acciones hostiles dan soporte a esos actores interpuestos -dinero, material, entrenamiento, cobertura- para que actúen por delegación a favor del agresor. Estos actores se convierten, de esta manera, en *proxies*.

[1150] Esta es la estrategia seguida por Rusia en mayo de 2014 cuando, con el apoyo de tropas rusas no identificadas -los famosos *hombrecillos de verde*-, da cobertura al proceso de autoproclamación de la República de Crimea. Disponible en: https://www.bbc.com/mundo/noticias/2014/03/140311_ucrania_rusia_soldados_crimea_jgc (04/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

consumados, pero, al mismo tiempo, tratan de no escalar al conflicto armado declarado y abierto[1151] (JORDÁN ENAMORADO, 2020).

Cabe destacar que, en este continuo que supone la ZG, el conflicto puede escalar o desescalar a voluntad de los actores quienes, de hecho, pueden decidir mantenerse de forma prolongada en alguna de las fases por considerar que esa es la estrategia que mejor favorece a sus intereses. Por ello, recordamos una vez más que la estrategia en ZG es una combinación sincronizada de instrumentos de poder con una visión a largo plazo, en la que los Estados autocráticos se mantienen más cómodamente que las democracias, por la propia conformación de los regímenes políticos que los sostienen y tienden a perpetuarse (BAQUÉS QUESADA, 2021, pág. 126).

Ante la realidad que constituye la ZG como escenario de confrontación entre Estados, donde *la naturaleza multidimensional e integrada de las amenazas híbridas* juega un papel protagonista, será preciso construir una estrategia de prevención, disuasión, detección y respuesta basada en un enfoque integral que, entre otras cuestiones, disponga de un sistema de indicadores y alertas que permita determinar, con un elevado porcentaje de fiabilidad, en qué nivel de escalada nos encontramos en un momento concreto, cuestión esencial para poder "trazar y comunicar líneas rojas que disuadan la futura manipulación de los umbrales de respuesta, que es precisamente una conducta habitual por parte del agresor en este tipo de conflicto" (JORDÁN ENAMORADO, 2020).

6.1.3. Disuasión y respuesta frente a la amenaza híbrida en la Zona Gris

Puesto que la ZG se instrumentaliza por los actores que en ella se instalan para alcanzar sus objetivos sin ser detectados, estrategia que en gran medida se basa en el control de la escalada, la respuesta que se construya para contrarrestarla debe dirigirse, por ello mismo, a recuperar dicho control (VILLANUEVA LÓPEZ, 2019). Esta lucha por recuperar la iniciativa en la escalada se va a desenvolver en el marco de los instrumentos de poder que el Estado maneja –militar, político, económico, social, comunicativo-, pero su implementación va a estar condicionada por una serie de cuestiones previas.

La primera de ellas se corresponde con *la dificultad de detección de la acción hostil y su atribución* como requisito previo de cualquier movimiento de respuesta. Delimitar los lindes entre la ZG y el conflicto armado es relativamente sencillo, no así distinguir las fronteras de aquella con la competencia pacífica en el marco de las relaciones convencionales entre Estados[1152]. La constatación de que, en un momento

[1151] Un ejemplo de esta escalada que amenaza con el salto inmediato al conflicto armado es el ataque de Irán a Israel del 13 de abril de 2024 como respuesta, en el contexto de la guerra entre Israel y Hamás, al bombardeo israelí unos días antes de un edificio consular en Damasco donde murieron siete altos mandos militares de la Guardia Revolucionaria iraní, entre los que se encontraba el general Mohammad Reza Zahedi, clave en las relaciones con Hezbolá, aliada de Hamás. La respuesta de Tel Aviv no se hizo esperar y, apenas una semana después, bombardeó varios enclaves cerca de la ciudad de Isfahán. Disponible en: https://es.euronews.com/2024/04/19/el-supuesto-ataque-israeli-a-iran-impacta-cerca-de-la-central-nuclear-de-isfahan
https://cnnespanol.cnn.com/2024/04/13/ataque-iran-israel-noticias-ultima-hora-orix/ (04/05/2024).

[1152] Un ejemplo de esta dificultad de identificación de la maniobra híbrida lo tenemos en la OPA lanzada en marzo de 2024 por el grupo empresarial húngaro Ganz-Mavag para la compra de la empresa ferroviaria

Ediciones Universidad de Salamanca | CC BY-NC-ND

determinado, ya se ha cruzado la línea y nos encontramos en ZG va a verse dificultada porque se tratará de una amenaza gestada bajo los umbrales de alerta, el adversario contará con la negación plausible de su autoría y, en múltiples ocasiones, se utilizarán *proxies* interpuestos que complican la identificación y, por consiguiente, la elaboración de una maniobra de réplica acorde (GUTIÉRREZ DE LEÓN, 2021).

La segunda de las cuestiones prioritarias para afrontar la amenaza en ZG es la definición de unos *objetivos estratégicos realistas y adaptados al contexto*, sobre los que asentar la decisión relativa a qué medidas disuasorias o de réplica adoptar una vez que haya sido identificado el ataque. El informe *Countering Hybrid Warfare* del MCDC señala tres objetivos estratégicos genéricos para contrarrestar la amenaza híbrida (MONAGHAN & et al., 2019, págs. 19-20):

1. *Mantener la capacidad de acción independiente y fortalecer la resiliencia* frente a este tipo de agresiones en ZG, identificando para ello nuestras vulnerabilidades y estableciendo un enfoque común y coordinado para abordarlas desde la cooperación público-privada, el compromiso de la sociedad civil y la concienciación a todos los niveles sobre la trascendencia de la amenaza híbrida y sus consecuencias para la democracia y las instituciones que la sustentan.
2. *Definir umbrales de respuesta para construir la barrera de disuasión*, teniendo en cuenta nuestros intereses y las posibles intenciones del adversario. En definitiva, se trata de establecer el nivel de hostilidad que estamos dispuestos a tolerar razonablemente, dado que una política de inmediata respuesta ante cualquier tipo de incidente híbrido que identifiquemos no es posible ni acertada.
3. *La firme y manifiesta voluntad de aplicar las medidas activas de respuesta* planificadas para impedir que el adversario siga adelante con la acción que nos perjudica.

La tercera de las claves de esta estrategia para contrarrestar la amenaza híbrida pasa por disponer de una *estructura institucional* -personal, procesos, herramientas, soporte operativo y legal- *con autoridad* para decidir en supuestos de crisis y *con capacidad* para coordinar y dirigir la respuesta. Este enfoque holista y multidisciplinar se integra en la política de Estado que define la estrategia de seguridad nacional y, como tal, se considera indispensable para la supervivencia en la ZG. Es así que el informe *Campaigning in the Grey Zone. Towards a Systems Approach to Countering Hybrid Threats* señala:

española Talgo, estratégica para la seguridad económica, la cohesión territorial y el desarrollo industrial nacional. El Gobierno español, a través de sus canales de inteligencia, pudo determinar que dicha compañía húngara mantenía conexiones informales con la rusa Transmashholding, incluso después de la sanción de bloqueo a los intereses empresariales de Rusia tras la invasión de Ucrania. Disponible en: https://elpais.com/economia/2024-08-28/el-cni-alerto-de-la-conexion-rusa-del-grupo-hungaro-que-puja-por-talgo.html
https://es.euronews.com/2024/08/27/el-gobierno-rechaza-la-venta-de-talgo-a-una-empresa-hungara-por-riesgos-para-la-seguridad-
https://www.publico.es/economia/gobierno-rechaza-opa-hungara-talgo-razones-seguridad-nacional.html
https://www.eleconomista.es/transportes-turismo/noticias/12672715/02/24/la-conexion-rusa-en-la-opa-de-talgo-la-sombra-de-putin-se-extiende-sobre-el-fabricante-espanol.html (28/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] It is now a cliche to say that countering hybrid threats requires an integrated, whole-of-government approach. In recent years many nations have placed campaigning in the grey zone between peace and war at the heart of their national security and defence strategies. This approach makes sense: in an era of strategic competition important ground is gained or lost far short of war"[1153] (MONAGHAN & McDONALD, 2023, pág. 1).

Sobre la base de estos tres pilares -conciencia de la dificultad de detección, definición de objetivos estratégicos realistas y disponibilidad de una estructura institucional de respuesta- se construye la estrategia de disuasión y defensa frente a la agresión en la ZG.

Por lo que concierne a la disuasión, componente esencial de la defensa, tradicionalmente se ha entendido como una maniobra de coerción en la que la amenaza se utiliza para influir en la decisión estratégica del rival, pudiendo ejercerse por negación o por represalia. La disuasión por negación tiene como fin socavar la capacidad del contrario para alcanzar su objetivo, minimizando las ganancias de la acción y reforzando, por ello, la resiliencia propia. En el segundo caso, se trata de persuadir al agresor amenazando con un castigo que supondrá para él un coste mayor y desproporcionado respecto a los posibles beneficios obtenidos con su acción ofensiva. En este enfoque tradicional de la disuasión la principal herramienta coercitiva es la amenaza militar, aunque también intervienen otros instrumentos de poder del Estado de carácter diplomático[1154], económico, social o de información (JORDÁN ENAMORADO, 2022, pág. 67).

Esta estructura clásica de la disuasión operó con relativo éxito entre EE.UU. y la URSS durante el periodo de la Guerra Fría, gracias a tres factores: el modelo de actor racional en la toma de decisiones, la presunción del deseo de supervivencia del adversario y la posesión de arsenales nucleares por parte de ambos contendientes. Sobre esta amenaza de *destrucción mutua asegurada*[1155] se configuró el equilibrio entre los competidores sistémicos durante la segunda mitad del siglo XX (JORDÁN ENAMORADO, 2022, pág. 68).

Pero este planteamiento tradicional de la disuasión sustentado en la credibilidad de la respuesta con que se amenaza, la capacidad de llevarla a efecto y la percepción de la voluntad de ejecutarla, es desafiado por la amenaza híbrida que, como hemos señalado, se desenvuelve en la ambigüedad y bajo los umbrales de alerta. Como señala Jordán, en las dos primeras fases de la escalada -configuración del entorno e interferencia[1156]- es muy complicado conseguir influir de manera efectiva en el cálculo de costes y beneficios del agresor, pero pese a ello:

[1153] "Ahora es un cliché decir que contrarrestar las amenazas híbridas requiere un enfoque integral de todo el gobierno. En los últimos años, muchas naciones han colocado las campañas en Zona Gris entre la paz y la guerra en el centro de sus estrategias de seguridad y defensa nacionales. Este enfoque tiene sentido: en una era de competencia estratégica se gana o se pierde terreno mucho antes de comenzar la guerra" (Traducción propia).

[1154] Ver apartado 5.3.2. sobre el uso de operaciones cibernéticas maliciosas en las relaciones entre Estados.

[1155] Ver apartado 2.1.2.

[1156] Ver gráfico 6.1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] la disuasión es útil para mantener la estabilidad estratégica en un nivel bajo-intermedio, evitando la escalada a escalones superiores de la zona gris y alejando además la posibilidad de un conflicto armado abierto" (JORDÁN ENAMORADO, 2022, pág. 78).

Sin embargo, en las fases superiores de la escalada en ZG -desestabilización y empleo puntual de la fuerza- la disuasión vuelve a recobrar todo su sentido, aunque con una serie de consideraciones.

La primera de ellas es que en la ZG debe implementarse una *estrategia de disuasión no escalatoria*, es decir, orientada a lograr la estabilidad en los niveles más bajos del conflicto, que esté adaptada a las particularidades del adversario -valores, intereses, cultura estratégica- y que ofrezca garantías de que si se cumplen los límites señalados no habrá consecuencias. La segunda es la relevancia de la *credibilidad para conseguir articular una disuasión efectiva*, siendo clave para ello que el agresor visualice como altamente probable que el disuasor materialice su amenaza coercitiva si continúa adelante. Y la tercera se refiere a la claridad en el proceso de transmisión del mensaje, es decir, la *comunicación efectiva de las líneas rojas* que no deben ser traspasadas y que deben actuar como puntos de encuentro para conformar una disuasión acumulativa, la cual no pretende una victoria incontestable y total sino que busca el equilibrio mediante éxitos intermedios con los que:

> "[…] trata de alcanzar la estabilidad estratégica a través de un proceso de aprendizaje donde van tomando forma normas de conducta, a veces conocidas como *reglas del juego*" (JORDÁN ENAMORADO, 2022, pág. 82).

Pero, con todo, hay que asumir que la disuasión en la ZG puede fracasar o, simplemente, llegar demasiado tarde. En esta situación, donde la amenaza híbrida ya está desplegando todos sus efectos, surge el dilema de considerar si se debe o no responder ante la acción detectada. Serán el contexto y los objetivos estratégicos del agredido los que le lleven a decidir en uno u otro sentido, siendo que si es afirmativa la solución deberá contar con un marco de respuesta planificado para adoptar las acciones y medidas asertivas oportunas a través de las que lograr los fines pretendidos, entre los que el principal habrá de ser impedir que el adversario continúe con la agresión.

En el informe *Countering Hybrid Warfare* del MCDC este marco de respuesta a la amenaza híbrida se construye sobre tres elementos: las opciones políticas, los factores clave y los instrumentos de poder (MONAGHAN & et al., 2019, págs. 53-60).

Las *opciones políticas* conforman el primer nivel de definición de la respuesta. Son básicamente cuatro, interdependientes:

1. *Reconocer la amenaza híbrida* y enfrentarla o, por el contrario, ignorarla, con las consecuencias que, a posteriori, esta decisión conllevaría de cara al apoyo público y la posibilidad de adoptar otras medidas.
2. *Convenir una respuesta* focalizada hacia el interior, orientada a los propios decisores y la ciudadanía -fomento de la resiliencia, educación contra la

Ediciones Universidad de Salamanca | CC BY-NC-ND

desinformación-, o dirigida al exterior, hacia el adversario o la comunidad internacional -sanciones económicas, medidas diplomáticas-.

3. *Responder* a través de una acción abierta, pública, oficial y transparente, muy eficaz de cara a lograr el soporte y apoyo público -cierre de fronteras-, o mediante una acción encubierta, de conocimiento limitado, que permite enviar un mensaje directo al adversario sin desvelar la autoría del mismo -ciberataque ofensivo-.
4. Proyectar una *respuesta asertiva* para coaccionar al adversario, generándole un alto coste por su agresión -sanciones económicas-, o procurar una serie de medidas para *tratar de inducir un cambio* en el comportamiento del rival -oferta de incentivos o acuerdos ventajosos para ambos-.

Respecto a los *factores clave*, se trata de elementos a tener en cuenta al considerar las opciones políticas para adoptar las medidas de respuesta ante el ataque híbrido. Estos factores a considerar son los riesgos inherentes a la propia acción, la vulnerabilidad del agresor a la que se dirija la respuesta, los instrumentos de poder empleados y la coordinación de las estructuras políticas internas, el control de la escalada, el carácter nacional o internacional de la respuesta y la base jurídica sobre la que se justifique la acción.

En tercer lugar, los *instrumentos de poder* a través de los que se canaliza la respuesta frente al ataque de naturaleza híbrida:

1. La utilización de la *fuerza militar*, buscando el equilibrio entre la proporcionalidad de la respuesta y la máxima eficacia en su aplicación a las vulnerabilidades del agresor. Como ejemplo, la realización de maniobras militares en frontera para mostrar la decisión de actuar y la capacidad para hacerlo[1157].
2. El empleo de *medidas políticas* para controlar el alcance del impacto producido en el adversario, como la expulsión de diplomáticos o el establecimiento de visados u otras restricciones de viaje.
3. Las *medidas económicas*, como la disminución de los intercambios comerciales, la retirada de ayudas, la compra de deuda pública o la imposición de sanciones financieras.
4. La *comunicación estratégica* basada en la aplicación de la transparencia y la unidad de doctrina para hacer pública la agresión y, desde los principios y valores del Estado de Derecho, hacer valer la confianza de la sociedad en las instituciones públicas.

[1157] Un ejemplo de este empleo simultáneo de los instrumentos de poder en ZG, donde se combina las maniobras militares para manifestar esa decisión firme de utilizarlas llegado el caso y exhibir la capacidad de la fuerza junto con la acción diplomática, podemos apreciarlo en el desarrollo del ejercicio de la OTAN denominado "Swift Response" que las fuerzas noratlánticas aliadas llevan a cabo a mediados de mayo de 2024, en escenarios del norte y el este de Europa colindantes con Rusia, al tiempo que el secretario de Estado de EE.UU., Antony Blinken, visita Kiev para reunirse con el presidente Zelenski y su cúpula militar, para reafirmar el compromiso estadounidense con el apoyo logístico y económico a Ucrania. Disponible en: https://www.elconfidencialdigital.com/articulo/defensa/salto-paracaidistas-espanoles-rumania-ejercicio-otan/20240426000000768528.html
https://efe.com/mundo/2024-05-14/antony-blinken-llega-a-ucrania-para-reiterar-apoyo-duradero/ (14/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

5. Medidas de *apoyo a los medios de comunicación* para mejorar el acceso de la población a información veraz y de calidad, junto con la educación frente a la propaganda y la desinformación o la colaboración institucional para elaborar contranarrativas.

En este contexto y en lo que se refiere a la utilización de operaciones en el ciberespacio como medida de respuesta a una acción bajo el umbral de la guerra, tal y como vimos en el capítulo anterior, se imbrican perfectamente en las estrategias híbridas por su particular naturaleza que opera en el quinto dominio, donde la dificultad de atribución, la asimetría entre los actores, la gran vulnerabilidad de las infraestructuras, la ambigüedad de los límites y la desproporcionada y ventajosa relación entre costes y beneficios caracterizan su utilidad como medida de respuesta en la ZG. Al mismo tiempo, conviene recordar que una ciberoperación de bajo nivel y subrepticia con afectación a un servicio esencial del adversario puede tener un mayor impacto táctico que otra acción más notoria y visible, con las consecuencias derivadas en el nivel de la escalada que, como vemos, no guarda una relación directa con los medios aplicados ni con el alcance de los efectos generados.

Asimismo, merece especial atención el uso de las fuerzas armadas en la ZG, entorno de *no guerra* donde se considera que la utilización de medios militares de respuesta puede ser contraproducente e insuflar oxígeno a la estrategia del agresor, al tiempo que reste legitimación al defensor del *statu quo* ante la comunidad internacional. Y no podemos perder de vista que es frente a ésta, precisamente, donde se juega gran parte de la estrategia en ZG, por cuanto el agresor -mayormente un Estado revisionista- enmascara sus acciones en el sistema internacional para alcanzar sus objetivos sin violencia y sin recurrir a capacidades militares relevantes, de manera que, si le funciona, incrementa su cuota de poder dentro del orden establecido debilitando además al adversario.

Por ello, la primera regla fundamental de la doctrina anglosajona para preservar el delicado equilibrio en la ZG establece que los medios más adecuados para responder a la amenaza híbrida, sin escalar al conflicto armado, son todos aquellos que no tengan un componente militar.

Pero a este respecto, cuando se infiere directamente que del uso de las capacidades militares se deriva una escalada en el nivel de agresividad, debemos decir, como señala Nieto, que existe un sesgo que distorsiona la realidad del papel que pueden desempeñar las fuerzas armadas en este tipo de escenarios, sustentado en dos errores principales: por la asociación del término *capacidad militar* con el uso de la fuerza y la violencia, y por la traslación de la deontología y la praxis del ejército estadounidense al español (NIETO FERNÁNDEZ, 2021).

En cuanto al primero de ellos, es razonable asociar la capacidad militar con el empleo de armas pero, al mismo tiempo, es simplista considerar que todas las capacidades militares acaban en el uso de estas. Las fuerzas armadas son uno más de los instrumentos de poder en manos del Estado para actuar en cualquier contexto, por

Ediciones Universidad de Salamanca | CC BY-NC-ND

cuanto están capacitadas para desempeñar multitud de tareas, algunas de las cuales no implican el uso de armas ni, desde luego, de violencia[1158].

En lo concerniente al segundo de los errores, la asimilación directa de la praxis militar anglosajona, hay que señalar que la deontología en el uso de la fuerza del ejército español y del estadounidense es radicalmente distinta, por las diferentes arquitecturas de seguridad nacionales que determinan zonas grises morfológicamente diferentes a las nuestras, su integración en el modelo de Estado y la cultura de defensa de ambos países (NIETO FERNÁNDEZ, 2021).

En este mismo sentido se pronuncia el Centro Conjunto de Desarrollo de Conceptos del EMAD, en la nota conceptual *El papel de las FAS en la Zona Gris (ZG) – (NCZG)*, significando que:

> "Para garantizar su seguridad en los escenarios de ZG, los estados deben dotarse de un sistema capaz de prevenir, detectar, disuadir y responder a estas agresiones, también con carácter ofensivo cuando corresponda, mediante un enfoque integral que contemple todos los instrumentos de poder a su alcance, incluyendo el militar.
> De este modo, las FAS desempeñan en este tipo de conflictos un papel que, aunque limitado, es imprescindible, pues son las encargadas de proyectar la disuasión necesaria para impedir que la parte agresora atraviese un determinado umbral de violencia, evitando así una potencial escalada hacia un conflicto armado entre las partes"[1159].

Como ya hemos señalado, la ZG no se circunscribe a un solo tipo de escenario, sino que evoluciona y se desenvuelve en la ambigüedad y la multiplicidad de frentes. Por ello, la respuesta a la amenaza híbrida debe ser integral. En esta línea, el artículo 9 de la LSN 2015 establece que los componentes fundamentales de la Seguridad Nacional son la Defensa Nacional, la Seguridad Pública y la Acción Exterior[1160]. Cada uno de ellos contribuirá en la medida y en el nivel de intensidad que se determine, junto con el resto de *instrumentos de poder* del Estado, apoyados en la colaboración público-privada, para conformar la respuesta en ZG, de acuerdo con la coordinación que a su nivel lleva a cabo el Gobierno de la nación en línea con las *opciones políticas* y los *factores clave* que maneje para alcanzar sus objetivos estratégicos[1161].

Las fuerzas armadas, en cuanto instrumento de poder utilizable en el contexto de ZG, presentan una serie de características útiles que las hacen particularmente adecuadas,

---

[1158] En este sentido, recordar el papel desempeñado por las Fuerzas Armadas españolas durante la pandemia del COVID-19, en el marco de la Operación Balmis, por la que el Ministerio de Defensa desplegó al ejército en todo el territorio nacional para luchar contra la propagación del coronavirus. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/defensa/Paginas/2020/240320-visita.aspx (12/05/2024).

[1159] Nota Conceptual *El papel de las FAS en la zona gris (ZG) – (NCZG)*. Centro Conjunto de Desarrollo de Conceptos del Estado Mayor de la Defensa. 14 de marzo de 2022. Prefacio.

[1160] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, articulo 9.1: "Se consideran componentes fundamentales de la Seguridad Nacional a los efectos de esta ley la Defensa Nacional, la Seguridad Pública y la Acción Exterior, que se regulan por su normativa específica".

[1161] Ver apartado 4.3.1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

como son su resiliencia en el combate, su capacidad de adaptación a entornos complejos y de coordinación con el resto de elementos de respuesta a disposición del Estado, la interoperabilidad con las autoridades civiles y las Fuerzas y Cuerpos de Seguridad, la propia deontología militar -responsabilidad, servicio público, ética- que asegura un alto nivel de eficacia, su amplio despliegue territorial, el componente de pensamiento geopolítico y la aportación permanente de la inteligencia militar, la competencia técnica para desenvolverse en el ciberespacio, en el ámbito cognitivo y en el conjunto de dominios físicos, así como la capacidad para llevar a cabo operaciones especiales de manera discreta y con bajo nivel de visibilidad en el uso de la fuerza (NIETO FERNÁNDEZ, 2021).

Podemos concluir, en este sentido, que las fuerzas armadas tienen un papel limitado pero necesario en la estrategia de disuasión y respuesta en ZG, basada en el enfoque integral y sinérgico de todos los instrumentos de poder del Estado para recuperar la iniciativa en los distintos ámbitos -económico, diplomático, político, militar, narrativa-. Para ello será necesario modular el factor tiempo en la respuesta y tratar de llevar al ámbito del Derecho Internacional, a través de la interlocución con el resto de actores nacionales y supranacionales, las acciones híbridas que está utilizando el agresor para aprovecharse de este orden prestablecido y alcanzar sus objetivos revisionistas.

6.2. La desinformación como nueva dimensión de la amenaza

Recapitulando lo expuesto hasta ahora, podemos convenir que la visión clásica del mundo occidental ha cambiado. Aquel *Estado moderno* que desplaza a la persona de su foco de atención y se sustenta en el tridente que consagra la Paz de Westfalia sobre la soberanía, el territorio y el monopolio del legítimo ejercicio de la fuerza, es literalmente barrido en la última década del siglo XX.

El final de la Guerra Fría, la caída del Muro de Berlín, la disolución del Pacto de Varsovia o el surgimiento de la *World Wide Web* traen consigo un nuevo panorama geoestratégico que comporta la caducidad del concepto de *Estado moderno*, la desaparición del bipolarismo representado por EE.UU. y la URSS y, sin duda, el fin de la vieja Europa como modelo político y cultural. A partir de ese momento concurren al tablero de juego global nuevos actores públicos y privados, con intereses distintos -incluso enfrentados- y con visiones diferentes de los problemas y de lo que pueden constituir soluciones. Con ello, el individuo pasa a ocupar el centro de atención de la seguridad y de aquellos otros ámbitos con los que, en adelante, se va a interrelacionar de manera indivisible[1162]. Es ahora cuando la seguridad se constituye en el auténtico pilar sobre el que la "sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones"[1163].

[1162] Nos referimos aquí al concepto de seguridad humana, íntimamente relacionada con el desarrollo de las personas y el respeto de los derechos humanos. Véase el apartado 1.3.1.

[1163] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. BOE núm. 233, de 29 de septiembre de 2015. BOE-A-2015-10389. Preámbulo-I, página 3.

Ediciones Universidad de Salamanca | CC BY-NC-ND

A este caldo en ebullición se incorporan Internet, la transformación digital y las nuevas tecnologías para impulsar definitivamente el fenómeno de la *globalización*, caracterizado por tres notas distintivas:

1. La integración como nunca antes se había visto a lo largo de la historia de los ámbitos productivo, económico, político, militar, social y cultural.
2. La acelerada expansión tecnológica de las sociedades modernas, que incorporan las nuevas tecnologías a sus usos y costumbres mucho más rápidamente que en el pasado.
3. Y la hiperconectividad, gracias a la cual los ciudadanos tienen acceso en tiempo real a datos, información y noticias de cualquier parte del mundo.

Como ya hemos estudiado, esta interdependencia ofrece evidentes oportunidades pero, a su vez, conlleva nuevas amenazas como la instrumentalización política de los flujos migratorios[1164], el crecimiento en su dimensión y alcance tanto del crimen organizado como del terrorismo internacional, la llegada de los ciberataques, el auge de las campañas de desinformación y de influencia a través de los medios de comunicación digitales y las redes sociales, la insondable dependencia tecnológica de las infraestructuras y servicios esenciales, las crisis económicas consecutivas e interconectadas a nivel mundial o los graves efectos para la vida del ser humano derivados del cambio climático, entre otras.

Como resultado, nuestra forma de vida se supedita de manera crítica a todas estas tecnologías, hasta el punto de que podemos colapsar si falla el suministro de servicio de alguna de ellas[1165], con el problema añadido de que gran parte de la infraestructura, los datos y las comunicaciones sobre las que se sustenta se hallan bajo el control de empresas privadas[1166]. Es así como las TIC, sobre las que "se depositó la esperanza de

[1164] Un ejemplo de ello lo tenemos en los intentos de asalto a la valla fronteriza de Ceuta durante el mes de septiembre de 2024, tras una campaña en redes sociales incitando a la irrupción masiva de migrantes que pone sobre la mesa derivadas que superan el mero hecho del cruce ilegal de la frontera y hacen pensar en la instrumentalización de la crisis migratoria, que saca a relucir las vulnerabilidades de la política común de la Unión frente a este desafío y, al mismo tiempo, fortalece la imagen de Marruecos como necesario aliado en la región. Disponible en: https://elpais.com/espana/2024-09-15/un-masivo-despliegue-policial-marroqui-impide-que-cientos-de-migrantes-salten-la-valla-de-ceuta.html https://efe.com/espana/2024-09-15/ceuta-intento-salto-valla-marruecos/ https://es.euronews.com/my-europe/2024/09/16/disturbios-y-detenciones-en-castillejos-tras-el-intento-de-saltar-la-valla-de-ceuta (22/09/2024).

[1165] Sirva como ejemplo el fallo generado en los sistemas de Microsoft, en julio de 2024, a raíz de una actualización defectuosa de la plataforma de seguridad CrowdStrike, que tuvo repercusión inmediata en aerolíneas, bancos, sistemas de sanidad, empresas de todo tipo y millones de dispositivos a nivel mundial. Disponible en: https://efe.com/economia/2024-07-19/actualizacion-crowdstrike-fallo-incidencias-microsoft/ https://ciberseguridadtic.es/reportajes/los-principales-detalles-del-incidente-de-crowdstrike-y-microsoft-202407226156.htm https://www.europapress.es/portaltic/ciberseguridad/noticia-crowdstrike-avanza-error-ocasiono-apagon-global-no-puede-repetirse-hecho-evitarlo-20240807141103.html (22/09/2024).

[1166] En este sentido podemos citar como ejemplo la red intercontinental de cables submarinos de fibra óptica, pieza esencial de la infraestructura de comunicaciones global que permite la disponibilidad de servicios de Internet y otros tipos de transacciones de diversa naturaleza. La mayoría de estos sistemas de cables submarinos son propiedad de empresas privadas de telecomunicaciones e Internet. Disponible en: https://www.nbr.org/publication/submarine-cables/ (24/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

fortalecer el debate público, la contribución a la mejora de la calidad democrática y la transparencia, así como el estímulo y favorecimiento del acercamiento de los ciudadanos con sus administraciones e instituciones públicas" (SANSÓ-RUBERT PASCUAL, 2024, pág. 30), se convierten en pieza clave de la amenaza híbrida y desinformadora.

Este paisaje conforma el escenario de la amenaza híbrida, tal y como expuso el anterior Secretario General de la OTAN, Jens Stoltenberg, en la inauguración en octubre del 2017 del Centro Europeo de Excelencia Contra las Amenazas Híbridas (Hybrid CoE) en Helsinky:

> "Las amenazas híbridas son muchas cosas distintas combinadas, desde la propaganda y la desinformación hasta el uso de fuerzas regulares, desde los 'tuits' hasta los tanques"[1167]

Pero hemos de decir que nada nuevo supone el uso de la propaganda y la desinformación como arma de guerra[1168]. En concreto, el siglo XX en sí mismo fue un "vasto laboratorio de pruebas de la desinformación y la mentira profesional organizada, sobre todo durante los años de entreguerras y la guerra fría" (RID, 2021, pág. 12) . Sin embargo, lo que sí es novedoso es el aumento exponencial, tanto en magnitud como en frecuencia y eficacia, de su utilización y alcance gracias a la tecnologización de la sociedad, sus nuevos hábitos de comunicación y la consabida transformación digital de las infraestructuras y servicios esenciales. Corren tiempos en los que las fuentes de información oficiales han perdido credibilidad y son escrutadas desde la desconfianza epistémica, a lo cual coadyuva de manera decisiva la tecnología por cuanto muchas personas, desde el anonimato que ofrece la red, amparadas por la seguridad de un *nickname*, defienden posiciones violentas, totalitarias o extremistas que alimentan falsedades y narrativas alternativas que, en definitiva, vienen a dar aún mayor pábulo al *todo es mentira* (RAMONET, 2022, pág. 74).

[1167] El 2 de octubre de 2017 el Secretario General de la OTAN, Jens Stoltenberg, y la jefa de la diplomacia europea, Federica Mogherini, inauguraron en Helsinki el Centro Europeo de Excelencia Contra las Amenazas Híbridas (Hybrid CoE), momento en el que se refirieron a las operaciones encubiertas y la desinformación. Disponible en: https://www.lavanguardia.com/politica/20171002/431759376364/otan-y-ue-inauguran-en-helsinki-un-centro-europeo-contra-amenazas-hibridas.html (15/09/2024).

[1168] En este sentido puede citarse a personajes históricos del pasado siglo como el líder de la socialdemocracia rusa Vladimir Lenin, que empleó la propaganda para promover sus ideales políticos y revolucionarios, o el ministro de Propaganda del Tercer Reich, Joseph Goebbels, máximo exponente del régimen nazi sobre el uso de la propaganda como arma de guerra. También es destacable el uso de la la imagen y la caricatura como herramienta de propaganda en la guerra, donde destaca Mario Armengol que, al servicio del Gobierno británico, dibujó alrededor de 2000 caricaturas contra el líder nazi Adolf Hitler, publicados en diarios aliados. Al respecto puede ampliarse información en las referencias en prensa a la exposición temática de sus dibujos en el MUVIM de Valencia, desde octubre de 2024 hasta febrero de 2025, con el título *Tinta contra Hitler. Mario Armengol, caricaturista en la II Guerra Mundial*. Disponible en: https://elpais.com/cultura/2024-10-03/mario-armengol-el-gran-desconocido-de-la-caricatura-de-la-segunda-guerra-mundial-contra-hitler.html
https://www.rtve.es/play/videos/telediario-2/armengol-dibujante-caricaturas-contra-hitler/16279995/
https://www.dival.es/sala-prensa/sites/default/files/sala-prensa/VERSI%C3%93%20DIGITAL%20TRILING%C3%9CE%20TINTA%20CONTRA%20HITLER.pdf
(11/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

En este campo abonado de crisis de racionalidad, donde cualquier ciudadano de la *aldea global* se deja mecer por el atractivo del rumor y la conspiración, la amenaza desinformativa ha echado raíces y busca alimento a través de *generar confusión y manipular la opinión de las personas, desestabilizar las instituciones y fomentar la radicalización y el odio*. El objetivo es activar las emociones para captar la atención del público que, además, carece de una adecuada alfabetización digital y mediática que le habilite mínimamente para consumir de manera adecuada esa información que le llega a raudales por cauces desbordados. Estas emociones -miedo, enfado, sorpresa, tristeza, etc.- calan en una sociedad porosa y predispuesta que va a responder inmediatamente exagerando sus propias diferencias -sociales, culturales, territoriales, religiosas, etc.-, amplificando a su vez esta complicada situación al utilizar masivamente las redes sociales (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 58)

A esto hay que sumar, coincidiendo con Aznar Fernández-Montesinos, que no parece ser este un proceso pacífico sino todo lo contrario, puesto que "la globalización progresa mediante el conflicto", unido al permanente cambio y la incertidumbre que éste conlleva (AZNAR FERNÁNDEZ-MONTESINOS, 2024).

Avanzando en el análisis de la cuestión, debemos señalar que los responsables de estos ataques pueden ser Estados -a través de sus estructuras de inteligencia o grupos aliados de naturaleza privada- con el objetivo de debilitar a sus adversarios, o grupos de presión que buscan influir en las decisiones de un país conforme a sus intereses o, incluso, hacktivistas que pretenden defender su particular interpretación del libre intercambio de información o de la libertad de expresión por encima de cualquier otro tipo de derecho fundamental o interés común de la sociedad democrática.

Pero, a veces, el ataque proviene del interior, de alguien *de los nuestros*. En estos supuestos la fractura institucional y política no es causada por un actor exógeno sino, aún mucho peor, por un elemento endógeno que no casa con el resto de la estructura social y que aprovecha todos los medios a su alcance -principalmente las redes sociales- para transmitir el mensaje que quieren oír sus seguidores, buscando de esta manera la confrontación con los que piensan distinto, alimentar fanatismos entre los que comparten sus teorías y sellar lealtades con el grupo de pertenencia, haciendo suyo el lema de *a donde va uno, vamos todos*[1169].

Un ejemplo de ello es el asalto al Capitolio de los EE.UU., el 6 de enero de 2021, cuando los fanáticos seguidores del recién derrotado candidato a la presidencia, Donald Trump, se lanzaron a la conquista del vértice de la democracia estadounidense, bajo la consigna de remediar la *gran estafa en las urnas* que, según su líder, los adversarios del Partido Demócrata habían urdido contra él. Ese grave acontecimiento de carácter político:

> "[…] fue el resultado de una gran confrontación previa en las redes sociales, en la que los fanáticos conspiracionistas leales a Donald Trump lograron imponer la tesis de un gran engaño electoral que nunca existió. A lo largo del controvertido mandato del magnate republicano se produjo una encendida batalla frontal, en las redes, por el control del relato: una confrontación digital de gran envergadura

[1169] Este es uno de los lemas principales del movimiento complotista estadounidense QAnon.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> para desinformar, tratar de imponer una falsa verdad complotista y ocultar la realidad de las urnas. Ahí, las redes fueron absolutamente decisivas" (RAMONET, 2022, pág. 79)

La cuestión es que cuando una persona como Donald Trump, paradigma de la intriga y la mentira aplicadas a la consecución del poder, llega a gobernar e, incluso, a repetir mandato en una democracia como la de EE.UU., surge la duda de si las instituciones que le han llevado a presidir el país serán capaces de contenerlo o, por el contrario, el personaje las subvertirá al utilizarlas en su propio interés. A esta pregunta tratan de responder Steven Levitsky y Daniel Ziblat cuando afirman que:

> "Las instituciones por sí solas no bastan para poner freno a los autócratas electos. Hay que defender la Constitución, y esa defensa no sólo deben realizarla los partidos políticos y la ciudadanía organizada, sino que también debe hacerse mediante nomas democráticas. Sin unas normas sólidas, los mecanismos de control y equilibrio no funcionan como los baluartes de la democracia que suponemos que son. Las instituciones se convierten en armas políticas, esgrimidas enérgicamente por quienes las controlan en contra de quienes no lo hacen" (LEVITSKY & ZIBLAT, 2021, pág. 16).

Por ello la desinformación, que es consustancial al ser humano, forma parte de las amenazas híbridas, capaces de combinar el empleo de cualquier tipo de medio -civil, militar, político- con ataques cibernéticos, con elementos de presión económica, la utilización sediciosa de personas e instituciones, el engaño, la difusión de narrativas con interés subrepticio o las campañas de influencia en las redes sociales, constituyendo así uno de los grandes desafíos de seguridad para cualquier democracia, puesto que aprovecha las debilidades y temas de fricción de la sociedad para alcanzar sus fines hostiles o utilitarios. Este reto solo puede afrontarse desde un gran compromiso compartido, político y social, de Estado. No debemos olvidar que, en última instancia, la supervivencia de los valores que sustentan la democracia depende de los ciudadanos:

> "[…] Los valores de la libertad y la igualdad se justifican por sí mismos, pero no se ejecutan solos" (LEVITSKY & ZIBLAT, 2021, pág. 247).

6.2.1. Marco conceptual de la desinformación

El fenómeno de la desinformación tiene multitud de ramificaciones que hacen complejo encontrar un prisma unificado para definirlo. Así, existe una amalgama de acepciones que, consecuentemente, complica sobremanera la elaboración de una estrategia concreta contra esta amenaza. Por ello, al no estar acordado unánimemente el concepto y alcance de la desinformación, es complicado concertar líneas de acción entre diferentes organismos, tanto en clave nacional como internacional, dirigidas a identificar, analizar, compartir información y responder a sus ataques de manera coordinada. Asimismo, al tratarse de una cuestión siempre atractiva y generadora de contenido en los medios de comunicación y, en general, seductora para el conjunto de la población, las injerencias de formadores de opinión, no siempre cualificados, tienen su influencia en la percepción social del término desinformación, siendo así que esta

Ediciones Universidad de Salamanca | CC BY-NC-ND

realidad, en su conjunto, termina por distorsionar el entorno relacionado con esta amenaza híbrida.

Por si esto fuera poco, el entorno cultural y social en el que se contextualice el uso del término repercute en el propio concepto y la realidad que engloba. Así, el profesor Díaz Fernández, en una aproximación a los términos propios de la cultura de inteligencia rusa, se refiere al concepto *desinformatzia*[1170] como:

> "Préstamo del ruso que hace referencia al conjunto de prácticas cuyo objetivo es promover la manipulación de las élites políticas y de la opinión pública mediante la difusión de noticias falsas con la finalidad de alterar la percepción del destinatario, para favorecer los intereses de quien lo pone en práctica. Si bien históricamente los Estados la han aplicado profusamente, es en 1952 cuando se oficializa su uso tras su incorporación a la *Enciclopedia Soviética*. Desde el ámbito de los servicios de inteligencia, en el ejercicio de actividades proactivas se ha empleado profusamente con la intención de influir sobre actores y procesos políticos, condicionando así el curso de los acontecimientos" (DÍAZ FERNÁNDEZ, y otros, 2013, pág. 111).

A mayores, el marco de referencia conceptual difiere del ámbito anglosajón al español, que concentra los términos utilizados en aquel. En este sentido, Wardle y Derakhshan en su informe de 2017 para el Consejo de Europa muestran tres diferentes acepciones:

> "Dis-information. Information that is false and deliberately created to harm a person, social group, organization or country.
> Mis-information. Information that is false, but not created with the intention of causing harm.
> Mal-information. Information that is based on reality, used to inflict harm on a person, organization or country"[1171].

Por este motivo, nuestra Estrategia de Seguridad Nacional 2021 advierte que:

> "Las campañas de desinformación tienen clara repercusión en la Seguridad Nacional y deben diferenciarse de otros factores como la información falsa —*fake news*— o información errónea —*misinformation*—. De hecho, las campañas de

[1170] Es relevante el dato temporal por cuanto que, ya en 2013, la inteligencia rusa visualiza claramente el amplio espectro operacional de la desinformación mientras que, en Europa, como veremos más adelante, no será hasta 2015 cuando, en el seno del servicio Europeo de Acción Exterior, se cree el Grupo de Trabajo East StratCom con el fin de analizar y proponer una respuesta conjunta y coordinada frente a esta amenaza principalmente orquestada desde el Kremlin.

[1171] "Dis-information: Información falsa y creada deliberadamente para dañar a una persona, grupo social, organización o país. Mis-information: Información que es falsa, pero que no se creó con la intención de causar daño. Mal-information: Información que se basa en la realidad, utilizada para infligir daño a una persona, organización o país" (Traducción propia).
Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe report DGI(2017)09. Claire Wardle, PhD and Hossein Derakhshan. Disponible en: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html (06/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> desinformación no contienen necesariamente noticias falsas, sino que pretenden distorsionar la realidad mediante contenido manipulado"[1172].

Esta panoplia de diferentes enfoques relacionados con información falsa, o malinterpretada o tergiversada, es descrita por Tandoc, Thomas y Bishop que, después de una revisión exhaustiva de diferentes entornos de la información desde el 2013 al 2017, terminan infiriendo que el término es aplicado en fenómenos muy diferentes como la parodia, la imitación de noticias, la propaganda o, incluso, la publicidad (TANDOC , THOMAS, & BISHOP, 2021, págs. 215-217). Esta circunstancia no invita a afirmar que las noticias falsas no puedan ser parte de una estrategia de carácter híbrida contra los intereses que debe proteger la Seguridad Nacional. Tampoco debe inferirse que, en otras sociedades de la información, las noticias falsas no puedan englobarse dentro de la desinformación puesto que la veracidad de la noticia tiene mucho que ver con la percepción y la cultura que engloba a los individuos receptores de la información.

En español nuestra Academia, la RAE, entiende el verbo *desinformar* como "dar información intencionadamente manipulada al servicio de ciertos fines", poniendo así el foco de atención en la falsedad del mensaje y en la intencionalidad del emisor de ocultar al receptor el conocimiento fundado de los hechos. Conforme a ello, el profesor Fernández Rodríguez entiende la desinformación como:

> "[…] la situación final del proceso comunicativo que falsea el mensaje con relación a los datos veraces. […] De esta forma, la desinformación puede ser uno de los efectos habituales de la susodicha manipulación informativa que determina la imposibilidad del conocimiento fundado de los distintos sucesos, que en ocasiones serán relevantes en la conformación de la opinión pública democrática" (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 25).

Parece por ello necesario considerar que el acceso a la información verdadera, contrastada y diversa que ayude a formar la opinión pública constituye uno de los cimientos principales de las democracias, por lo que debe ser empeño de las instituciones proteger a sus ciudadanos de un fenómeno tan abrasivo para aquellas como la desinformación. *El lugar que ocupan tanto la verdad como la desinformación, o incluso la mentira, es el elemento diferenciador entre las democracias y los sistemas autocráticos y dictatoriales*. Tanto es así que el Consejo de Seguridad Nacional advierte que la información es:

> "[…] el instrumento que permite a los ciudadanos formarse una opinión sobre los distintos asuntos políticos y sociales. Además, la información permite a la ciudadanía adquirir conciencia y fundamento para participar en los debates públicos y, entre otros derechos democráticos, en los procesos electorales"[1173].

[1172] Estrategia de Seguridad Nacional 2021. Capítulo 3, página 60. Presidencia del Gobierno, Madrid, 2021. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 (06/10/2024).

[1173] Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Apartado 1. Contexto. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-13663 (06/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

La Comisión Europea, en su Comunicación titulada *La lucha contra la desinformación en línea: un enfoque europeo*, establece que:

> "La desinformación se define como información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público. El perjuicio público comprende amenazas contra los procesos democráticos políticos y de elaboración de políticas, así como contra los bienes públicos, como la protección de la salud, el medio ambiente o la seguridad de los ciudadanos de la UE. La desinformación no incluye los errores de información, la sátira y la parodia ni las noticias y los comentarios claramente identificados como partidistas"[1174].

En este mismo sentido, el Grupo de Trabajo East StratCom en su página web, recurriendo como fuente al *Plan de Acción para la Democracia Europea*, define la desinformación como:

> "Contenido falso o engañoso compartido sin intención de causar daño. Sin embargo, sus efectos pueden ser igualmente dañinos, por ejemplo, cuando las personas comparten información falsa con amigos y familiares de buena fe"[1175].

Avanzando un paso más en cuanto a la catalogación como amenaza híbrida, el documento titulado *Strategic communications as a key factor in countering hybrid threats,* del Servicio de Estudios del Parlamento Europeo[1176] considera que:

> "Disinformation is a key component of hybrid threats. It can be defined as «verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public». Disinformation campaigns take advantage of the possibilities opened up by digital platforms"[1177].

[1174] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La Lucha contra la desinformación en línea: un enfoque europeo. Bruselas, 26.4.2018. COM(2018) 236 final. Página 4. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236 (26/08/2024).

[1175] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción para la Democracia Europea. Bruselas, 3.12.2020. COM(2020) 790 final. Página 21. Disponible en: https://commission.europa.eu/document/63918142-7e4c-41ac-b880-6386df1c4f6c_es (27/08/2024).

[1176] "Las Comunicaciones estratégicas como factor clave para contrarrestar las amenazas híbridas" (Traducción propia). *Strategic communications as a key factor in countering hybrid threats. European Parliamentary Research Service*. March 2021. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656323/EPRS_STU(2021)656323_EN.pdf (27/08/2024).

[1177] IBIDEM, página 1. "La desinformación es un componente clave de las amenazas híbridas. Se puede definir como «información verificablemente falsa o engañosa que se crea, presenta y difunde para la obtención de un beneficio económico o para engañar intencionalmente al público». Las campañas de desinformación aprovechan las posibilidades que ofrecen las plataformas digitales" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por su parte, en el Plan de Acción para la Democracia Europea[1178] se distingue *entre diferentes fenómenos que se suelen denominar «desinformación» para permitir diseñar respuestas políticas adecuadas,* buscando los rasgos distintivos de ésta con respecto a la información engañosa, la injerencia extranjera y las operaciones de influencia. En cuanto a la información engañosa:

> "[…] es la información con contenidos falsos o engañosos compartida sin intención de perjudicar, aunque sus efectos pueden ser nocivos, es decir, cuando la gente comparte información falsa con amigos y familia, de buena fe".

En lo que respecta a las operaciones de influencia:

> "[…] por operación de influencia en la información se entiende los esfuerzos coordinados tanto de actores nacionales como extranjeros para influir en un público destinatario usando una serie de medios engañosos, como la supresión de fuentes de información independientes, unida a la desinformación".

La injerencia extranjera se define como:

> "[…] por injerencia extranjera en el espacio de información, a menudo realizada como parte de una operación híbrida más amplia, pueden entenderse los esfuerzos coercitivos y engañosos para perturbar la libre formación y manifestación de la voluntad política de las personas por parte de un actor estatal extranjero o de sus agentes".

Finalmente, la desinformación se conceptualiza como:

> "[…] la desinformación es un contenido falso o engañoso que se difunde con intención de engañar o de obtener una ganancia económica o política y que puede causar un perjuicio público".

Tal y como indica el profesor Torreblanca, actores malintencionados han empleado las redes sociales para, mediante operaciones de influencia y desinformación cuidadosamente planificadas y ejecutadas, debilitar la confianza del público en las instituciones democráticas y en los medios de comunicación (LAPUENTE, y otros, 2020, pág. 139). Las estrategias híbridas dirigidas contra la seguridad nacional, que utilizan la desinformación como uno de sus vectores de ataque, pretenden erosionar los derechos y libertades fundamentales consagrados tanto en nuestra Carta Magna[1179] como en la

[1178] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción para la Democracia Europea. COM(2020) 790 final. Bruselas, 3.12.2020. Página 21. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423 (07/09/2024).

[1179] En concreto en el artículo 20.1 CE se protege el derecho a comunicar y recibir libremente información veraz por cualquier medio de difusión: "1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. b) A la producción y creación literaria, artística, científica y técnica. c) A la libertad de cátedra. d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades".

Ediciones Universidad de Salamanca | CC BY-NC-ND

Carta de los Derechos Fundamentales de la Unión Europea[1180] y en la Declaración Universal de los Derechos Humanos[1181]. Es por todo ello que se advierte esencial acordar el marco conceptual en el que nos movemos al utilizar el término de desinformación.

Como conclusión, a los efectos de esta tesis seguiremos la línea terminológica marcada por la UE y nuestra ESN 2021, con la consideración de que la desinformación referencia a un hecho que, no siendo real en su comprensión global -por el tipo de información transmitida o por el momento temporal en que se difunde- se malinterpreta o tergiversa por el agente actor para, en el contexto superior de una estrategia de ataque, contribuir al objetivo final que resulta beneficioso para él[1182]. Es importante recalcar que esta malinterpretación o tergiversación de la información se produce en el marco de una estrategia específica de ese actor, orientada a producir de una u otra forma un desgaste en la seguridad y estabilidad del Estado atacado. Una acción desinformativa que no forme parte de un marco superior estructurado, esto es, de una estrategia, no es necesario que tenga una respuesta desde la arquitectura de la seguridad nacional que, como hemos visto, basa su actuación en una aproximación de tres pilares: la defensa nacional, la acción exterior y la seguridad pública[1183].

6.2.2. Contexto y causas principales de la desinformación

Como hemos mencionado, el uso de la rumorología, el espionaje, la comunicación tendenciosa o la propaganda como herramientas en la guerra, o en la paz, para desgastar o perjudicar al rival es algo que podríamos considerar consustancial a la naturaleza humana. La manipulación informativa ha existido a lo largo de la historia como medio para alcanzar objetivos diversos, siendo así utilizado frecuentemente por el poder para asentar su dominio y perpetuar su influencia, o por razones religiosas, otras veces movida por intereses geopolíticos o, también, para alimentar determinados liderazgos o episodios de tinte nacionalista que alimenten la alineación del pueblo con la visión idealizada que interese difundir.

Sin embargo, el actual aprovechamiento que de la desinformación se hace en el contexto internacional es algo que, por sus dimensiones y particular adaptación al entorno tecnologizado moderno, puede considerarse novedoso. Este crecimiento

[1180] El artículo 11 tutela la libertad de expresión y de información: "1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. 2. Se respetan la libertad de los medios de comunicación y su pluralismo".

[1181] Su artículo 19 señala que "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

[1182] En este sentido, la ESN 2021 señala que "las campañas de desinformación tienen clara repercusión en la Seguridad Nacional y deben diferenciarse de otros factores como la información falsa —fake news— o información errónea —misinformation—. De hecho, las campañas de desinformación no contienen necesariamente noticias falsas, sino que pretenden distorsionar la realidad mediante contenido manipulado". Estrategia de Seguridad Nacional 2021. Capítulo 3, página 60. Presidencia del Gobierno, Madrid, 2021. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 (18/09/2024).

[1183] Ver Capítulo 4, apartado 4.3.

Ediciones Universidad de Salamanca | CC BY-NC-ND

exponencial de la amenaza desinformativa es fechado y sistematizado por Thomas Rid al señalar que la *era moderna de la desinformación:*

> "[…] comenzó a principios de los años veinte del siglo XX, y el arte y la ciencia de lo que la CIA una vez llamó «guerra política» fue creciendo y cambiando en cuatro grandes oleadas, cada una en una generación. A medida que la teoría y la práctica de la desinformación fueron evolucionando, también lo hicieron los términos que describían lo que estaba sucediendo" (RID, 2021, pág. 10).

Siguiendo a este autor, podemos distinguir *cuatro oleadas en la evolución moderna de la desinformación*. La primera de ellas abarca los años previos a la Segunda Guerra Mundial, cuando el salto del papel impreso a la radio transforma la manera de hacer periodismo imponiendo un ritmo mucho más ágil de la comunicación y del tratamiento de la información. En ese momento la desinformación no está profesionalizada y se esgrime por los débiles frente al poder hegemónico -los EE.UU. y la URSS-, casi en una visión romántica del enfrentamiento entre contendientes desiguales, operando mediante acciones conspirativas y anónimas que acuden a cualquier medio disponible, muchas veces obligados a la innovación por la falta de recursos (RID, 2021, págs. 10-11).

Tras la guerra, en el periodo que transcurre desde 1945 hasta finales de los años setenta, las agencias de inteligencia rusa y estadounidense dan un nuevo contexto a la desinformación mucho más profesionalizado. Se trata de la segunda oleada, donde aparece la televisión y los recursos aumentan, aunque esta táctica sigue teniendo un marcado componente de complementariedad de las vías política y militar. Terminológicamente los servicios secretos estadounidenses se refieren a la mezcla de revelaciones secretas, datos falsos e influencia psicológica como *political war*, mientras que los rusos prefieren denominarla *desinformatzia*. En ambos casos el objetivo no es otro que:

> "[…] exacerbar las tensiones y contradicciones existentes en el seno del cuerpo político del adversario utilizando hechos reales y falsos y, a poder ser, una desconcertante combinación de ambos" (RID, 2021, pág. 11).

La tercera oleada de la *era moderna de la desinformación* comienza en los años ochenta y se alarga hasta comienzos del nuevo siglo, caracterizándose por la aparición de Internet y el despliegue de tácticas de persuasión más perfeccionadas, soportadas por amplios recursos específicos y gestionadas de manera profesional que recurren, incluso, a la sociología y la psicología para mejorar sus resultados. Las medidas aplicadas son cada vez más activas y se orientan en gran parte hacia la influencia psicológica a medio y largo plazo, personalizada a través de agentes muy cualificados, pacientes y próximos al objetivo manipulado. El bloque soviético alcanza en este arte una clara ventaja que, con la caída de la URSS, prácticamente desaparece (RID, 2021, pág. 11).

La cuarta oleada que cataloga Rid alcanza su máximo desarrollo en torno al año 2015, cuando la desinformación se imbrica con las nuevas capacidades que le brinda la tecnología y la masiva implantación de Internet, lo cual transforma el mundo de la información y la comunicación al permitir el envío de mensajes en tiempo real a audiencias cada vez más amplias. Fruto de ello, el nivel de actividad y el poder de

Ediciones Universidad de Salamanca | CC BY-NC-ND

penetración de las operaciones de influencia se exacerban hasta límites nunca antes imaginados (RID, 2021, pág. 11).

Nosotros nos atrevemos a proponer una *quinta oleada de la era moderna de la desinformación*, la que denominamos *era de la competencia cognitiva*, que se iniciaría en las elecciones presidenciales estadounidenses de 2016 y que llegaría hasta el momento actual, cuando Donald Trump vuelve a erigirse por segunda vez como Presidente electo. El elemento diferencial de la desinformación en esta última fase es la mutación de su naturaleza: pasa de ser una táctica aplicada a un fin, un método complementario utilizado entre los contendientes en el marco de sus propias estrategias de enfrentamiento, a constituir por sí misma una *amenaza* poliédrica y de alcance global con repercusiones que superan el tradicional conflicto entre competidores. La desinformación adquiere en esta última etapa una nueva dimensión impulsada por la aplicación de extraordinarios -y opacos- algoritmos informáticos que, favorecidos por la IA, combinan la minería de datos con el *microtargeting* y el análisis de la psicología del comportamiento humano. Esto da como resultado una espectacular capacidad para clasificar la información y segmentar al público objetivo conforme a sus creencias y tendencias de opinión, lo cual permite lanzar inmediatamente a través de cualquier medio mensajes personalizados *ad hoc* para orientar, manipular o enmarañar la información y, con ella, la realidad percibida por cada uno de los destinatarios. Es el conocido como *sesgo del algoritmo*, con el que entramos de lleno en la *era de la competencia cognitiva*, en la que la desinformación y la comunicación algorítmica se convierten en sus principales adalides, elevando a niveles máximos el margen de manipulación e influencia subliminal que el uso de la tecnología permite sobre el comportamiento humano.

En este sentido, el profesor Fernández Rodríguez también se refiere a una nueva dimensión de la manipulación informativa a partir de la campaña presidencial estadounidense del 2016, que vendría a corroborar la distinción propuesta de una *quinta oleada* de la desinformación:

> "Cuando Donald Trump recurrió de manera insistente en su campaña de 2016 a la denuncia de las *fake news*, en lo que metía casi cualquier información que entendía que no le beneficiaba, en el fondo buscaba confundir al electorado, lo que a la postre le ayudaría a conseguir más votos. Al candidato de fuera del sistema le interesaba el caos en la campaña para tener más opciones. Quizá sea en ese 2016 cuando todo el mundo se dio cuenta de la dimensión a la que había llegado la manipulación informativa" (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 57).

Abunda en esta consideración Ángel Badillo al referirse a la generalización de las técnicas de *microtargeting* y la utilización de datos de millones de personas sin su consentimiento tanto en la campaña electoral de Donald Trump como en el referéndum del Brexit en 2017:

> "El caso Cambridge Analytica puso en evidencia que los datos acumulados por las redes sociales permiten, en cualquier caso, la planificación de campañas específicas dirigidas a grupos muy pequeños de usuarios (*microtargeting*) con noticias falsas que por la propia naturaleza de las redes sociales solo pueden ser

Ediciones Universidad de Salamanca | CC BY-NC-ND

> vistas por esos usuarios y, por tanto, escapan del escrutinio de los medios o de otros actores de la esfera pública, con el consiguiente riesgo de contribuir a campañas de desinformación" (BADILLO, 2019, pág. 22).

Una vez contextualizada la amenaza desinformativa como el gran desafío que representa, podemos pasar a analizar sus causas. Por su equilibrio entre síntesis y nitidez, recurrimos para vertebrar este estudio a la Comunicación de la Comisión Europea de 2018 titulada *La lucha contra la desinformación en línea: un enfoque europeo*[1184], en la que se apunta a la interrelación de causas económicas, tecnológicas, políticas e ideológicas.

Podemos decir que con este documento, en primer lugar, la Comisión plantea un enfoque visionario al calificar a la desinformación como *síntoma* de aquellas sociedades tensionadas por la rapidez con que evolucionan. Según esta interpretación, la amenaza desinformativa es un indicio que sugiere problemas económicos, culturales e ideológicos que conforman el caldo de cultivo de la polarización, el extremismo y la desconfianza epistémica. Lógicamente, la gravedad de estos síntomas no es la misma para todos los cuerpos sociales y dependerá de factores propios como los niveles de educación, la firmeza de las convicciones y valores democráticos, la confianza en las instituciones y el grado de desigualdad económica y social, entre otros[1185]. En este sentido, como señala Ángela González Montes, Experta Nacional Destacada en la Comisión Europea, "la relación entre desinformación, nuevas formas de consumo de noticias y auge de ideas autoritarias entre los jóvenes no es casual. Se está creando un caldo de cultivo que pone en peligro el relevo generacional de nuestras democracias" (GONZÁLEZ MONTES, 2024).

En segundo lugar, la Comisión Europea vincula la difusión de la desinformación con la profunda transformación de los medios de comunicación y el novedoso papel que las plataformas digitales desempeñan en base al gran número de usuarios que congregan, el máximo rendimiento económico que consiguen del tiempo que aquellos utilizan consumiendo sus servicios en línea, y el consiguiente resultado desinformador que se genera al privilegiar la cantidad de información suministrada sobre su calidad[1186].

Finalmente, esta Comunicación se refiere a la manipulación de las redes sociales como instrumento facilitador de esta amenaza a través de tres pasos secuenciales:

1. La *rentabilidad* de la desinformación por su bajo coste y el elevado poder de influencia que consigue mediante el aprovechamiento de las nuevas tecnologías.
2. La *amplificación de sus efectos* por el uso de algoritmos que facilitan el intercambio de contenidos personalizados, la utilización de servicios automatizados para su difusión y el manejo de la publicidad en las redes sociales.

[1184] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La Lucha contra la desinformación en línea: un enfoque europeo. Bruselas, 26.4.2018. COM(2018) 236 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236 (22/09/2024).
[1185] IBIDEM, página 5.
[1186] IBIDEM, página 5.

Ediciones Universidad de Salamanca | CC BY-NC-ND

3. La *contribución de los propios usuarios* a este problema por la propensión a compartir contenidos sin verificar entre sus grupos de pertenencia[1187].

Se trata por lo tanto de un conglomerado de factores -incluido el de la rentabilidad económica para las plataformas digitales- y de intereses de distintos actores -privados, políticos, institucionales- el que explica por qué la desinformación tiene el dimensionamiento actual que percibimos.

A modo de conclusión, podemos señalar ocho de estas causas que contribuyen a impulsar el uso cada vez más recurrente de las acciones de desinformación:

1. La *falta de estandarización conceptual* para poder unificar criterios de actuación normativa y de respuesta tanto en el ámbito nacional como internacional.
2. El *alto nivel de efectividad* que los mensajes difundidos obtienen gracias a la evolución tecnológica y la ciberdependencia de la sociedad actual, factores que se potencian con peculiaridades atávicas del ser humano, como la que concluye que los rumores y la mentira resultan más atractivos que la simple y desnuda verdad. A este aspecto se refiere el propio Tribunal de Cuentas Europeo:

   > "Una de las principales razones por las que la desinformación es tan grave se debe al uso generalizado de internet, combinado con la llegada de las nuevas tecnologías y la utilización cada vez mayor de plataformas en línea para acceder a la información. Esto facilita enormemente la creación, intensificación y divulgación de informaciones falsas"[1188].

3. La *dificultad para determinar la atribución directa* de una campaña de desinformación, debido a la anonimidad que garantiza la propia naturaleza de Internet a través de los perfiles digitales anónimos, el software de ocultación de direcciones IP, los algoritmos que favorecen el contenido personalizado, la volatilidad de los contenidos publicados o la deslocalización propia de la red, todo lo cual afecta a las tareas de búsqueda y hace que sea muy compleja y laboriosa la misión de trazar la información y su fuente de origen para conseguir una evidencia digital que permita sustanciar una denuncia con base legal firme.
4. La *falta de cobertura penal en los Estados democráticos* para criminalizar las acciones de desinformación y de manipulación de la opinión pública. Por ejemplo, en el caso de España, la libertad de expresión y de opinión garantizados en el artículo 20 CE[1189] son derechos fundamentales que no pueden ser restringidos mediante ningún tipo de censura previa y cuyo único límite es el respeto al resto de derechos fundamentales[1190]. Por ello, un medio de

[1187] IBIDEM, páginas 5 y 6.

[1188] Tribunal de Cuentas Europeo. Informe Especial 9/2021 *El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada*. 2021/C 215/06. Apartado 77, página 33. Disponible en: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_ES.pdf (22/09/2024).

[1189] Articulo 20 CE: 1. Se reconocen y protegen los derechos: *a)* A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. *d)* A comunicar o recibir libremente información veraz por cualquier medio de difusión.

[1190] En este sentido, pueden verse las sentencias del Tribunal Constitucional STC 52/1983, de 17 de junio, y STC 13/1985, de 31 de enero.
STC 52/1983, de 17 de junio. BOE núm. 168, de 15 de julio de 1983. ECLI:ES:TC:1983:52. Disponible en: https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1983-19845.pdf .

Ediciones Universidad de Salamanca | CC BY-NC-ND

comunicación que difunde datos no suficientemente contrastados no comete ningún tipo de delito, por más que dicha información contribuya a generar confusión o falsas opiniones en los lectores. Estas conductas no son siempre delictivas, tan solo aquellas manifestaciones que atenten directa y manifiestamente contra el derecho a comunicar o recibir información veraz por cualquier medio de difusión, plasmado en el citado artículo de nuestra Carta Magna, tal y como recoge el Plan Estratégico contra la Cibercriminalidad de 2021[1191].

5. La *práctica imposibilidad de establecer un nexo causal entre el mensaje desinformador y los pretendidos cambios de opinión* de los ciudadanos que hacen suyo ese mensaje, llegando incluso a difundirlo ellos mismos como propio entre sus personas próximas y grupos de pertenencia. En este sentido, como señala Douglas Rushkoff:

> "No siempre es fácil determinar cuándo hemos renunciado a nuestro criterio y a la toma de decisión para entregárselos a otro. Cuanto mejor y más sofisticada es la manipulación, menos conscientes somos de ella" (RUSHKOFF, 2000, pág. 19)

6. El *aprovechamiento que la narrativa desinformadora hace de las vulnerabilidades detectadas en la sociedad* para penetrar profundamente en ella y alcanzar sus objetivos. Los actores de la amenaza no inician sus operaciones desde cero, sino que se dedican a aumentar y polarizar el debate social y político preexistente, por lo que resulta complejo acusar a estos actores de *provocar* crisis políticas o sociales cuando, ciertamente, su papel consiste en *distorsionar* los conflictos que ya están creados, intensificándolos, moderándolos o introduciendo nuevos elementos para variar su rumbo conforme a sus propios objetivos. En cierto modo este proceso se asemeja al de *dominación cultural*, donde, primeramente, se descubren los mitos dominantes en la población al tiempo que se va ganando su confianza, en segundo lugar se encuentran las supersticiones en sus creencias y, finalmente, se reemplazan o incrementan estas con hechos que modifiquen la percepción de la realidad o los valores del grupo (RUSHKOFF, 2000, pág. 160).
7. La *amplia aceptación de la desinformación en los medios de comunicación*, tanto digitales como tradicionales, *y su insondable capilaridad* que alcanza prácticamente a todo tipo de narrativa cotidiana -política, económica, social, cultural- que hace aún más complicado distinguir lo que forma parte del legítimo discurso de convicción de las técnicas de influencia con propósitos de injerencia maliciosa.
8. Y, finalmente, la *carencia de competencias sociales para detectar las narrativas desinformativas y la dificultad que conlleva su mitigación*, por el propio

STC 13/1985, de 31 de enero. BOE núm. 55, de 05 de marzo de 1985. ECLI:ES:TC:1985:13. Disponible en: https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1985-3609.pdf (17/11/2024).

[1191] No disponible en fuentes abiertas. Puede consultarse la nota de prensa de La Moncloa sobre la Instrucción 1/2021, del Secretario de Estado de Seguridad, por la que se aprueba el Plan Estratégico contra la Cibercriminalidad.

Ediciones Universidad de Salamanca | CC BY-NC-ND

compromiso institucional, político y social a medio y largo plazo que conlleva la alfabetización digital y mediática.

6.2.3. La categorización y la medición del impacto de las operaciones de influencia y desinformación desde la perspectiva europea

Cualquier investigación que pretenda alcanzar un conocimiento profundo sobre su ámbito de estudio necesita sistematizar la información que reciba para comprender los datos, poder compartirlos para mejorar su explotación y, con ello, aplicarlos a políticas o planes concretos de actuación. Dentro de este procedimiento de sistematización, la categorización y la definición de variables objetivas, replicables y verificables serán necesarias para poder atribuir valor y clasificar nuestros objetos de medición.

En este sentido, uno de los mayores desafíos en el análisis y comprensión de las campañas de desinformación es, precisamente, medir su impacto e influencia. Por lo tanto, si pretendemos caracterizar de manera adecuada este tipo de operaciones debemos conseguir estandarizar unas variables y unos procedimientos que todos comprendamos, tenemos que capitalizar el máximo rendimiento posible de toda la información de que dispongamos y, además, debemos trabajar con una gama de recursos interoperables para agilizar la aplicación práctica de la misma a través de la respuesta que demos a dicha amenaza.

Pero a ello hay que sumar otras dificultades propias de la Zona Gris. La primera de ellas es, una vez identificada la narrativa desinformadora, determinar qué fin pretende alcanzar con dicha maniobra el actor hostil. El segundo reto consiste en aplicar variables objetivas al análisis y la medición de su verdadero alcance, es decir, la influencia que haya podido tener en el destinatario. El tercer desafío pasa por la consideración de que, en el contexto geopolítico actual, las campañas de desinformación forman parte de estrategias más amplias orientadas a la consecución de objetivos complejos donde se entrecruzan intereses políticos, militares o económicos, entre otros. Finalmente, en cuarto lugar, los investigadores no podrán en la mayoría de las ocasiones tener un panorama completo de la operación de influencia por cuanto que, usualmente, cuando ésta sea detectada ya estará en un avanzado estadio de desarrollo, lo que implica trabajar con datos parciales y en constante evolución, lo cual afecta a la medición y catalogación del evento (NIMMO, 2020, págs. 2-3).

Esta tarea referida a la medición de impacto de las operaciones de influencia ha recibido diferentes soluciones como, entre otras, la *Breakout Scale* que basa su modelo en la tipificación de la amenaza dentro de una escala ascendente con seis categorías, cada una de las cuales está vinculada con un momento temporal en el proceso de evolución de la operación desinformativa de acuerdo a su capacidad de propagación a través del complejo ecosistema de difusión de la información -plataformas tecnológicas, redes sociales, medios de comunicación tradicionales, declaraciones políticas, etc.-. Para esta evaluación se utilizan dos conceptos clave: el *punto de inserción*, referido al medio en el que se origina la difusión, y el *momento de ruptura*, que define el salto de un medio a otro (NIMMO, 2020, págs. 3-5).

Ediciones Universidad de Salamanca | CC BY-NC-ND

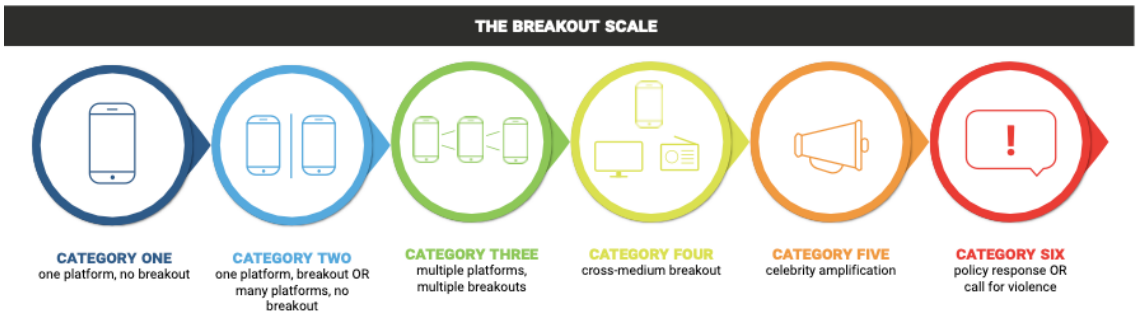


Imagen 6.2.
Escala del momento de ruptura (The Breakout Scale)
Fuente: Ben Nimmo, 2020

Dado el objetivo de nuestro estudio, cual es tratar de demostrar la vinculación de la desinformación con los efectos sobre la seguridad nacional en el marco de las democracias europeas y, en concreto, la española, atenderemos en este apartado específicamente a la respuesta que se le otorga desde la UE por dos motivos: primeramente, por el carácter avanzado del esquema europeo de evaluación de la amenaza desinformativa, su categorización y medición de impacto y, en segundo lugar, porque esto es lo que conviene a nuestro propósito último.

6.2.3.1. El ciclo de análisis FIMI: buscando un marco común de defensa

Desarrollar un marco analítico y una metodología comunes para recopilar, estudiar y categorizar la amenaza vinculada a la desinformación y a la manipulación e interferencia de información extranjera (FIMI)[1192] es uno de los objetivos del Servicio Europeo de Acción Exterior (SEAE) que, a través de su división StratCom[1193], publica en febrero de 2023 el *1st Report on Foreign Information Manipulation and Interference Threats: towards a framework for networked defence*[1194]. En este sentido, conviene resaltar el hecho de que el SEAE centra su trabajo de detección y análisis en la amenaza proveniente de actores externos, dado que carece de mandato para hacerlo sobre los de carácter interno. Por ello, la desinformación se entiende desde la perspectiva de manipulación informativa intencionada de origen externo[1195].

Sobre la base del estudio de los principales actores externos y las narrativas más activas durante un periodo de varios meses de 2022[1196], se propone una base conceptual y un

[1192] FIMI corresponde al acrónimo en inglés de Foreign Information Manipulation Interference
[1193] Ver referencia al Grupo de Comunicación Estratégica (StratCom) del SEAE en el Capítulo 3, apartado 3.3.3.
[1194] Primer Informe del SEAE sobre Amenazas de Manipulación e Interferencia de Información Extranjera: hacia un marco para la defensa en red. European Union External Action. Febrero de 2023. Disponible en: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en (28/09/2024).
[1195] La metodología FIMI, en cuanto al uso de sus patrones y parámetros de análisis, serían extrapolables al análisis de la desinformación de actores internos (hablaríamos entonces de DIMI, acrónimo de Domestic Information Manipulation Interference). De hecho, los análisis sobre narrativas desinformadoras y de manipulación de VIGINUM se basan en los patrones FIMI.
[1196] En concreto, durante los meses de octubre, noviembre y diciembre de 2022, se comprueba que los 100 casos de FIMI detectados se refieren a Rusia, en el marco de la guerra de agresión a Ucrania, y de

Ediciones Universidad de Salamanca | CC BY-NC-ND

marco analítico descentralizado e interoperable, con especial atención a la cooperación entre las partes interesadas, como elementos clave para tratar de alcanzar una comprensión integral de la amenaza. Pero el modelo no acaba en la detección de dicha amenaza sino que, también, apunta hacia las acciones de respuesta mediante el apoyo a la toma de decisiones políticas adecuadas, efectivas y proporcionadas.

En cuanto a la definición de lo que se entiende por *FIMI*, desde un primer momento se considera que:

> "Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory"[1197].

En este contexto se presenta el *marco analítico ABCDE* de las amenazas FIMI, que se sustenta en cinco parámetros básicos:

1) Los actores (*Actors*): La categorización de los objetivos pretendidos por los actores de la amenaza FIMI conforme a la denominada Clasificación 5D (*Dismiss, Distort, Distract, Dismay, Divide*)[1198].
2) El comportamiento (*Behaviour*): La metodología de parametrización de comportamiento de los actores a través de sus TTP (Tácticas, Técnicas y Procedimientos)[1199], entendiéndolo como un proceso con tres fases: planificación, preparación y ejecución. De esta manera, se analiza la *huella digital* vinculada al comportamiento particular de cada actor, que sin duda resulta clave a la hora de la identificación y atribución de sus acciones[1200].

China, respecto a su elaborada y compleja imagen erigida en el entorno informativo mundial a partir de su estrategia de expansión económica y militar.

[1197] "La Manipulación e Interferencia de Información Extranjera (FIMI) describe un patrón de comportamiento mayormente no ilegal que amenaza o tiene el potencial de impactar negativamente en los valores, los procedimientos y los procesos políticos. Dicha actividad es de naturaleza manipuladora y se ejecuta de manera intencional y coordinada. Los actores de tal actividad pueden ser de carácter estatal o no estatal, incluidos sus representantes dentro y fuera de su propio territorio" (Traducción propia). IBIDEM, página 25.

[1198] *Dismiss, Distort, Distract, Dismay, Divide* que se pueden traducir al español como Descartar, Distorsionar, Distraer, Consternar y Dividir. Primer Informe de Amenaza FIMI del SEAE, Op. Cit., página 12.

[1199] Las *tácticas* se corresponden con los objetivos que puede buscar el actor FIMI, como por ejemplo la división social ante un determinado hecho o la distorsión de éste conforme a sus propios intereses. Las *técnicas* equivalen a las diferentes formas en que pueden alcanzarse esos objetivos a lo largo de las tres fases del proceso FIMI, como por ejemplo la difusión de narrativas a través de redes sociales mediante la palabra, el uso de vídeos o imágenes modificadas por IA, la amplificación de esos contenidos a través de proxies, etc. Finalmente, los *procedimientos* podemos entenderlos como la huella digital concreta de un determinado actor, que lo caracteriza y permite identificarlo en el caso de que se vuelva persistente.

[1200] IBIDEM, página 13.

Ediciones Universidad de Salamanca | CC BY-NC-ND

3) El contenido (*Content*): El análisis del contenido del incidente FIMI para identificar las narrativas utilizadas por los actores y el contexto sociopolítico en el que se engloba[1201].
4) El grado (*Degree*): El estudio del grado de distribución de las narrativas a través del ecosistema de canales de información utilizados para propagarlas y el nivel de confianza que ostentan, distinguiéndose entre los denominados *canales atribuidos* y los *no atribuidos*[1202].
5) El efecto (*Effect*): La medición del efecto o impacto de un incidente FIMI a través de parámetros como el alcance de su difusión, el nivel de compromiso conseguido, el daño causado o la relación causal con cambios de comportamiento en el público objetivo, entre otros.

Una novedosa cuestión es la perspectiva *killchain*[1203] de las contramedidas FIMI que, en el marco de la *EU Hybrid Toolbox* creada al amparo de la Brújula Estratégica para la Seguridad y la Defensa, pretende romper el progreso de las fases consecutivas que conforman el comportamiento del actor de la amenaza, y que se visualiza a través de las TTP del incidente. En definitiva, lo que se busca es negarle al agresor la capacidad de perfeccionar su ataque *matando la cadena* del proceso que conlleva, desde la planificación de la agresión, su preparación y ejecución hasta la evaluación de efectos. De esta forma, las contramedidas FIMI están siempre activas y no es necesario esperar a que se produzca la agresión para empezar a implementarlas como gestión preventiva o anticipativa. Para que este enfoque *killchain* funcione se necesita, por un lado, el análisis objetivo de las TTP del actor de la amenaza para entender qué vulnerabilidades busca en el objetivo y, por otro, desarrollar respuestas sistemáticas que permitan evitar la perfección del ataque, medir la efectividad de los efectos causados y detectar los efectos secundarios no deseados[1204].

El enfoque *killchain* se construye sobre *DISARM*, una taxonomía independiente y de código abierto para combatir la desinformación mediante el análisis y la compartición de datos[1205] necesaria para la clasificación y análisis de las TTP en el *marco analítico ABCDE*, lo suficientemente ágil y abierta como para permitir su adaptación a las nuevas

[1201] En el citado informe se identifican narrativas rusas en el contexto de la guerra de agresión a Ucrania como: "Occidente es el agresor de Rusia", "Ucrania es el agresor de Rusia", "Las sanciones contra Rusia resultan contraproducentes", "Occidente es hipócrita" o "Ucrania es un Estado nazi y terrorista". IBIDEM, páginas 19 y 20.

[1202] Conforman los *canales atribuidos* los *canales de comunicación oficiales* -utilizados por el Estado y sus representantes para difundir contenidos-, los *canales controlados por el Estado* -medios afiliados oficialmente a un Estado- y los *canales vinculados al Estado* -medios cuya afiliación a un Estado no es reconocida oficialmente, pero que es confirmada por fuentes de inteligencia o servicios de información-. A estas tres categorías hay que añadir el amplio ecosistema de canales y redes de comunicación que interactúan de manera regular en los incidentes FIMI y que no están atribuidos a ningún actor estatal. IBIDEM, páginas 20, 21 y 22.

[1203] Puede traducirse *killchain* como "cadena de ataque".

[1204] Primer Informe de Amenaza FIMI del SEAE, Op. Cit., páginas 25 y 26.

[1205] DISARM, marco maestro de código abierto para combatir la desinformación a través del análisis de datos y su puesta en común con otros actores, de la Fundación del mismo nombre, se comenzó a utilizar por la OTAN en el año 2021 y, posteriormente, se acordó su utilización como el estándar de taxonomía aplicado a la manipulación informativa tanto por EE.UU. como por la UE. Disponible en: https://www.disarm.foundation/ (28/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

TTP que vayan surgiendo, al tiempo que suficientemente concreta para impulsar respuestas específicas a aquellas[1206].

El ciclo de análisis FIMI consta de cinco fases que, en su conjunto, componen un flujo de trabajo con un doble objetivo: a largo plazo detectar, analizar y contrarrestar la amenaza, y a corto plazo proporcionar datos que den soporte al ámbito decisor para que pueda poner en práctica respuestas rápidas y oportunas.



Imagen 6.3.
Ciclo de análisis FIMI
Fuente: 1º Informe FIMI del SEAE, 2023

La primera fase corresponde con la *monitorización estratégica*, que consiste en la adecuada selección de datos que nos permita comprender los patrones de comportamiento de los actores hostiles.

La segunda se refiere a la *priorización y triaje* para filtrar y categorizar los datos recogidos del entorno de información analizado[1207], priorizando los eventos de mayor relevancia para concentrar en ellos los recursos disponibles.

[1206] IBIDEM, páginas 29 y 30. La matriz DISARM para analizar los ataques de desinformación consta de múltiples TTP con dos tipos de indicadores básicos: el marco ROJO que detalla las fases del ataque, y el AZUL que señala las de la defensa. Disponible en: https://disarmframework.herokuapp.com (28/09/2024).
Un ejemplo práctico del uso de DISARM es el documento del Hybrid CoE de noviembre de 2022 titulado Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework DISARM. Disponible en: https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf (28/09/2024).
[1207] Canales de comunicación formales e informales, medios de comunicación tradicionales, plataformas tecnológicas, redes sociales, foros, etc.

Ediciones Universidad de Salamanca | CC BY-NC-ND

La tercera fase es la de *análisis de incidentes y recopilación de evidencias*, que conlleva la codificación de la información obtenida conforme a la taxonomía DISARM[1208] y su enfoque *killchain* de desinformación[1209], así como la preservación de pruebas para, desde una perspectiva forense, poder hacer una atribución -política o jurídica- y sustentar las acciones que se deriven contra el actor de la amenaza. En este sentido, resulta imprescindible disponer de un formato de datos ampliamente acordado que facilite la puesta en común y el intercambio de información y hallazgos sobre aspectos específicos detectados en los ataques, con el objetivo de aprovechar las lecciones aprendidas y, así, lograr un alto nivel colectivo en las contramedidas adoptadas contra la amenaza FIMI.

La cuarta fase del ciclo de análisis FIMI se trata de la *puesta en común y el intercambio de conocimientos* con las partes interesadas y, al mismo tiempo, con aquellos componentes que se encuentran en disposición de adoptar medidas de reacción inmediata frente al incidente detectado e identificado.

La última fase corresponde al *conocimiento de la situación* en base al impacto de las contramedidas adoptadas y las acciones derivadas, en un proceso que retroalimenta el propio ciclo de análisis para volver a iniciar la monitorización de nuevos canales, posibles actores o el estudio de patrones derivados del análisis de TTP compartidas por otros equipos de trabajo.

Pese a su solidez conceptual, la perspectiva presentada en el Primer Informe FIMI del SEAE adolece de una limitación, como ella misma señala, en cuanto que "*only refers to information manipulation by actors foreign to the EU and its member states, thus not applying to domestic sources*"[1210], cuestión con la que discrepamos profundamente puesto que supone una visión parcial que lastra al marco analítico en su conjunto al dejar fuera de su enfoque la perspectiva endógena de la amenaza que, como ya hemos expuesto anteriormente, es cuanto menos igual de grave que la foránea, si no más, en atención a las connotaciones domésticas que comporta[1211].

Esta inconsistencia hace que en enero de 2024 el SEAE publique un *2nd Report on Foreign Information Manipulation and Interference Threats: a framework for networked defence*[1212], que completa y perfecciona el marco analítico de defensa integral contra la FIMI, mediante la vinculación entre el análisis de riesgos y las contramedidas adaptativas

[1208] Esta taxonomía incluye la denominación del incidente y la fecha de inicio, el canal de detección, la narrativa que sustenta, el destinario del ataque, el supuesto autor de la amenaza, la vulnerabilidad instrumentalizada para el ataque, las TTP y las medidas adoptadas, entre otras.

[1209] La *killchain* de desinformación se estructura en cuatro fases -planificación, preparación, ejecución y evaluación- cada una de las cuales incluye diferentes tácticas y técnicas. Puede consultarse en el Primer Informe FIMI del SEAE, Op. Cit., página 29.

[1210] "Sólo se refiere a la manipulación de la información por parte de actores extranjeros a la UE y sus estados miembros, por lo que no se aplica a fuentes internas" (Traducción propia). IBIDEM, página 25.

[1211] Ver referencia a esta cuestión en el apartado 6.2.

[1212] Segundo informe del SEAE sobre Amenazas de Manipulación e Interferencia de Información Extranjera: un marco para la defensa en red. European Union External Action. Enero de 2024. Disponible en: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (29/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

frente a dicha amenaza. En el Prólogo del referido documento, el AR/VP Josep Borrell manifiesta que:

> […] "FIMI is closely connected to both hybrid threats and cyber threats and has become a crucial component of modern-day warfare […]. If information is manipulated, our society and the way we engage in public debate cannot work. If information becomes toxic, democracy cannot work"[1213].

A partir de este Segundo Informe el modelo se orienta más hacia la acción de *respuesta a la amenaza*, lo cual encaja perfectamente con el enfoque práctico que impone la Brújula Estratégica para la Seguridad y la Defensa (BESD)[1214], en cuyo contexto se crea la *EU Hybrid Toolbox* para dar cabida a la estrategia de lucha contra la FIMI:

> "5. Crearemos un conjunto de instrumentos de la UE contra las amenazas híbridas que reúna diferentes herramientas para detectar una amplia gama de amenazas híbridas y responder a ellas. En este contexto, desarrollaremos un conjunto de instrumentos específicos para hacer frente a la manipulación de información y la injerencia por parte de agentes extranjeros"[1215].

El análisis de actividad FIMI en el periodo de referencia del segundo Informe[1216] concluye los siguientes extremos de interés desde la perspectiva general de su permanente evolución y la consiguiente necesidad de adaptar la respuesta a las nuevas TTP detectadas:

1) Los objetivos de la amenaza FIMI son globales y se dirigen no solo a países sino, también, a organizaciones, instituciones y personas de relevancia pública.
2) Los actores de la FIMI aprovechan la actividad institucional y mediática[1217] de manera oportunista para proyectar sus narrativas a audiencias más amplias.
3) Los ataques FIMI utilizan canales de distribución coordinados y estrategias concretas para amplificar su difusión y alcance en la red[1218].
4) Por ahora la IA generativa no está siendo clave para el desarrollo de operaciones FIMI -lo cual no significa que pase a serlo en un corto espacio de tiempo-.

[1213] "La FIMI está estrechamente relacionada tanto con las amenazas híbridas como con las ciberamenazas y se ha convertido en un componente crucial de la guerra moderna[…]. Si se manipula la información, nuestra sociedad y la forma en que participamos en el debate público no pueden funcionar. Si la información se vuelve tóxica, la democracia no puede funcionar" (Traducción propia). Segundo Informe de Amenaza FIMI del SEAE. Op. Cit., página 2.

[1214] Ver apartado 3.3.3.

[1215] Una Brújula Estratégica para la Seguridad y la Defensa. Op. Cit., página 3 (versión en español). Disponible en: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf (29/09/2024).

[1216] Periodo que comprende desde diciembre de 2022 a diciembre de 2023.

[1217] Declaraciones públicas de jefes de Estado y de Gobierno, cumbres políticas, elecciones, situaciones de crisis y emergencias, incidentes militares de repercusión internacional, etc.

[1218] Una técnica utilizada para amplificar el contenido del mensaje desinformador a través de una variedad de canales y perfiles bajo una falsa apariencia de autenticidad es la conocida como *astroturfing*, una técnica de marketing que consiste en proyectar una imagen falsa de naturalidad y espontaneidad, simulando por ejemplo un debate entre diferentes personas con intereses legítimos y contrastados, con el fin de ganar apoyo y, con ello, que se viralice el mensaje mediante la difusión que hagan los propios receptores del mismo.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En clara consonancia con los objetivos que marca el *Plan de Acción para la Democracia Europea*, que señala la necesidad de arbitrar una respuesta global, estructurada y colectiva frente a la desinformación y la manipulación de la información proveniente no solo de actores extranjeros sino, también, de actores nacionales[1219], se presenta el *Marco de Respuesta FIMI* como nuevo pilar del sistema europeo de lucha contra la amenaza desinformativa, con tres líneas de desarrollo para su implementación:

1. La amenaza FIMI es compleja y multifacética por lo que la respuesta debe ser igualmente multinivel y adaptativa. Para ello se crea la *FIMI Toolbox* como el conjunto de múltiples instrumentos y medidas a corto, medio y largo plazo, incluidas en un sistema dinámico que permite su permanente adaptación a los cambios del entorno y que, al mismo tiempo, se complementa con la *EU Hybrid Toolbox*. Este elemento es clave, pues la interconexión operativa de los dominios es lo que permite utilizar sus capacidades en todo su potencial. Los instrumentos de respuesta que presenta la *FIMI Toolbox* se agrupan en cuatro dimensiones: 1) la referida a la toma de conciencia sobre la situación de amenaza; 2) el fomento de la resiliencia frente a ella; 3) la disrupción y regulación normativa que sustente la respuesta; 4) y la vinculación con la PESC y la acción diplomática de la UE[1220].
2. El desarrollo metodológico del Marco de Respuesta FIMI es adaptativo y se compone de tres elementos:
    a. El *enfoque holístico de la amenaza* y la necesidad de afrontarla desde la interoperabilidad de todas las fuentes de información al alcance para, de esta manera, generar inteligencia aplicable a la decisión sobre la respuesta.
    b. La complejidad de la amenaza FIMI exige un *catálogo abierto de contramedidas preventivas, reactivas y de resiliencia*, donde el estudio técnico de las TTP es clave para definir el tipo de ataque e identificar al autor, pero que necesita también del examen del componente sociocognitivo característico de la desinformación, cuestión diferencial respecto a la ciberdefensa.
    c. La efectividad y potencia del Marco de Respuesta FIMI se sustenta en la fuerza de la *comunidad de los defensores* -gobiernos, sector privado, sociedad civil, instituciones, academia, etc.- que comparten sus diferentes recursos, capacidades y competencias para, dependiendo del contexto global del ataque, poner en marcha las contramedidas que correspondan conforme a los procedimientos acordados, de manera ágil y coordinada. Para el adecuado funcionamiento de esta tela de araña es preciso impulsar de manera constante el establecimiento de vínculos entre posibles socios y disponer de procesos que permitan compartir la información en tiempo óptimo de respuesta.
3. La implementación práctica del Marco de Respuesta FIMI integra los procesos de análisis y respuesta sobre la base del intercambio continuo de información y

[1219] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción para la Democracia Europea. COM(2020) 790 final. Bruselas, 3.12.2020. Página 23. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423 (29/09/2024).
[1220] Segundo informe FIMI del SEAE. Op. Cit., página 14.

Ediciones Universidad de Salamanca | CC BY-NC-ND

la evaluación constante del sistema. Se estructura en cuatro fases: 1) la preventiva o de evaluación de riesgos; 2) la de establecimiento de prioridades para definir las contramedidas adecuadas; 3) la activación de la respuesta, 4) y una vez concluido el incidente, la recuperación a través de las lecciones aprendidas buscando dificultar ataques futuros.

Este Marco de Respuesta FIMI está perfectamente diseñado para su aplicación en incidentes relacionados con procesos electorales, de forma que el propio SEAE propone un flujo de trabajo para abordar la desinformación y la interferencia extranjera en estas situaciones, que analizamos en un apartado posterior[1221]. De hecho, esta es la metodología adoptada por prestigiosas instituciones como el Observatorio Complutense de Desinformación, que congrega a investigadores de todo el mundo para "explorar y entender el fenómeno de la desinformación, sus causas, consecuencias y antídotos"[1222], procurando dotar una respuesta híbrida de naturaleza institucional a dicha amenaza a través de sus informes y trabajos de observación electoral[1223].

La principal conclusión que podemos extraer del ciclo de análisis FIMI es que la garantía del éxito en la lucha contra la amenaza desinformativa requiere un esfuerzo conjunto y continuo en el tiempo, donde la fuerza del grupo de defensores consiste en su propia participación en el proceso y en la puesta en común de la información de que disponen para, de esta manera, tener una visión de conjunto de la amenaza para responder a ella de manera multidisciplinar y coherente. Por ello, se advierte que:

> "[…] To start preparing against FIMI in advance by building communities of purpose is the best means to minimize risk and to be ready for a potential intensification of threat activity around key election moments and beyond"[1224].

6.2.3.2. La aplicabilidad del Derecho Internacional a la FIMI

De acuerdo con esta estrategia de la UE frente a la amenaza desinformativa y la búsqueda de líneas de convergencia con la comunidad internacional, en noviembre de 2023 el SEAE publica su *Study on International Norms for Foreign Information Manipulation and Interference (FIMI)*[1225], cuyo propósito es analizar la aplicación de las normas de Derecho Internacional existentes a la manipulación e interferencia de información extranjera, partiendo del presupuesto de que no existen normas *ad hoc*.

[1221] Ver Capítulo 7, apartado 7.3.2.

[1222] Puede ampliarse información sobre el Observatorio Complutense de Desinformación en la página web de la Universidad Complutense de Madrid. Disponible en: https://www.ucm.es/observatoriodesinformacion/ (24/11/2024).

[1223] El Observatorio Complutense ha llevado a cabo trabajos de análisis de casos de desinformación en procesos electorales de diversos países como Argentina, Ecuador, Chile, México, España, Perú, Uruguay, Estados Unidos y en las elecciones del Parlamento Europeo de 2024.

[1224] "Comenzar a prepararse previamente contra la amenaza FIMI mediante la creación de comunidades de propósito es la mejor forma de minimizar el riesgo y de estar preparados para una posible intensificación de la actividad de la amenaza en momentos clave del proceso electoral y más allá" (Traducción propia). Segundo Informe de Amenaza FIMI del SEAE. Op. Cit., página 34.

[1225] Estudio sobre el desarrollo de normas internacionales específicas para FIMI. European Union External Action. Noviembre de 2023. Disponible en: https://www.eeas.europa.eu/eeas/study-international-norms-foreign-information-manipulation-and-interference-fimi_en (28/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Este compendio normativo internacional va más allá de la FIMI y cubre el amplio espectro de las *operaciones de información* entre Estados, donde el ciberespacio cobra especial protagonismo como ámbito operacional[1226]. El punto de partida en este sentido está claro por cuanto el propio texto señala que:

> "International law does not have a specific set of rules or principles tailored to FIMI or other information operations. Though some have proposed the adoption or consideration of an 'international law for information operations' (ILIO), especially by the adoption of a treaty on the matter, States are yet to agree on such a legal framework […]. However, the lack of a specific legal regime for information operations does not mean that these exist in a legal vacuum. Quite the contrary: existing international law, as a whole, continues to apply to information operations, just as it applies to other online phenomena, to the extent relevant"[1227].

Una aproximación a los principios jurídicos cardinales que conforman el Derecho Internacional y el estudio sobre su aplicabilidad para combatir la amenaza FIMI permite extraer varias conclusiones:

1. En cuanto al *principio de soberanía de los Estados* aplicado al ámbito digital y a las operaciones de influencia y FIMI[1228], únicamente será conculcado, como regla general, en el supuesto de que exista una acción de Estado que cause efectos en el territorio de otro, origine daño funcional a las infraestructuras cibernéticas o interfiera en las funciones inherentemente gubernamentales[1229].
2. Respecto al *principio de no intervención en los asuntos de otro Estado*, éste cubre únicamente las formas coercitivas de interferencia, aplicadas no solo al uso de la fuerza militar sino, también, a otras formas indirectas de coerción, como por ejemplo el apoyo a actividades subversivas del orden interno de otro Estado, a la interferencia en el libre acceso a la información por los ciudadanos de aquel o, desde luego, la propagación de desinformación que limite el pleno desarrollo de sus políticas internas o externas y la libertad de decisión que las gobierne[1230].
3. El *principio de diligencia debida* conlleva una serie de obligaciones de responsabilidad que, aplicadas a las relaciones entre Estados en el ciberespacio y el ámbito FIMI, implican que dicho concepto sea vulnerado por aquel actor estatal que no tome medidas para evitar las operaciones de influencia o

[1226] Ver referencia a esta cuestión en el apartado 5.3.

[1227] "El Derecho Internacional no tiene un conjunto específico de normas o principios adaptados a la FIMI u otras operaciones de información. Aunque algunos han propuesto la adopción o consideración de un "Derecho Internacional para las operaciones de información" (ILIO), especialmente mediante la adopción de un tratado al respecto, los Estados aún no han acordado dicho marco legal […]. Sin embargo, la falta de un régimen legal específico para las operaciones de información no significa que exista en un vacío legal. Todo lo contrario: el Derecho Internacional existente, en su conjunto, sigue aplicándose a las operaciones de información, así como a otros fenómenos en línea, en la medida en que sean relevantes" (Traducción propia). Estudio sobre el desarrollo de normas internacionales específicas para FIMI, Op. Cit., página 9.

[1228] Ver a este respecto el apartado 1.1.2.

[1229] Estudio sobre el desarrollo de normas internacionales específicas para FIMI, Op. Cit., páginas 9 y 10.

[1230] IBIDEM, páginas 10 y 11.

Ediciones Universidad de Salamanca | CC BY-NC-ND

desinformación que, desde su territorio o soporte de infraestructuras, afecte a los derechos de otro Estado, de las personas o el medio ambiente[1231].

4. La obligación de los Estados con respecto al *Derecho Internacional de los Derechos Humanos* aplica al ámbito del ciberespacio y, por ello, también opera para restringir las acciones de FIMI. En este sentido, el Pacto Internacional de Derechos Civiles y Políticos[1232] protege en su artículo 19 contra la interferencia ilegal de los Estados en la libertad de expresión e información y, por ende, en la participación en los procesos democráticos[1233]. De igual manera, en el artículo 20 prohíbe la propaganda de guerra y la incitación a la discriminación, la hostilidad o violencia[1234]. De ahí la obligación de los Estados de proteger activamente a las personas frente a la FIMI y las operaciones de influencia.
5. De igual manera, el *Derecho Internacional Humanitario* aplicable a las operaciones militares cinéticas tanto en el ámbito físico como en el ciberespacio, es relevante para las operaciones de FIMI y desinformación obligando, por ejemplo, a los Estados a impedir y abstenerse de la difusión de cualquier tipo de información que promueva la violación del DIH o siembre el terror entre la población, entre otras[1235].
6. Por lo que se refiere a la *responsabilidad internacional del Estado*, éste lo será si participa activamente en una operación de manipulación de la información o de FIMI, o si no toma las medidas necesarias para prevenirla o mitigarla. Por su parte, el Estado perjudicado por tales interferencias podrá responder a esta agresión ilícita tomando contramedidas proporcionadas contra el Estado actor[1236].

Conforme a este análisis de los principios fundamentales que conforman el Derecho Internacional, y visto que su interpretación extensiva al ámbito del ciberespacio es el camino hacia el deseable establecimiento de un cuerpo normativo específico para regular la FIMI y las operaciones de información que amenacen la paz y la seguridad internacionales, la Unión Europea hace un llamamiento de cooperación a los Estados con el objetivo de conseguir establecer un acuerdo de conformidad que permita, entre

[1231] IBIDEM, páginas 11 y 12.

[1232] Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Disponible en: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (29/09/2024).

[1233] Pacto Internacional de Derechos Civiles y Políticos, Op. Cit., artículo 19: "1) Nadie podrá ser molestado a causa de sus opiniones. 2)Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 3) El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas".

[1234] IBIDEM, artículo 20: "1) Toda propaganda en favor de la guerra estará prohibida por la ley. 2) Toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley".

[1235] Estudio sobre el desarrollo de normas internacionales específicas para FIMI, Op. Cit., página 14.

[1236] IBIDEM, página 15.

Ediciones Universidad de Salamanca | CC BY-NC-ND

otros, enjuiciar el uso de la FIMI con fines terroristas, impedir el uso de la IA para el desarrollo de operaciones de información ilegales o que afecten a sectores críticos, impulsar la implementación de marcos de análisis como ABCDE y DISARM para contrarrestar las TTP identificadas y atribuidas a actores estatales, y compartir información sobre ellos para determinar las contramedidas aplicables.

Desde el convencimiento de que los riesgos y daños generados por las actividades FIMI se encuentran en el ámbito de aplicación del Derecho Internacional, se distinguen tres pilares clave de las normas FIMI:

1. Aquellas *normas que fijen qué tipo de actividades FIMI legales pero dañinas deben abordarse*, y qué contramedidas son aplicables a las mismas. Respecto a las primeras, se conviene que tanto los actores estatales como los no estatales deben prevenir y reparar todo tipo de manipulación de la información que cause daños físicos o no físicos significativos en el territorio o las infraestructuras de otro Estado, como consecuencia de la propia actividad FIMI o por los medios o métodos empleados. En cuanto a las contramedidas, se señala la legislación nacional para la protección de datos, las estrategias de ciberseguridad, la habilitación de marcos analíticos como ABCDE y DISARM, la cooperación internacional y los acuerdos institucionales a nivel nacional e internacional[1237].
2. *Normas referidas a la regulación del FIMI potencialmente ilegal*, que supondría la obligación de los Estados de abstenerse de aquellas acciones de manipulación de la información que causen daños a otro Estado o que socaven sus funciones inherentemente gubernamentales, que interfieran en sus asuntos de orden interno o externo, que infrinjan los derechos humanos o el DIH o, incluso, socaven los derechos de otros Estados o causen daño a sus ciudadanos a través de, por ejemplo, la difusión de propaganda o desinformación[1238].
3. *Normas aplicables al FIMI manifiestamente ilegal* según el Derecho Internacional, como la propaganda de guerra o que induce el conflicto civil en otro Estado, el proselitismo del odio en cualquiera de sus formas, la discriminación o la violencia, la incitación al genocidio o la instigación para cometer delitos internacionales[1239].

Podemos de esta manera afirmar que las normas de Derecho Internacional aplicables a la FIMI deben tener en consideración no solo la forma en que se ejecuta la amenaza desinformativa sino, también, la evaluación de otros factores como la autoría, el contenido de la acción, los efectos alcanzados y los objetivos pretendidos, entre otros, y siempre desde la consideración de que en el centro de todo ello se encuentra la protección de los derechos a la libertad de expresión y libre acceso a la información de los ciudadanos.

De otra forma se perdería gran parte del camino avanzado por los Estados democráticos en relación con la protección y salvaguarda de los derechos y libertades de los ciudadanos, a cuenta de articular una respuesta efectiva frente a dicha amenaza.

[1237] IBIDEM, páginas 22 y 23.
[1238] IBIDEM, páginas 23 y 24.
[1239] IBIDEM, página 24.

Ediciones Universidad de Salamanca | CC BY-NC-ND

6.3. Conclusiones: la Zona Gris en expansión

Como hemos comprobado, la Zona Gris conforma un espacio impreciso entre la paz y la guerra consustancial a las relaciones de poder, caracterizado por su ambigüedad, la naturaleza híbrida, asimétrica y gradual de su rango operacional, y el definido enfoque que sostiene hacia la población civil para la consecución de sus objetivos.

Los protagonistas usuales del conflicto en la Zona Gris suelen ser los Estados, especialmente aquellos de carácter revisionista y autocrático, pero la llegada del siglo XXI ha traído consigo nuevos actores no estatales, conocidos como *proxies*, que difieren el enfrentamiento entre aquellos en base a intereses propios y diversos -económicos, políticos, ideológicos, tácticos, etc.-.

En todo caso, los fines perseguidos serán de alta relevancia estratégica para el actor de la agresión, de forma que compensen los medios empleados, los cuales tendrán un elevado componente multidimensional por cuanto supondrán el recurso coordinado, integral y gradual de toda herramienta o instrumento de poder a su alcance. Por ello, el control de la escalada en la estrategia híbrida es pieza clave para determinar la fase en la que se encuentra la agresión y, conforme a ella, colegir la respuesta aplicable que permita recuperar el control de la situación. No obstante, la dificultad para detectar la agresión en la Zona Gris, la delicada coyuntura en la que debe aplicarse la medida disuasoria y la exigencia de un enfoque holista y multidisciplinar de la estructura operativa de respuesta, no facilita la gestión de las opciones de réplica sin escalar la tensión ante un ataque híbrido.

En este contexto la desinformación, aupada a manos de la tecnología y la globalización, se postula como el nuevo alter ego de la amenaza híbrida, con una afectación directa a la calidad de la convivencia, a la salud del sistema democrático y a la seguridad nacional de los Estados a través de la desafección ciudadana que genera, el desgaste institucional que supone y el fomento de posturas intolerantes, radicales y de odio que instaura desde todo tipo de narrativas manipuladas que, bajo una falsa apariencia de progreso y respeto a la igualdad, oculta peligrosas consignas populistas y de adoctrinamiento social.

Detrás de la amenaza desinformativa pueden encontrarse agentes exógenos o, lo que es peor, endógenos, que escarban sutilmente en los dilemas internos de la sociedad que les cobija y ahondan las grietas que socavan los pilares de la democracia que, paradójicamente, vela por sus derechos y libertades que éstos instrumentalizan para atacarla.

Por todo ello, la respuesta a esta grave amenaza solo puede afrontarse como un gran compromiso compartido donde todos los agentes involucrados, de carácter público y privado, intervengan en el marco de una estrategia institucional y de carácter global que debe tener como puntos bifocales de su actuación, en primer lugar, la alfabetización mediática de los ciudadanos con el objetivo de fomentar su pensamiento crítico y la participación en la democracia y, en segundo lugar, la regulación normativa para la protección de sus derechos y libertades, por encima de intereses particulares, por muy elevados o ventajosos que estos puedan llegar a ser, con especial atención al uso de

Ediciones Universidad de Salamanca | CC BY-NC-ND

algoritmos y las obligaciones de transparencia y rendición de cuentas de las plataformas digitales.

Únicamente desde la comprensión de la verdadera naturaleza de la democracia, con sus debilidades y fortalezas, puede abordarse la estrategia de defensa frente a la desinformación, que requiere un enfoque holista de la seguridad y de las conexiones con los principios y valores que sustentan aquella, para no caer en excesos que puedan encubrir censuras o quiebras de derechos inapelables como la libertad de expresión o la libertad de información (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 186).

Un ejemplo es el Pacto Internacional de Derechos Civiles y Políticos, de diciembre de 1966[1240] que en su artículo 19 ya protege contra la interferencia ilegal de los Estados en la libertad de expresión e información y, por ende, en la participación en los procesos democráticos, pero que señala en su párrafo 3 una importante limitación al respecto:

> "1. Nadie podrá ser molestado a causa de sus opiniones.
> 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
> 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:
> a) Asegurar el respeto a los derechos o a la reputación de los demás;
> b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas".

Conforme a ello, los Estados pueden limitar estos derechos privados relacionados con la comunicación en orden a proteger sus valores e intereses, como la seguridad nacional o el orden público, pero con estrictas condiciones: la legalidad conforme al cuerpo jurídico y normativo existente, la legitimidad de los objetivos perseguidos por dicha limitación, la necesidad del medio adoptado para preservar ese interés superior del Estado, y la proporcionalidad del mismo conforme a la entidad del bien jurídico lesionado.

Sin duda, la democracia necesita de la verdad para vivir y la desinformación supone un ataque a su corazón, por lo que la ciudadanía debe comprometerse con la salud de este sistema que le protege y permite desarrollarse con seguridad y en libertad.

Estos valores se explican por sí mismos pero necesitan de nuestro compromiso diario para mantenerse vivos. Por eso, como dijo Arsenio Escolar en la II Jornada contra la Desinformación del Club Abierto de Editores, celebrada en octubre de 2024, que el periodismo, la política, las plataformas digitales, las redes sociales y la ciudadanía tienen

[1240] Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Disponible en: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (12/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

que preguntarse qué pueden hacer cada uno de ellos para que "este preocupante fenómeno de la desinformación no acabe con la democracia"[1241].

[1241] Presentación de Arsenio Escolar, presidente del Club Abierto de Editores (CLABE), durante la II Jornada contra la Desinformación, celebrada el 14 de octubre de 2024 bajo el título "Comprometidos con la verdad". Disponible en: https://clabe.org/2024/10/15/intervencion-arsenio-escolar-ii-jornada-contra-la-desinformacion/ (20/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 7. LA ESTRATEGIA DE LA UNIÓN EUROPEA FRENTE A LA AMENAZA DESINFORMATIVA

Habiendo ya presentado la Zona Gris (ZG) como el espacio de relación entre Estados, impreciso y ambiguo, donde los límites de la guerra y la política se tergiversan conscientemente para alcanzar objetivos estratégicos recurriendo a acciones híbridas, de manipulación encubierta, con fines desestabilizadores y hostiles, corresponde ahora focalizar nuestro estudio en la forma en que se desenvuelve en este complejo entorno la UE y, en el siguiente Capítulo, nuestro país como ámbito principal de referencia.

Partiendo de que en este contexto de confrontación *pacífica* y de proyección de influencia *soterrada* van a interactuar todos los instrumentos de poder del Estado y que la ciudadanía será objetivo central de la estrategia de la información, la supervivencia de los valores y principios democráticos en liza va a exigir la asistencia mutua basada en la solidaridad europea junto con un firme y decidido compromiso con la protección de los derechos fundamentales, en particular con la libertad de expresión y la libertad de opinión en lo relativo a la lucha contra la desinformación y la injerencia extranjera, tal y como puso de manifiesto la Presidenta de la Comisión Europea, Úrsula Von der Leyen, en su discurso para la reunión del Foro Económico Mundial, celebrado en enero de 2024 en la ciudad suiza de Davos[1242]. Un año más tarde, el Foro se sigue mostrando altamente preocupado ante la amenaza desinformativa, la cual ocupa el cuarto puesto en el panorama de riesgos actuales a nivel mundial y se posiciona como el primero en el corto plazo, tal y como indica su Directora Gerente, Saadia Zahidi, en el prólogo de *The Global Risks Report 2025 – 20th Edition*, en el que señala:

> "Polarization within societies is further hardening views and affecting policy-making. It also continues to fan the flames of misinformation and disinformation, which, for the second year running, is the top-ranked short- to medium-term concern across all risk categories. Efforts to combat this risk are coming up against a formidable opponent in Generative AI-created false or misleading content that can be produced and distributed at scale" (World Economic Forum, 2025, págs. 4-12)[1243].

[1242] Úrsula Von der Leyen elevaba el tono de la alerta frente a este tipo de amenaza global y se refería a que "la preocupación principal durante los próximos dos años no son los conflictos o el clima, sino la desinformación y la información incorrecta, seguido de la polarización en nuestras sociedades". Disponible en: https://www.eldebate.com/internacional/20240117/von-der-leyen-davos-preocupacion-principal-durante-proximos-dos-anos-desinformacion_167647.html (22/10/2024).

[1243] "La polarización de las sociedades está radicalizando aún más las posturas y afectando a la formulación de políticas. También sigue avivando las llamas de la información errónea y la desinformación que, por segundo año consecutivo, es la principal preocupación a corto y medio plazo en todas las categorías de riesgo. Los esfuerzos para combatir este riesgo se están enfrentando a un oponente formidable, a través del contenido falso o engañoso creado por IA generativa, el cual se puede producir y distribuir a gran escala" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

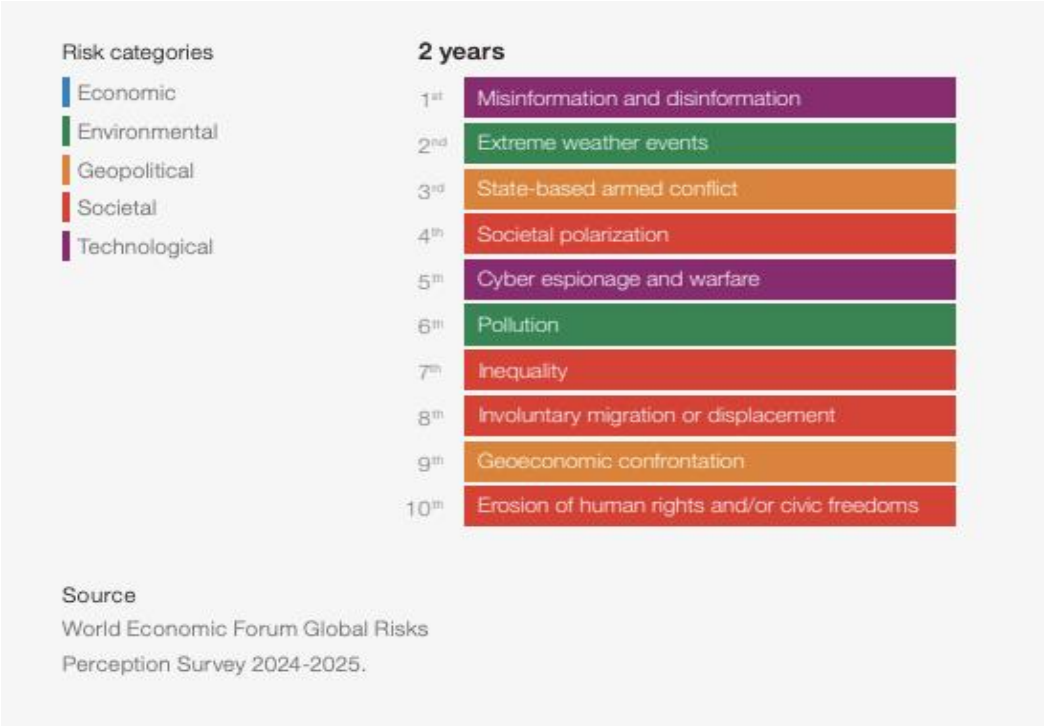


Gráfico 7.1.
Encuesta de percepción de riesgos globales 2024-2025
Fuente: World Economic Forum Global Risks Report 2025

Serán por ello necesarias medidas estratégicas y proactivas de amplio recorrido, ampliamente consensuadas y respaldadas inequívocamente por todos los EEMM de la Unión, en estrecha colaboración con sus aliados noratlánticos y el resto de actores internacionales alineados con el Derecho Internacional en el marco de NNUU, para contrarrestar las amenazas híbridas y las injerencias de terceros Estados autocráticos en los procesos políticos y electorales que buscan atacar la base misma de las democracias liberales. Llegados a este punto, no solo se trata de fijar la amenaza en el punto de mira, sino también de avanzar en su comprensión y entendimiento, de aprender a identificarla e, indudablemente, de concienciar a los ciudadanos en cuanto a la gravedad de su impacto para, de esta forma, mejorar la eficacia en la respuesta, puesto que:

> "Enfrentar las estrategias híbridas se ha convertido en un objetivo prioritario para las democracias liberales. Para desarrollar capacidades eficaces de prevención, disuasión, detección o respuesta, es necesario un completo entendimiento de sus fines, modos y medios de actuación" (GUTIÉRREZ DE LEÓN, 2022).

7.1. La movilización de políticas e instrumentos de colaboración internacionales y europeos contra las amenazas híbridas

Resulta conveniente en este punto recordar que, de acuerdo a lo estudiado en el Capítulo 3, la UE es un mecanismo supranacional de integración, tanto en el ámbito normativo como decisional, donde prima el enfoque constitucional sobre el de carácter internacional que, a la postre, determina que la seguridad y defensa europea sean una

Ediciones Universidad de Salamanca | CC BY-NC-ND

parte primordial "de ese proyecto político que, como en cualquier Estado, cuenta de forma expresa o implícita con la irreductible necesidad de prever su propia defensa como faceta inherente a su naturaleza soberana" (COELLO DE PORTUGAL, 2024, pág. 95).

Dicho lo cual, debemos convenir que, dado el carácter de nuestra investigación, es necesario referirse a la respuesta que se propone frente a las amenazas híbridas desde NNUU y la OTAN para, posteriormente, analizar la respuesta europea como paso previo al análisis de su estrategia contra la desinformación.

7.1.1. Las Naciones Unidas frente al desafío híbrido

La diplomacia como herramienta vinculada al arte de gobernar que se consolida a partir de la Paz de Westfalia de 1648, base de las relaciones internacionales modernas inspiradas en el reconocimiento del Estado como único actor y representante formal de las naciones, y la lógica evolución hacia la necesidad de encontrar respuestas coordinadas y cooperativas en el marco de esas relaciones internacionales, han sido una constante desde comienzos del siglo XX, cuando se pacta la Sociedad de las Naciones[1244] con el objetivo de promover el compromiso de los países para lograr la paz y la seguridad internacionales sin recurrir a la guerra, legado que recoge la Carta de las Naciones Unidas en el contexto de la Guerra Fría, soportada en el equilibrio del poder bilateral que representan en ese momento EE.UU y la URSS.

Pero al mismo tiempo, y precisamente por ello, la consecución de este vasto desafío ha supuesto un frente de dificultades debido al conflicto de intereses que nace del hecho de tratar de aunar voluntades en busca de un beneficio global dejando de lado las posibles ventajas particulares, las cuales vienen determinadas por el complejo entramado geopolítico propio de cada nación en cada momento histórico. Este modelo de cooperación y armonización de respuestas frente a las amenazas compartidas representa, sin lugar a dudas, el *santo grial* de las diferentes organizaciones internacionales y estructuras supranacionales que, en el ámbito noroccidental, han liderado la política mundial en los últimos ciento veinticinco años.

En este sentido, en la primera parte del Capítulo 2 analizábamos los problemas sistémicos que NNUU afronta para hacer valer su papel de árbitro de la seguridad internacional y que se mantienen vigentes casi ochenta años después de la firma de la Carta de San Francisco[1245]. No obstante, convenimos que la Organización atesora en su haber unos niveles sin precedentes de cooperación internacional que han permitido la toma de conciencia sobre la innegable vigencia del multilateralismo como única vía para alcanzar mayores cotas de igualdad, resiliencia y sostenibilidad del mundo. La perspectiva integral de la seguridad que en 1994 comienza a construir NNUU sobre el concepto de la *seguridad humana* y su firme compromiso con la ciberseguridad, que ya

[1244] Ver la introducción del Capítulo 2.

[1245] Ver apartado 2.1.3., en el que se exponen cuestiones limitativas para el desempeño de este rol como el relativo compromiso de los Estados con el Derecho Internacional, el efecto en las relaciones internacionales que generan los arsenales armamentísticos y nucleares, o las servidumbres estructurales y la naturaleza instrumental de las NNUU, entre otras.

Ediciones Universidad de Salamanca | CC BY-NC-ND

en 2011 identifica como problema global que únicamente puede afrontarse desde la confianza y la cooperación internacional[1246], le llevan a considerar que los principios jurídicos del Derecho Internacional, ideados en clave analógica, son aplicables en el quinto dominio mediante la correspondiente interpretación de sus normas.

Sin embargo, como comprobamos en el Capítulo 5[1247], no parece ser esta una cuestión aceptada unánimemente por todos los actores interesados, en cuanto que en el seno de las NNUU existen dos posturas diametralmente opuestas al respecto: la que sostienen EE.UU. y la UE, valedores de dicha tesis, y la de aquellos otros como Rusia y UK, para los que el cuerpo normativo internacional no debe aplicarse tal cual al ciberespacio, sino que se necesita del acuerdo específico entre Estados para precisar la interpretación y adaptación de los conceptos jurídicos internacionales a cada caso concreto que se plantee en el ámbito digital. Probablemente sea esta una diatriba que se alargue en el tiempo más de lo deseado, a tenor del recibimiento anticipado por Rusia al primer Proyecto de Convención de las NNUU contra la Ciberdelincuencia elaborado por el Comité Especial creado *ad hoc* en el seno de NNUU[1248], y presentado en agosto de 2024 tras casi cinco años de negociaciones[1249].

Otro de los retos que afronta NNUU en este contexto de Zona Gris es, sin duda, la adecuada gestión de las operaciones de paz en las situaciones de emergencia compleja donde se conjugan factores económicos, de desestabilización política y de estructuras institucionales, de crisis sanitarias y éxodos migratorios obligados, entre otros, que exigen actuar en varios frentes de manera simultánea como son la acción humanitaria[1250] y el uso de la fuerza armada, junto con otros mecanismos como la diplomacia de alto nivel o la actuación de unidades policiales que permitan contrarrestar las nuevas formas de amenaza no tradicional que impiden la restauración de la paz (COSTIGAN & HENNESSY, 2024, págs. 54-55).

Igualmente, la respuesta de las NNUU a las amenazas híbridas y, en concreto, la desinformación, se enfrenta a desafíos propios de su consideración universal que la convierten, aún más si cabe, en un reto sin parangón por la implicación del Derecho Internacional que conlleva, la amplitud de su finalidad por la evidente afectación a los derechos y libertades fundamentales[1251], y por el hecho de que algunos de sus miembros más cualificados son reconocidos promotores de esta amenaza. Por ello, cobra especial

[1246] Ver apartado 2.1.4., donde se refiere la reunión del Consejo Económico y Social de NNUU (ECOSOC) en el año 2011 en Nueva York.
[1247] Ver apartado 5.3.
[1248] Proyecto de Convención de las NNUU contra la Ciberdelincuencia elaborado por el Comité Especial creado *ad hoc* en el seno de NNUU. Disponible en: https://ciberprisma.org/wp-content/uploads/2024/08/v2405509-espanol.pdf (05/09/2024).
[1249] Rusia, que inicialmente apoyó la redacción de un Tratado en el seno de las NNUU que expresamente recogiese la interpretación de la ciberdelincuencia en al ámbito internacional, no recibe con agrado el texto presentado. Amplia repercusión en prensa. Disponible en: https://efe.com/mundo/2024-08-09/naciones-unidas-primer-tratado-ciberdelincuencia/
https://www.rtve.es/noticias/20240809/naciones-unidas-aprueba-su-primer-tratado-contra-ciberdelincuencia/16213537.shtml (21/08/2024).
[1250] Acción humanitaria referida a la provisión de bienes y servicios básicos y la protección de las víctimas.
[1251] Derechos que afectan a participación política y los procesos electorales, a la defensa de las minorías, a la salud de las personas, al cambio climático, a las migraciones y la educación, entre otros.

Ediciones Universidad de Salamanca | CC BY-NC-ND

relevancia el informe de su Secretario General, de 2022, titulado *Contrarrestar la desinformación para promover y proteger los derechos humanos y las libertades fundamentales*[1252], por cuanto sostiene el necesario enfoque multifacético de la lucha contra las estrategias desinformativas por parte de los Estados al tiempo que aboga por una respuesta basada en el respeto de los derechos humanos, con especial atención a la libertad de expresión de las personas y la libertad de buscar, recibir y difundir información consagradas en el artículo 19 de la Declaración Universal de Derechos Humanos[1253] y los apartados 1 y 2 del artículo 19 del Pacto Internacional de Derechos Civiles y Políticos[1254]. Es por ello que, específicamente, se determine que:

> "Los Estados tienen un papel crucial que desempeñar en la lucha contra los efectos de la desinformación, tanto en lo que respecta a sus propias acciones como en lo relativo a su deber de protección contra los abusos de derechos humanos por parte de terceros, incluidas las empresas comerciales. Dar una respuesta al polifacético fenómeno de la desinformación es una tarea compleja. Las normas de derechos humanos y de libertad de expresión, desarrolladas a lo largo del tiempo, proporcionan una orientación adecuada para los retos que plantea la desinformación, pues establecen señales normativas para que una ciudadanía bien informada participe en los procesos democráticos. Al crear las condiciones para que florezcan los derechos humanos, el pluralismo y la tolerancia, los Estados pueden contribuir a reducir los riesgos asociados a la desinformación"[1255].

Íntimamente relacionada con la anterior, se publica en 2023 las *Directrices de la UNESCO para la gobernanza de las plataformas digitales*[1256], que pretende la salvaguarda de la libertad de expresión y del derecho de acceso a la información "mientras se aborda la desinformación, el discurso de odio y las teorías de conspiración"[1257] por parte de la gran multiplicidad de partes interesadas, entre las que se encuentran los Estados, las plataformas digitales, las organizaciones intergubernamentales, la sociedad civil, los medios de comunicación, la academia y otros actores con competencias específicas -tecnológicas, digitales o investigativas-.

[1252] Contrarrestar la desinformación para promover y proteger los derechos humanos y las libertades fundamentales. Informe del Secretario General de Naciones Unidas. Asamblea General. 12 de agosto de 2022. A/77/287. Disponible en: https://documents.un.org/doc/undoc/gen/n22/459/27/pdf/n2245927.pdf (23/11/2024).

[1253] "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

[1254] "1) Nadie podrá ser molestado a causa de sus opiniones. 2) Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".

[1255] Informe del Secretario General de Naciones Unidas, Op. Cit., página 7/22.

[1256] Directrices para la gobernanza de las plataformas digitales: salvaguardar la libertad de expresión y el acceso a la información mediante un enfoque de múltiples partes interesadas. Publicado en 2023 por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000387360 (23/11/2024).

[1257] Ibidem, página 3.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En la misma línea se presenta también en 2023 el *Informe de políticas de Nuestra Agenda Común 8: integridad de la información en plataformas digitales* de las Naciones Unidas[1258], en el que se resalta la importancia crucial de estas plataformas en el control de la integridad de la información y su impacto en las interacciones sociales, políticas y culturales a nivel global, refiriendo para ello unos principios que conforman un Código de Conducta "that will help to guide Member States, the digital platforms and other stakeholders in their efforts to make the digital space more inclusive and safe for all, while vigorously defending the right to freedom of opinion and expression, and the right to access information"[1259].

Este conjunto de directrices e informes sustentan un año después, en junio de 2024, el documento referido a los *Principios globales de las Naciones Unidas para la integridad de la información*[1260] en el que se identifican las claves del ecosistema de la información en la era digital: 1) confianza y resiliencia de la sociedad; 2) incentivos positivos para evitar la proliferación de la desinformación; 3) empoderamiento de los usuarios en línea; 4) garantía de la independencia, la libertad y la pluralidad de los medios de comunicación; y 5) la transparencia del entorno de la información y el decidido compromiso tanto público como privado con la investigación y el avance de las tecnologías en este marco de respeto de derechos fundamentales.

Para lograr el éxito en la aplicabilidad y el respeto de estos principios aseguradores de la integridad de los espacios de información, se hace un llamamiento a los diferentes actores implicados[1261] proponiendo a cada uno de ellos una serie de recomendaciones para operativizar esos principios. Es de destacar que son las empresas tecnológicas las que más recomendaciones reciben -hasta veintidós- con una doble prioridad: la transparencia de sus tecnologías y la revaluación del modelo de negocio actual sustentado en la publicidad dirigida. Seguidamente son los Estados los que más propuestas de acción reciben -doce-, como máximos responsables de respetar, proteger y promover los derechos humanos, en particular la libertad de expresión y el acceso a la información. Por su parte, NNUU se compromete a intensificar su esfuerzo para reforzar la integridad de la información en el ámbito de la comunidad internacional, apoyar las iniciativas de desarrollo de capacidades de los Estados, promover estos Principios Globales, facilitar recursos y apoyar planes de acción multilaterales en este sentido.

[1258] Our Common Agenda Policy Brief 8: Information Integrity on Digital Platforms. June 2023. Disponible en: https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf (23/11/2024).

[1259] "que ayudará a guiar a los Estados Miembros, las plataformas digitales y otras partes interesadas en sus esfuerzos por hacer que el espacio digital sea más inclusivo y seguro para todos, al tiempo que se defiende enérgicamente el derecho a la libertad de opinión y expresión y el derecho de acceso a la información" (Traducción propia). Ibidem, página 2.

[1260] Principios globales de las Naciones Unidas para la integridad de la información. Recomendaciones para la acción de las partes interesadas. Disponible en: https://www.un.org/sites/un2.un.org/files/principios_globales_onu_integridad_informacion.pdf (23/11/2024).

[1261] Empresas tecnológicas y de desarrollo e investigación de la IA, publicistas y otros agentes del sector privado, medios de comunicación, investigadores y organizaciones de la sociedad civil, verificadores, Estados y la propia NNUU.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Se evidencia a través de este cuadro de acciones directivas y operativas que NNUU, aún cuando tiene problemas como los analizados en el Capítulo 2, mantiene un firme compromiso con la lucha contra la amenaza híbrida en sus diferentes manifestaciones y, en concreto, con la desinformación como reto presente y futuro que, invariablemente, se ve favorecido por los rápidos avances de la tecnología y la IA, a la que expresamente se refiere el Secretario General de NNUU, António Guterres, como factor sobrealimentador de las amenazas a la integridad de la información[1262]. Cuestión diferente será el compromiso de los distintos miembros de la comunidad internacional, las grandes plataformas digitales, empresas tecnológicas, publicistas y medios de comunicación, con esos principios universales que miran al bienestar común y al respeto de los Derechos Humanos como base de su existencia.

7.1.2. La respuesta a la amenaza híbrida de la OTAN

Por otro lado, tal y como estudiamos en la segunda parte del Capítulo 2, análoga suerte habría tenido la OTAN al afrontar dicho reto a tenor de la deriva iniciada con el nuevo siglo, cuando en algún momento la Alianza parece que perdió parte de las referencias que gobernaban el rumbo hacia su verdadero objetivo: procurar la defensa conjunta de sus miembros como uno solo.

Como ya expusimos[1263], el contexto geopolítico actual ha supuesto para la OTAN un importante desafío en cuanto al mantenimiento de la unidad de criterio de sus integrantes a la hora de apoyar y consensuar sus actuaciones, cuestión que resulta, entre otras, de la lógica evolución autónoma e independiente de la política exterior de sus socios, de la propia estrategia expansionista de la Alianza que ha conllevado abrirse a países que difieren en la forma de interpretar el mundo y sus relaciones, o las implicaciones anejas a esa nueva forma de amenaza, híbrida y desdibujada, que ataca a las bases de la democracia socavando sus instituciones, cuestionando sus procedimientos y polarizando el debate social interno para llevar a los ciudadanos a posturas altamente radicalizadas, donde fructifican a su antojo los nacionalismos y, también, los postulados de gobiernos autocráticos que constantemente se mueven en la Zona Gris.

Es por ello que, en 2008, se crea en Tallinn (Estonia) el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE por sus siglas en inglés)[1264], con la misión de apoyar a los países miembros y a la OTAN "con experiencia interdisciplinaria única en el campo de la investigación, entrenamiento y ejercicios de ciberdefensa cubriendo las áreas prioritarias de tecnología, estrategia, operaciones y derecho"[1265]. Su trabajo se materializa en iniciativas como el ejercicio de ciberdefensa anual aliado *Locked*

[1262] Mensaje sobre el lanzamiento de los Principios Universales para la Integridad de la Información. António Guterres. Secretario General de Naciones Unidas. 24 de junio de 2024. Disponible en: https://mexico.un.org/es/272346-mensaje-sobre-el-lanzamiento-de-los-principios-universales-para-la-integridad-de-la (25/10/2024).
[1263] Ver apartado 2.2.6.
[1264] NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE). Puede ampliarse información en la página web oficial de la OTAN. Disponible en: https://ccdcoe.org/ (25/10/2024).
[1265] Página oficial del CCDCOE. Disponible en: https://ccdcoe.org/about-us/ (25/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Shields[1266], orientado al entrenamiento de las capacidades de análisis y respuesta por parte de los equipos que representan a los países participantes o, también, la redacción de relevantes documentos como el ya referido *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, que conforma actualmente la base de la doctrina existente al respecto a través de sus 154 reglas que atienden a 20 cuestiones relacionadas con el ciberespacio y el Derecho Internacional aplicable, y cuya actualización se prepara ya ante el continuo posicionamiento que los Estados vienen haciendo sobre dichas materias. Esta línea de actuación para mejorar las capacidades de análisis estratégico y de comunicación de la Alianza y sus socios se continúa en 2014 mediante la creación en Riga (Letonia) del Centro de Excelencia de Comunicaciones Estratégicas de la OTAN (StratCom COE)[1267], dedicada a la recopilación, análisis y estudio de la información disponible para elaborar productos que interpretan el contexto geopolítico y el nivel de amenaza existente, como el referido a la manipulación de la información en redes sociales a partir de la invasión rusa de Ucrania[1268], o la detección de narrativas y el modelado de contenidos en los países bálticos[1269], entre otros.

El progreso en la lucha contra la amenaza híbrida lleva a la creación en 2017, bajo el lema *Una OTAN*, de la División Conjunta de Inteligencia y Seguridad (JISD, por sus siglas en inglés)[1270] como respuesta directa al desafío ruso en Crimea, la permanente transformación de la faceta mediática y operativa del terrorismo internacional y la inestabilidad del flanco sur de la Alianza, que suponen una amenaza real y directa totalmente distinta de la militar convencional, en la que las estrategias asimétricas, el aprovechamiento de las oportunidades del ciberespacio y el enfrentamiento híbrido en Zona Gris exigen nuevas capacidades y, desde luego, un conocimiento situacional mucho más profundo del contexto en que todo ello se reproduce. No es por tanto casualidad que, casi al mismo tiempo, se inaugure en Helsinki el Centro Europeo de Excelencia contra las Amenazas Híbridas (Hybrid CoE) con el objetivo de mejorar las capacidades de detección temprana, avanzar en las opciones de respuesta activa y aumentar la resiliencia de los aliados frente a este nuevo desafío de perfil no tradicional.

Un ejemplo de la materialización por parte de la OTAN de esta política de empleo de herramientas de respuesta integral contra la actividad híbrida en Zona Gris de sus adversarios, es el despliegue en 2021 de un Equipo de Apoyo contra Híbridos (CHST, por

[1266] Ver apartado 2.2.7.

[1267] NATO Strategic Communications Centre of Excellence (NATO StratCom COE). Disponible en: https://stratcomcoe.org/ (25/10/2024).

[1268] Manipulación de redes sociales a la venta: Experimento sobre las capacidades de la plataforma para detectar y contrarrestar interacciones no auténticas en las redes sociales. 4 de noviembre de 2024. Disponible en: https://stratcomcoe.org/publications/social-media-manipulation-for-sale-experiment-on-platform-capabilities-to-detect-and-counter-inauthentic-social-media-engagement/311 (22/11/2024).

[1269] Detección de narrativas y modelado de temas en los países bálticos. 14 de mayo de 2024. Disponible en: https://stratcomcoe.org/publications/narrative-detection-and-topic-modelling-in-the-baltics/303 (22/11/2024).

[1270] Puede ampliarse información de la Joint Intelligence and Security División (JISD) en la página web oficial de la OTAN. Disponible en: https://www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html (25/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

sus siglas en inglés)[1271] para analizar y contrarrestar la campaña de migración irregular impulsada desde Bielorrusia[1272] hacia Lituania, Letonia y Polonia a raíz del deterioro de relaciones con la UE con el doble objetivo de, por un lado tensionar a estos gobiernos aliados y, por otro, tratar de manipular, confundir, dividir y polarizar sus sociedades para socavar la cohesión interna a través de la instrumentalizando de la migración como factor de la amenaza[1273].

Por todo lo anterior, para afrontar estos conflictos desde un enfoque holístico de la seguridad, el Concepto Estratégico de Madrid ha supuesto un avance en la equiparación de las operaciones hostiles en los dominios ultraterrestre y ciberespacial con respecto a los ataques armados en los entornos convencionales, llamando a los aliados a su "preparación, disuasión y defensa contra el uso coercitivo de tácticas políticas, económicas, energéticas, de información y otras tácticas híbridas por parte de actores estatales y no estatales"[1274], dando incluso acceso a la posibilidad de invocar el artículo 5 del Tratado para la defensa común[1275]. Con ello se pretende una visión integral de la defensa frente a los diferentes vectores de ataque que pueden utilizar los actores de la amenaza sobre la base de una disuasión activa en todos los dominios, donde las estrategias híbridas pasan a ser calificadas por la OTAN como arma ofensiva aplicable en el marco de la gestión cooperativa de la seguridad de sus miembros.

La amplia panoplia de frentes de acción no tradicionales que los actores de la amenaza híbrida pueden utilizar, favorecidos por el espectacular desarrollo de la tecnología y las comunicaciones modernas, se materializan en operaciones en el ámbito cultural, tecnológico, social, político, diplomático, militar, económico, financiero, de manejo de la información y de gestión de la inteligencia, que exigen por parte de los Estados un alto nivel de comprensión y manejo de la escalada en la Zona Gris, so pena de enfrentarse a un efecto acumulativo de la maniobra del agente hostil que constriña su propia capacidad de actuación en el margen de las relaciones *pacíficas* entre Estados. Esta concienciación sobre la complejidad del desafío híbrido y el ofrecimiento de herramientas que puedan ser adaptadas a las particulares necesidades geopolíticas y estratégicas de sus aliados inspiran documentos como el *Hybrid Threats and Hybrid*

[1271] Contra-Hybrid Specialist Team. Puede ampliarse información en la página web oficial de la OTAN. Disponible en: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html (25/10/2024).

[1272] Amplio tratamiento en prensa de esta crisis migratoria. Disponible en: https://www.dw.com/es/lituania-r%C3%A9cord-de-inmigrantes-por-crisis-con-bielorrusia/a-58679564 https://es.euronews.com/2023/07/13/migrantes-en-europa-muchos-cruzan-a-lituania-desde-bielorrusia-para-quedarse-o-continuar-a https://www.rtve.es/noticias/20211118/bielorrusia-polonia-nueva-frontera-desinformacion/2225622.shtml (26/10/2024).

[1273] Esta estrategia ya fue utilizada por Rusia en 2014 en la invasión de Crimea como medio para implantar en el territorio un número de población afín a los intereses rusos y, de nuevo, lo ha sido a partir de 2022 en Ucrania para, desplegando civiles y dándoles alojamiento en viviendas creadas *ex profeso* en tiempo récord, asegurar los territorios conquistados por las tropas del Kremlin.

[1274] Considerando 27 del Nuevo Concepto Estratégico de la OTAN (Madrid, 29 de junio de 2022). Disponible en: https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf (26/10/2024).

[1275] Ver apartados 2.2.5. y 2.2.7.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Warfare Reference Curriculum[1276], con el que la OTAN ofrece a sus miembros una hoja de ruta que pueden seguir para la mejora de sus capacidades nacionales a nivel estratégico, táctico y operativo frente a las amenazas híbridas, de forma que:

> "A comprehensive framework may not exist within a country adopting this reference curriculum. It is unsafe to assume that all necessary domestic governments and civil society stakeholders are now involved. Therefore, local subject matter experts and representatives from nongovernmental organizations (NGOs) and private sector entities should be engaged through formal and informal activities, with government leaders who can speak to teamed national and societal efforts to counter a broad range of hybrid threat activity" (COSTIGAN & HENNESSY, 2024, pág. 61)[1277].

En este compromiso con el desarrollo y el mantenimiento de capacidades en los distintos planos de acción, los próximos años se antojan cruciales para comprobar si la Organización es capaz de mantener su original carácter euroatlántico, al tiempo que robustece su estructura defensiva ampliando el ámbito de influencia en un doble sentido: buscando la unidad de intereses con nuevos aliados más allá de sus fronteras que no aspiren a integrarse como miembros de la OTAN, y mediante la creación de una red cooperativa de socios no gubernamentales y asociaciones regionales que, de manera simbiótica, compartan sus necesidades de seguridad y defensa en todos los dominios en los que, actualmente, se desenvuelve la amenaza.

Podemos de esta forma concluir resaltando el enmarañado conjunto de intereses que subyace en estas estructuras internacionales y las relaciones que las vinculan, así como el beneficio que de ello pueden extraer los actores de la amenaza, por cuanto:

> "Members of international organizations, such as the UN, NATO, or the EU, have clear common interests but also have conflicting national interests. Friction between competing interests greatly increases the relevance of hybrid threats and hybrid warfare.
> Hybrid warfare, hybrid threats, and gray area conflict challenge the traditional understanding of the current world order and international norms. In particular, hybrid threats and warfare call into question the distinction between state and nonstate actors, the standard dichotomy between war and peace, and even the "great power" concept" (COSTIGAN & HENNESSY, 2024, pág. 41)[1278].

[1276] Hybrid Threats and Hybrid Warfare Reference Curriculum. NATO Headquarters Brussels, June 2024. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf (23/11/2024).

[1277] "Puede que no exista un marco integral en un país para adoptar este currículo de referencia. No es seguro asumir que necesariamente todos los gobiernos nacionales y las partes interesadas de la sociedad civil están involucrados. Por ello, los expertos locales en la materia, los representantes de las organizaciones no gubernamentales (ONG) y las entidades del sector privado deben participar a través de actividades formales e informales, junto con los líderes gubernamentales que puedan hablar de los esfuerzos nacionales y sociales conjuntos para contrarrestar una amplia gama de actividades de amenazas híbridas" (Traducción propia).

[1278] "Los miembros de organizaciones internacionales como NNUU, la OTAN o la UE, tienen evidentes intereses comunes, pero también tienen intereses nacionales contrapuestos. La fricción entre intereses contrapuestos aumenta la relevancia de las amenazas y la guerra híbrida.

Ediciones Universidad de Salamanca | CC BY-NC-ND

7.1.3. La estrategia de respuesta europea frente a la amenaza híbrida

En lo que respecta a la Unión Europea, cuyo ideal de defensa estudiado en el Capítulo 3 pretende garantizar la estabilidad y el orden mundial desde el multilateralismo bajo el mandato de las NNUU y el auspicio del Derecho Internacional, consideramos que representa el caso de éxito más consistente hasta la fecha en lo relativo a la armonización de intereses y la gestión cooperativa de un proyecto de seguridad holista y común para sus miembros. En este sentido, pudimos profundizar en las tres líneas de acción puestas en práctica por la Unión para alcanzar este objetivo asociativo, a través del cual generar respuestas unificadas ante amenazas compartidas: la Política Exterior y de Seguridad Común (PESC)[1279], la Política Común de Seguridad y Defensa (PCSD)[1280] y la estrategia política de seguridad interior europea[1281].

Como explicamos en su momento, no podemos colegir que sea esta una cuestión concluida y unívoca por cuanto la seguridad europea sigue respondiendo a un equilibrio dinámico y complejo con una derivada interna, como pieza necesaria para el buen gobierno de la Unión, y otra externa, que debe ayudar a conseguir su posicionamiento como referente en el orden y la seguridad internacionales. En este conglomerado de intereses de todo tipo, de amenazas, de presiones y de posturas políticas no siempre coincidentes, en el marco de la defensa exterior la UE ha apostado de manera decidida por alcanzar su autonomía estratégica y tecnológica al tiempo que busca redefinir su relación con la OTAN mientras que, en el plano de la seguridad interior, focaliza su acción en la nueva dimensión de la amenaza híbrida que supera la capacidad de respuesta independiente de sus Estados miembros y que exige un tratamiento integrado e integral.

En esta idea, ya el Consejo Europeo de junio de 2015 reflexiona sobre la evidencia de que el entorno de seguridad y defensa de los veintisiete ha sufrido una *transformación radical*, e incide específicamente sobre la migración como instrumento de coerción internacional que demanda una PCSD más eficaz sobre la base de, entre otras cuestiones, la necesidad de "movilizar los instrumentos de la UE a fin de contribuir a la lucha contra las amenazas híbridas" y de "intensificar las asociaciones, en particular con las Naciones Unidas, la OTAN, la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Unión Africana"[1282].

Con ello no se trata únicamente de llamar la atención sobre las nuevas formas que adopta la amenaza híbrida sino también, y esto es lo verdaderamente relevante, de

---

La guerra híbrida, las amenazas híbridas y los conflictos en Zona Gris desafían la tradicional comprensión del orden mundial actual y las normas internacionales. En particular, las amenazas y la guerra híbrida ponen en tela de juicio la distinción entre actores estatales y no estatales, la dicotomía clásica entre guerra y paz, e incluso el concepto de "gran potencia" (Traducción propia).

[1279] Ver apartado 3.2.3.

[1280] Ver apartado 3.3.4.

[1281] Ver apartado 3.4.6.

[1282] Conclusiones de la Reunión del Consejo Europeo (25 y 26 de junio de 2015). Bruselas, 26 de junio de 2015. EUCO 22/15. Página 6, apartado 10 C. Disponible en: https://www.consilium.europa.eu/media/21701/euco-conclusions_26062015_es.pdf (22/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

resaltar la *necesidad de actuar unidos y generar sinergias asociativas con sus aliados para unificar la respuesta* ante la misma.

Con estos antecedentes y espoleada por la controvertida invasión rusa de Crimea, la UE comienza a percibir claramente a las amenazas híbridas como una de las principales preocupaciones para su seguridad[1283], y a las narrativas desinformadoras como herramienta clave para su despliegue efectivo. Por esta razón, en 2015 el Consejo Europeo pide a la AR/VP que aborde el análisis de las campañas de desinformación de Rusia y comience a trabajar en su posible respuesta[1284]. De acuerdo con esta línea de acción, la Comisión Europea emite en abril de 2016 la *Comunicación conjunta sobre la lucha contra las amenazas hibridas. Una respuesta de la Unión Europea*[1285] donde se refiere a las campañas de desinformación masiva a través de los medios sociales como vector de la amenaza por su capacidad de control sobre el discurso político, su influencia para radicalizar y polarizar a la sociedad o para manipular a individuos que actúan por delegación, lo cual lleva a la Unión a considerar que:

> "En la medida en que la lucha contra las amenazas híbridas constituye un asunto de defensa y seguridad nacional y de mantenimiento del orden público, la responsabilidad principal recae en los Estados miembros, ya que la mayor parte de los puntos vulnerables son específicos de cada país. Ahora bien, muchos Estados miembros de la UE se enfrentan a amenazas comunes, que […] pueden tratarse con mayor eficacia si media una respuesta coordinada a escala de la UE que recurra a sus políticas e instrumentos y se asiente en la solidaridad europea, la asistencia mutua y todas las posibilidades que ofrece el Tratado de Lisboa"[1286].

El núcleo central de este enfoque integral de la UE frente a la amenaza híbrida fija un marco de responsabilidad individual, específico de cada uno de los Estados miembros, complementado con una estrategia basada en la solidaridad y la asistencia mutua que se sustenta en cuatro pilares: la mejora del conocimiento de la situación, el fomento de la resiliencia frente a la amenaza, el reforzamiento de la capacidad de actuación coordinada dentro de la Unión y el avance de la cooperación con la OTAN en la articulación de la respuesta.

[1283] Asi se entiende en el documento Strategic communications as a key factor in countering hybrid threats. European Parliamentary Research Service. March 2021. Página 40. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656323/EPRS_STU(2021)656323_EN.pdf (27/08/2024).

[1284] Así lo recoge expresamente la Comunicación Conjunta de la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción contra la desinformación. Bruselas 5.12.2018. JOIN(2018) 36 final. Disponible en: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036 (31/08/2024).

[1285] Ver el apartado 3.5. en el que nos referimos a esta Comunicación conjunta al Parlamento Europeo y al Consejo, sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea. Bruselas, 6.4.2016. JOIN(2016) 18 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52016JC0018 (19/08/2024).

[1286] IBIDEM, página 2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En base a ello, la Comisión propone hasta veintidós medidas para enfrentar la amenaza híbrida, aglutinadas en torno a tres grandes grupos temáticos[1287], cuya aplicación práctica es auditada a través de un par de informes en los años 2017[1288] y 2018[1289] respectivamente, que constatan los *avances notables* en esos cuatro pilares estratégicos al tiempo que concluyen la necesidad de seguir avanzando en la resiliencia y el desarrollo de capacidades para responder a la complejidad de este reto.

Acto seguido, en julio de 2016, la Comisión Europea publica un protocolo operativo para contrarrestar las amenazas híbridas, el *EU Playbook*[1290] donde, entre otras cuestiones, se acuerda la creación de la *Célula de Fusión Híbrida de la UE*, cuyas naturaleza y funciones serán:

> "The EU Hybrid Fusion Cell offers a single focus for the analysis of hybrid threats within the EU Intelligence and Situation Centre (EU INTCEN) of the EEAS. Its mandate and tasks will be defined in its Terms of Reference. The EU Hybrid Fusion Cell receives analyses and shares classified and open source information specifically relating to indicators and warnings concerning hybrid threats from different stakeholders within the EEAS (including EU delegations), Commission services, EU agencies and Member States. In liaison with existing similar bodies at EU and at national level, the Fusion Cell analyses external aspects of hybrid threats affecting the EU and its neighbourhood"[1291].

Esta estrategia debe, necesariamente, entenderse complementaria a los similares esfuerzos que otras estructuras internacionales, como la OTAN, llevan a cabo contra este tipo de amenaza. Para impulsar esta política de defensa común se crea en 2017 el

---

[1287] El primer grupo de medidas propuestas por la Comisión contra la amenaza híbrida se centra en la mejora de la concienciación y el grado de conocimiento de la dicha amenaza, así como en el fomento de la resiliencia frente a ella, abarcando desde la 1 a la 18. El segundo grupo de medidas, que comprende las propuestas 19 a 21, se orientan al reforzamiento de la capacidad de prevención, respuesta y recuperación conjunta ante la amenaza híbrida. Finalmente, la propuesta 22 insiste en el impulso de la cooperación con la OTAN con la idea de garantizar la complementariedad de las medidas articuladas frente a la amenaza y conseguir una respuesta más eficaz y coordinada.

[1288] Informe conjunto al Parlamento Europeo y al Consejo relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas – Una respuesta de la Unión Europea. Bruselas, 19.7.2017. JOIN(2017) 30 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=JOIN%3A2017%3A30%3AFIN (19/08/2024).

[1289] Informe conjunto al Parlamento Europeo, al Consejo Europeo y al Consejo relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas de julio de 2017 a junio de 2018. Bruselas, 13.6.2018. JOIN(2018) 14 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52018JC0014R%2801%29 (19/08/2024).

[1290] Council of the European Union. JOINT STAFF WORKING DOCUMENT EU operational protocol for countering hybrid threats *'EU Playbook'*. Brussels, 7 July 2016 (OR. En) 11034/16

[1291] El *EU Playbook* define en su apartado 2 (términos clave), página3, la Célula de Fusión Híbrida de la UE como: "La Célula de Fusión Híbrida de la UE ofrece un enfoque único para el análisis de amenazas híbridas dentro del Centro de Inteligencia y Situación de la UE (EU INTCEN) del SEAE. Su mandato y sus tareas se definirán en su mandato. La Célula de Fusión Híbrida de la UE recibe los análisis y comparte la información clasificada y de fuentes abiertas específicamente relacionada con indicadores y avisos sobre amenazas híbridas de las diferentes partes interesadas dentro del SEAE (incluidas las delegaciones de la UE), los servicios de la Comisión, las agencias de la UE y los Estados miembros. En colaboración con organismos similares existentes en la UE y a nivel nacional, la Célula de Fusión analiza los aspectos externos de las amenazas híbridas que afectan a la UE y a sus países vecinos" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Centro Europeo de Excelencia Contra las Amenazas Híbridas (Hybrid CoE)[1292], en cuyo seno se organizan grupos de interés por temáticas[1293], se programan ejercicios de entrenamiento y formación, y se generan productos de análisis a partir de las lecciones aprendidas para mejorar los procedimientos de respuesta e identificación de la amenaza que permitan, por ejemplo, neutralizar la desinformación generada por el Kremlin.

Es con este planteamiento con el que la Comisión Europea lanza en junio de 2018 su Comunicación para *Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas*[1294], conscientes de que:

> "Nuestras sociedades se enfrentan a un intrincado desafío planteado por quienes pretenden perjudicar a la UE y a sus Estados miembros con armas que van desde ciberataques que perturban la economía y los servicios públicos a acciones militares hostiles, pasando por campañas de desinformación con objetivos muy precisos"[1295].

En dicho documento se presentan cinco propuestas sobre las que cimentar la respuesta de la Unión frente al desafío híbrido:

1. La *mejora de la capacidad de detección temprana y la generación de inteligencia* para relacionar hechos y datos aparentemente inconexos, aprovechando para ello la experiencia analítica del EU INTCEN, incardinado dentro del SEAE[1296].
2. El *refuerzo de la acción europea* frente a la amenaza NRBQ a través de un régimen específico de sanciones y la puesta en marcha de medidas activas, como el control de precursores o la colaboración de los operadores privados y profesionales involucrados en la cadena de suministro, explotación y custodia de dichas sustancias, entre otras[1297].

[1292] El European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), constituido en abril de 2017 y con sede en Helsinki, es un centro internacional autónomo e independiente conformado por una red de profesionales y expertos en la materia, cuya misión es fortalecer la seguridad de los Estados y organizaciones participantes, proporcionando experiencia, conocimiento y capacitación a sus miembros para contrarrestar la amenaza híbrida. El Hybrid CoE promueve desde la UE y en colaboración con la OTAN un enfoque integral y conjunto contra las amenazas híbridas que pueden afectar a sus Estados miembros -36 en la actualidad-, con la misión de fortalecer la seguridad desde la prevención y, al mismo tiempo, preparar la respuesta proporcionando experiencia y capacitación, y compartiendo información frente a las interferencias externas hostiles. Disponible en: https://www.hybridcoe.fi/ (04/03/2024).

[1293] Estas comunidades de interés se refieren a la influencia híbrida, la estrategia y defensa, o las vulnerabilidades y la resiliencia.

[1294] Comunicación conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo. Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas. Bruselas, 13.6.2018. JOIN(2018) 16 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=JOIN%3A2018%3A16%3AFIN (19/08/2024).

[1295] IBIDEM, página 1.

[1296] Centro de Inteligencia y de Situación del Servicio Europeo de Acción Exterior.

[1297] En este sentido la Comisión Europea presenta en octubre de 2017 la Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones el Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares, como respuesta ante el avance tecnológico de la actual amenaza terrorista. COM/2017/0610 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52017DC0610 (19/08/2024).
En línea con ello, para el control de aquellas sustancias susceptibles de ser utilizadas indebidamente, la UE dota a sus Estados miembros de normativa armonizada como el Reglamento (UE) 2019/1148 del

Ediciones Universidad de Salamanca | CC BY-NC-ND

3. La *mejora de la comunicación estratégica de la UE* y de los procesos de difusión de la información facilitada a la población en caso de ataques híbridos, junto con la labor de concienciación y educación ciudadana para dotarles de herramientas que les permitan identificar y protegerse frente a la desinformación, elementos clave para salvaguardar la integridad de los procesos electorales democráticos[1298].
4. El *aumento de la resiliencia y de la disuasión* en materia de ciberseguridad, factores críticos para garantizar la prosperidad, procurar la seguridad y preservar los principios democráticos que caracterizan la naturaleza política de la Unión. En este sentido, también se requiere una mejora técnica en la capacidad de detección, rastreabilidad y gestión de la información para conseguir la atribución de la autoría de los ciberataques que, como ya hemos analizado, se benefician de la indeterminación propia de la Zona Gris, momento a partir del cual poner en marcha acciones de respuesta diplomática conjunta de la UE[1299].
5. El *desarrollo de la capacidad de identificación temprana, la coordinación de la respuesta y el regreso a la normalidad* frente a las actividades de inteligencia hostiles, principalmente en el ámbito de la injerencia extranjera en las instituciones y procedimientos de funcionamiento de la UE[1300].

Por su parte, el Consejo Europeo, consciente en todo momento de la necesidad de esta acción coordinada de los EEMM alineada con el resto de instituciones de la UE frente a la complejidad, diversidad y mutabilidad de la naturaleza de los nuevos desafíos, en sus

Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre la comercialización y la utilización de precursores de explosivos, por el que se modifica el Reglamento (CE) n.º 1907/2006 y se deroga el Reglamento (UE) n.º 98/2013. PE/46/2019/REV/1. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32019R1148 (19/08/2024).
En el caso de España, este Reglamento tiene desarrollo a través de la Ley 25/2022, de 1 de diciembre, sobre precursores de explosivos -BOE núm. 289, de 2 de diciembre de 2022-. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-20184 (19/08/2024).

[1298] En este contexto de refuerzo de las comunicaciones estratégicas de la Unión para hacer frente a la desinformación analizaremos en el punto 6.2.3. el Plan de Acción contra la Desinformación, aprobado por el Consejo Europeo en diciembre de 2018.

[1299] Este conjunto de herramientas de ciberdiplomacia se enmarcan en la PESC y, como tal, en el respeto del Derecho Internacional que conforman las normas y reglas de conducta responsable de los Estados, estableciéndose como medidas que pueden emplearse para responder a los comportamientos maliciosos en el ciberespacio que atenten contra la seguridad o los intereses de la UE. En este sentido, puede consultarse la Declaración del Alto Representante en nombre de la UE sobre el respeto del orden basado en normas en el ciberespacio de 12 de abril de 2019. Disponible en: https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/ (19/08/2024).

[1300] En febrero de 2019 el Consejo de la Unión Europea presenta sus Conclusiones del Consejo y de los Estados miembros sobre «Garantizar unas elecciones europeas libres e imparciales». Bruselas, 19 de febrero de 2019 (OR. en). En ella advierte sobre los agentes maliciosos, particularmente de origen ruso, que despliegan estrategias desinformativas con amplio impacto en las democracias europeas, frente a las que es necesaria articular una respuesta común guiada por el análisis de amenazas y la evaluación de inteligencia, compartiendo información de manera rápida, eficaz y segura (considerandos 14 y 15, página 4). Disponible en: https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/es/pdf (19/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Conclusiones de 20 de junio de 2019[1301] subraya que la Unión debe seguir avanzando en la sensibilización y la resiliencia de la democracia frente a la desinformación y garantizar una respuesta coordinada a las amenazas híbridas, reforzando incluso su cooperación con los agentes internacionales afectados, con el objetivo de proteger mejor las redes de información y comunicación europeas y sus procesos decisorios.

Un mes después, en julio de 2019, impulsa la creación del *Grupo de Trabajo Horizontal sobre la mejora de la resiliencia y la lucha contra las amenazas híbridas*[1302], con el que pretende dar un enfoque multidisciplinar a esa respuesta, tanto a corto como a largo plazo, analizar opciones, identificar posibles herramientas, desarrollar sinergias entre los EEMM y evitar solapamientos o lagunas en las acciones que se pongan en marcha para alcanzar estos objetivos. Esta filosofía del Grupo de Trabajo queda patente en el considerando 14 de su propuesta de creación:

> "[…] While acknowledging that the primary responsibility for countering hybrid threats lies with Member States, as most national vulnerabilities are country-specific, and while stressing that national security remains the sole responsibility of each Member State (TEU 4(2)), there is also a strong realisation of the fact that many Member States face common threats. Such threats may be addressed more effectively with a coordinated response at EU level. Countering hybrid threats and disinformation, improving strategic communication and enhancing resilience have been identified as key components of the EU's efforts to improve its security environment, building on European Solidarity. The EU should increase its capacities as a security provider including via the implementation of actionable proposals to help counter hybrid threats, disinformation, improve strategic communication and foster the resilience of Members States, EU institutions, as well as partners"[1303].

[1301] European Council meeting (19 and 20 March 2015) – Conclusions. Brussels, 20 March 2015 (OR. En). EUCO 11/15. Disponible en: https://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/en/pdf (27/08/2024).

[1302] El 8 de julio de 2019 el Consejo de la Unión Europea envía al Comité de los Representantes Permanentes la propuesta de creación de este Grupo de Trabajo, bajo la orientación del Comité de Representantes Permanentes -COREPER-, al que presentará un informe anual de actividades y conclusiones. Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats - Establishment and adoption of its Terms of Reference. Brussels, 8.7.2019. 10027/19. Disponible en: https://data.consilium.europa.eu/doc/document/ST-10027-2019-INIT/en/pdf (25/08/2024).

[1303] Documento del Consejo Europeo al COREPER, de 8 de julio de 2019, sobre la creación del Grupo de Trabajo Horizontal sobre la mejora de la resiliencia y la lucha contra las amenazas híbridas, considerando 14: "Reconociendo que la responsabilidad principal de luchar contra las amenazas híbridas es de los Estados miembros, puesto que la mayoría de las vulnerabilidades nacionales son específicas de cada país, y destacando que la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro (TUE 4, apartado 2), también es cierto de que muchos Estados miembros se enfrentan a amenazas comunes. Estas amenazas pueden abordarse de manera más eficaz con una respuesta coordinada a escala de la UE. La lucha contra las amenazas híbridas y la desinformación, la mejora de la comunicación estratégica y el refuerzo de la resiliencia se han identificado como componentes clave de los esfuerzos de la UE por mejorar su entorno de seguridad, basándose en la solidaridad europea. La UE debe aumentar sus capacidades como proveedor de seguridad, en particular mediante la aplicación de propuestas viables para ayudar a contrarrestar las amenazas híbridas y la desinformación, mejorar la comunicación estratégica y fomentar la resiliencia de los Estados miembros, las instituciones de la UE y sus socios" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

De esta manera se comienzan a gestar las políticas europeas de respuesta conjunta para combatir las amenazas híbridas y a trabajar en la identificación de herramientas transversales que permitan promover la coherencia de las iniciativas puestas en marcha en cuanto a la detección, la prevención, la preparación, la resiliencia, la respuesta, el intercambio de información y las mejores prácticas frente a aquellas por parte de la UE, sus Estados miembros y sus aliados, tanto en el marco de la OTAN como en el bilateral, tal y como se refleja en el informe *How Ukraine fights Russian disinformation: Beehive vs mammoth*[1304], en el que se incide en la necesidad de una labor conjunta de todos los aliados noratlánticos y miembros de la UE en sus respectivos ámbitos de actuación para contrarrestar de manera efectiva los canales rusos desinformativos y de propaganda, concluyendo entre otras cuestiones que:

> "[…] the primary takeaway for any other country would be to start dedicating significant resources to this fight sooner rather than later, because building a nation´s information resilience calls for the dedication and vigilance of many people and organizations over many years" (KALENSKY & OSADCHUK, 2024, pág. 39)[1305].

7.2. La lucha contra la desinformación en el marco de la Unión Europea

Debemos iniciar señalando que en la Unión no existe un marco jurídico como tal para regular la desinformación más allá del artículo 11 de su Carta de Derechos Fundamentales, referido al pluralismo de los medios de comunicación, la libertad de expresión y de información[1306], y las iniciativas políticas específicas que analizaremos a continuación[1307]. Una vez más, de acuerdo al reparto competencial del TUE que concretan los artículos 2 a 6 del TFUE[1308], la labor de identificar y neutralizar la desinformación cae bajo el paraguas de la propia responsabilidad de los Estados Miembros, siendo la UE la encargada de darles apoyo para promover la coordinación de sus acciones.

[1304] Informe de investigación híbrida del CoE n.° 11: "Cómo Ucrania lucha contra la desinformación rusa: colmena contra mamut". 24 de enero de 2024. Disponible en: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-11-how-ukraine-fights-russian-disinformation-beehive-vs-mammoth/ (22/11/2024).

[1305] "Lo más importante para cualquier país sería empezar a dedicar recursos significativos a esta lucha cuanto antes, porque reforzar la capacidad de resiliencia a la información de un país exige la dedicación y vigilancia de muchas personas y organizaciones durante muchos años" (Traducción propia).

[1306] Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de las Comunidades Europeas, 18.12.2000. C 364/1.
"Artículo 11: Libertad de expresión y de información 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. 2. Se respetan la libertad de los medios de comunicación y su pluralismo".
Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf (07/09/2024).

[1307] En este sentido se pronuncia el Tribunal de Cuentas Europeo en el considerando 09 de su Informe sobre el impacto de la desinformación en la UE. Informe Especial 9/2021 El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada 2021/C 215/06 (OJ C, C/215, 07.06.2021, p. 6, CELEX). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SA0009(01) (01/09/2024).

[1308] Ver apartado 3.4.2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por ello, el desarrollo de mecanismos de defensa adecuados frente a la desinformación requiere no solo de la identificación de la amenaza y su correspondiente disposición de respuesta por parte del Estado sino, también, de una participación activa de la sociedad civil y de los agentes del sector privado implicados junto a la estrategia institucional, cuyo punto de partida es la propia alfabetización mediática de los ciudadanos[1309] y, al mismo tiempo, la creación de normativa específica para la protección de sus intereses y datos personales.

Como podemos colegir, la desactivación de los efectos que causa la influencia manipuladora y la desinformación requiere un compromiso conjunto del tejido institucional y social en el que el sector privado resulta primordial. No en vano, como señala el profesor Fernández Rodríguez, el proceso de conformación de la opinión pública ha sufrido una importante evolución en el siglo XXI de mano de los mediadores de información y otros poderes fácticos interesados que, mediante su actuación guiada por ganancias comerciales o ventajas ideológicas, orientan de forma determinante el conocimiento de su público objetivo mediante la ocultación de ciertos datos y el énfasis de aquellos otros que les conviene. El resultado no es otro que la definitiva complicación del proceso de construcción de los cimientos de la opinión ciudadana por mor de la conjugación de la superabundancia de datos ofrecidos, su deformación y manipulación interesada (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 46).

En este contexto de respuesta integral y conjunta de toda la sociedad para prevenir, mitigar y responder frente a la amenaza híbrida, también la verificación de contenidos desempeña un papel determinante a la hora de detectar la manipulación informativa, identificar las estructuras en que se apoya y contrarrestar la desinformación generada, mitigando su impacto negativo. En este sentido, como señala el informe del Hybrid CoE *How Ukraine fights Russian disinformation: Beehive vs mammoth:*

> "Debunking lies is not in itself a sufficient condition in the counter-disinformation fight: it is not enough to counter the threat. However, it is a necessary condition: without it, it is just not possible to counter disinformation successfully" (KALENSKY & OSADCHUK, 2024, pág. 12)[1310]

[1309] Ya la Directiva 2010/13/UE del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), en su considerando 47 señala que: "La alfabetización mediática abarca las habilidades, los conocimientos y las capacidades de comprensión que permiten a los consumidores utilizar con eficacia y seguridad los medios. Las personas competentes en el uso de los medios podrán elegir con conocimiento de causa, entender la naturaleza de los contenidos y los servicios, aprovechar toda la gama de oportunidades ofrecidas por las nuevas tecnologías de la comunicación y proteger mejor a sus familias y a sí mismas frente a los contenidos dañinos u ofensivos. Por lo tanto, se debe promover el desarrollo de la alfabetización mediática en todos los sectores de la sociedad y seguirse de cerca sus avances".
Diario Oficial de la Unión Europea, de 15.4.2010, página 6. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010L0013&from=EN (12/10/2024).

[1310] "Desacreditar las mentiras no es en sí mismo una condición suficiente en la lucha contra la desinformación: no basta para contrarrestar la amenaza. Sin embargo, es una condición necesaria: sin ella, no es posible contrarrestar con éxito la desinformación" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

De esta manera podemos decir que todo este entorno desinformativo conforma un complicado constructo en el que se mezclan distintas variables, incluida la motivación económica que subyace a toda actividad comercial -como la propia de las plataformas digitales-, entre las que cabe destacar:

1. La complejidad de determinar lo que es verdad y lo que es mentira y, por tanto, la dificultad de considerar la autenticidad o falsedad de una información o noticia, que constituye *la narrativa.*
2. Los propios *sesgos intelectivos de los ciudadanos* que, inconscientemente, actúan como combustible facilitando la proliferación y el éxito de la manipulación informativa[1311] a través de técnicas que explotan este aspecto de la psique humana y su natural curiosidad. En el actual entorno informativo "las personas participan en los procesos políticos muy convencidas de lo que creen saber, pero ciegas a sus propios sesgos y a la intervención de los algoritmos en el filtrado del mundo real" (RUBIO NUÑEZ, FRANCO ALVIM, & DE ANDRADE MONTEIRO, 2024, pág. 58).
3. La *carencia de una base de educación de calidad de los ciudadanos para generar una serie de competencias digitales* con las que poder afrontar, con unas mínimas garantías de seguridad, el mundo que se abre ante ellos cada vez que, desde sus dispositivos móviles permanentemente conectados a la red, acceden a los servicios de todo tipo ofrecidos por las plataformas, donde la manipulación informativa y el desafío al pensamiento crítico es una constante (FERNÁNDEZ RODRÍGUEZ, 2024, págs. 155-164).
4. El *nuevo rol comunicador* que en la sociedad digital detentan los usuarios -como receptores y emisores- junto con la pérdida del papel intermediador de la prensa tradicional, promovido por la implantación masiva de las redes sociales y el nuevo modelo de negocio basado en el *clickbait*[1312].
5. El *complicado equilibrio* entre la defensa de las instituciones democráticas frente a la amenaza desinformativa y su afectación a los derechos fundamentales a expresar las propias ideas y a informar, pues son ellos los que sostienen dicha democracia haciendo posible la participación ciudadana, el pluralismo político y el control del ejercicio del poder.

[1311] En este sentido pueden citarse el *sesgo de confirmación*, que hace prevalecer en nuestro entendimiento la información que coincide con nuestras propias creencias, alimentando así la polarización paulatina de nuestras opiniones; la *simplificación de los hechos*, que reduce problemas complejos con múltiples perspectivas a un esquema binario basado en *conmigo* o *contra mí*; el efecto de la *verdad ilusoria*, por el que la constante repetición de una afirmación, independientemente de su naturaleza, acaba siendo percibida como una verdad irrefutable; el *filtro burbuja*, que nos lleva a rodearnos preferentemente de personas que comparten nuestras ideas y forma de pensar; o simplemente la propia *curiosidad humana* que convierte en más atractiva la información conspirativa o fantasiosa frente a la realidad, basa en datos objetivos y demostrables, lógicamente, menos apetecibles ante la sed de rumores y noticias.

[1312] Este modelo económico del *clickbait* se basa en el cómputo de los clics que realiza el cliente durante su navegación por la página web en cuestión, a cuyo propietario lo que le interesa es atraer la atención del usuario para ir saltando de enlace en enlace, donde se intercala publicidad o anuncios pagados. Esta dinámica perversa es la que alienta el uso de cualquier tipo de contenido -exagerado, inexacto, polarizador, populista, etc.- con el objetivo final de atraer la atención del cliente y *engancharlo* para que continúe navegando por los enlaces ofrecidos que son los que, por las ganancias de publicidad, aseguran la rentabilidad del servicio.

Ediciones Universidad de Salamanca | CC BY-NC-ND

6. La también *compleja relación* entre la defensa de los intereses geopolíticos y nacionales de los Estados frente a las amenazas híbridas y la desinformación, y su posible confrontación con los intereses económicos y comerciales de las grandes plataformas en línea -Google, Meta, etc.-, que pocas veces van a coincidir.
7. El *equilibrio* entre el impulso del desarrollo tecnológico y la digitalización frente a su instrumentalización para *infoxicar*[1313] a los usuarios o, directamente, *perfilarlos* de cara a lograr una mayor incidencia de los mensajes que se les dirige en función de su ideología y lealtad política.
8. El *conflicto de intereses* entre las plataformas de servicios en línea y los derechos de los usuarios en la lucha contra la desinformación, que por parte de las empresas queda a veces supeditada a programas de alfabetización mediática o de financiación de proyectos, y relegan verdaderas acciones de control de narrativas que pueden no interesar por las implicaciones comerciales que conlleven para sus anunciantes o inversores de capital.
9. El *complejo funcionamiento del entorno de comunicación digital* en cuanto a la difusión de narrativas desinformadoras y la estrategia de desactivación de éstas a través de la verificación de los datos aportados, siendo que la contranarrativa, en determinados casos, puede comportar sin pretenderlo una mayor propagación e impacto de la falsedad que se pretende desmontar, alimentando así teorías conspirativas de diversa índole.

7.2.1. La concienciación sobre la gravedad de la amenaza y el señalamiento de prioridades para contrarrestarla (2015-2018)

Partiendo de esta premisa por la que la estrategia de respuesta frente a la desinformación necesita una dimensión multifacética y de amplio espectro en cuanto a los actores implicados y las herramientas empleadas para ello[1314], podemos delimitar el año 2015 como el punto de inicio de las acciones específicas de la UE ante este grave desafío[1315].

[1313] El término infoxicación se construye mediante la unión de otros dos -información e intoxicación- y hace referencia a la estrategia de comunicación que satura la capacidad de atención y entendimiento de los destinatarios, utilizando gran cantidad de mensajes en los que se mezclan elementos verdaderos con otros tergiversados, manipulados o, directamente, falsos, con el objetivo final de generar confusión y desconcierto y, con ello, que los ciudadanos acaben no creyendo nada y, por lo tanto, guiando su conducta por parámetros que les llevan a la falta de confianza en los mensajes oficiales, la desafección de las instituciones o el desinterés por la participación en el modelo democrático, entre otros.

[1314] Desde 2013 la UE identifica las amenazas híbridas como fuente de riesgo, centrando inicialmente sus esfuerzos en el ámbito de la ciberseguridad. Enmarcada en esta estrategia europea frente a la amenaza híbrida de enfoque amplio, basada en el reforzamiento de la cooperación y la coordinación, la potenciación de los recursos y la inversión en capacidades tecnológicas, pudimos analizar en el Capítulo 3, apartado 5, la Directiva UE 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva SRI) y su derogación por la nueva Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI2). Como parte de esta respuesta multisectorial, también nos referimos en dicho Capítulo a la *Estrategia de Ciberseguridad de la UE para la Década Digital*, de diciembre de 2020 y a la creación del Hybrid CoE en el marco de relaciones con la OTAN, entre otras.

[1315] En este mismo sentido se pronuncia la Comisión Europea en la página 2 de la Introducción del Plan de Acción contra la desinformación, de diciembre de 2018, donde señala que "En 2015 el Consejo Europeo

Ediciones Universidad de Salamanca | CC BY-NC-ND

7.2.1.1. El Grupo de Trabajo East StratCom y la Comunicación Conjunta sobre la lucha contra las amenazas híbridas

En dicho contexto se debe entender la creación en marzo de 2015 del *Grupo de Trabajo East StratCom* en el seno del Servicio Europeo de Acción Exterior (SEAE)[1316], que se presenta como el paradigma de la respuesta especifica de la Unión ante la agresión de Rusia contra Ucrania tras las manifestaciones del *Euromaidán* de 2014[1317], que derivó en la anexión ilegal de la península de Crimea y sus continuas campañas de manipulación de la información contra los intereses europeos, que desde este momento se identifican ya como grave amenaza.

El Consejo Europeo en las *Conclusiones* de su reunión celebrada entre el 19 y el 20 de marzo de 2015[1318], muestra su preocupación por la situación de Rusia y Ucrania en su considerando 13 y, como objetivos al respecto, señala:

> "The European Council stressed the need to challenge Russia's ongoing disinformation campaigns and invited the High Representative, in cooperation with Member States and EU institutions, to prepare by June an action plan on strategic communication. The establishment of a communication team is a first step in this regard"[1319].

A partir de entonces el *Grupo de Trabajo East StratCom* es el responsable de coordinar la comunicación estratégica de defensa de la democracia europea para contrarrestar la

---

reconoció por primera vez la amenaza de las campañas de desinformación en línea, al pedir a la Alta Representante que abordara las campañas de desinformación de Rusia".
Comunicación Conjunta de la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción contra la desinformación. Bruselas 5.12.2018. JOIN(2018) 36 final. Disponible en: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036 (31/08/2024).

[1316] El Grupo de Trabajo East StratCom se forma dentro de la División de Comunicación Estratégica y Análisis de la Información del SEAE, y está integrado por expertos del campo de las comunicaciones, el periodismo, las ciencias sociales y los estudios rusos. Como parte de su estrategia de sensibilización y fomento de la resiliencia contra la desinformación, dispone del sitio web EUvsDisinfo y de cuentas en diferentes redes sociales. Una de sus principales herramientas es la Base de Datos de acceso público que recopila casos de desinformacion pro-Kremlin desde el año 2015 y que, a día de la fecha de consulta, dispone de más de 17.481 entradas de casos. Asimismo, dispone de publicaciones de libre acceso como el boletín semanal *Disinfo Review*, artículos y contenidos de colaboradores especializados, estudios e informes, entre otros. Disponible en: https://euvsdisinfo.eu/ (27/08/2024).

[1317] Ver el Capítulo 2, apartado 2.2.4.

[1318] European Council meeting (19 and 20 March 2015) – Conclusions. Op. Cit., página 5. Disponible en: https://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/en/pdf (27/08/2024).

[1319] "El Consejo Europeo ha destacado la necesidad de contrarrestar las actuales campañas de desinformación de Rusia y ha invitado a la Alta Representante a que, en cooperación con los Estados miembros y las instituciones de la UE, prepare antes de junio un plan de acción sobre comunicación estratégica. La creación de un equipo de comunicación constituye una primera medida en ese sentido" (traducción del Comunicado de Prensa en español de la Secretaría General del Consejo de la UE, sobre las Conclusiones del Consejo sobre relaciones exteriores, de 19/20 de marzo de 2015). Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2015/03/19/conclusions-russia-ukraine-european-council-march-2015/pdf/ (27/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

desinformación rusa mediante su identificación, recopilación y análisis, tal y como se especifica en su página web oficial:

> "El objetivo principal de EUvsDisinfo es aumentar la conciencia pública y la comprensión de las operaciones de desinformación del Kremlin, y ayudar a los ciudadanos en Europa y más allá a desarrollar resistencia a la información digital y la manipulación de los medios"[1320].

En paralelo, la Comisión Europea lanza en abril de 2016, como ya hemos examinado, la *Comunicación Conjunta sobre la lucha contra las amenazas híbridas: una respuesta de la Unión Europea*[1321], donde concretamente se refiere a las campañas de desinformación como magnitud a considerar para afrontar dicha amenaza, y en abril de 2018 avanza un paso más con otra Comunicación titulada *La lucha contra la desinformación en línea: un enfoque europeo*, buscando articular una respuesta política común y exhaustiva, consciente de que:

> "La exposición de los ciudadanos a una desinformación a gran escala, que incluye información engañosa o completamente falsa, representa un gran reto para Europa"[1322].

En ella se advierte del poder de las redes sociales y las nuevas tecnologías para dimensionar los efectos de la desinformación sobre sus destinatarios, mediante la creación de esferas de información personalizadas y la gran precisión de los selectores de grupos, entre otros recursos, con resultados como la pérdida de capacidad de los ciudadanos para adoptar decisiones oportunas e informadas, la proliferación de ideas radicalizadas y extremistas, el menoscabo de derechos fundamentales y libertades o, consecuentemente, la erosión de la confianza en las instituciones y medios de comunicación profesionales[1323].

También se llama la atención sobre las campañas desinformativas orquestadas por agentes nacionales y de otros países que, claramente, suponen una amenaza para la seguridad interna, con especial referencia a los procesos electorales por la gravedad de sus efectos para la salud de la democracia, que si bien corresponde al ámbito competencial de los Estados miembros no deja de tener una dimensión europea por sus evidentes vinculaciones de todo tipo -políticas, económicas, ideológicas, sociales, tecnológicas, defensivas, etc.-[1324].

[1320] Objetivo definido en su propia página web. Disponible en: https://euvsdisinfo.eu/about/ (27/08/2024).

[1321] En el apartado anterior al estudiar la respuesta de la Unión ante la amenaza híbrida nos referíamos al epígrafe 3.5. en el que analizábamos esta *Comunicación conjunta al Parlamento Europeo y al Consejo, sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea*. Bruselas, 6.4.2016. JOIN(2016) 18 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52016JC0018 (31/08/2024).

[1322] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La Lucha contra la desinformación en línea: un enfoque europeo. Bruselas, 26.4.2018. COM(2018) 236 final. Introducción, página 1. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236 (26/08/2024).

[1323] IBIDEM, página 1.

[1324] IBIDEM, página 2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Conforme a estas premisas la Comisión presenta su propuesta para combatir la desinformación en línea, sustentada en cuatro objetivos globales: 1) aumentar la transparencia de la información; 2) promover su diversidad para fomentar el análisis crítico; 3) fomentar la credibilidad de la información trazando su fiabilidad; y 4) crear soluciones inclusivas a través de la sensibilización, la alfabetización mediática y la participación de las partes interesadas[1325].

Para su logro se plantean las siguientes líneas de acción:

1. Crear una comunidad de plataformas en línea más transparente, fiable y responsable mediante la adopción de un *código de buenas prácticas* que, entre otros objetivos, reduzca la visibilidad de la desinformación, facilite la autoevaluación de contenidos por los usuarios y facilite la labor de los verificadores de datos acreditados, que son catalogados como parte esencial de la cadena de valor de los medios de comunicación. Asimismo, se incide en la importancia de la trazabilidad de las fuentes de información y en el aprovechamiento de las capacidades de las nuevas tecnologías aplicadas a estos fines[1326].
2. Velar por la seguridad de los procesos electorales como base de la democracia, identificando, gestionando y mitigando los ciberataques y las campañas desinformativas que los afectan[1327].
3. Fomentar una estrategia a largo plazo de educación y alfabetización mediática para dotar de competencias y capacidad de comprensión a los ciudadanos con las que poder utilizar con seguridad los dispositivos tecnológicos, madurar un pensamiento crítico que les permita discernir y razonar diferenciando entre opiniones y hechos y, en definitiva, alcanzar elevados niveles de resiliencia frente a la desinformación[1328]. Aquí se integran iniciativas como las recogidas en el *Plan de Acción de Educación Digital*[1329] para impulsar el desarrollo de un sistema educativo que permita mejorar las competencias y capacidades de los ciudadanos de cara a la transformación digital.
4. Garantizar un ecosistema plural y diverso de medios informativos de calidad, tanto tradicionales como en línea, comprometidos con la veracidad de la información y los intereses de los ciudadanos[1330].

[1325] IBIDEM, página 7.
[1326] IBIDEM, página 8.
[1327] IBIDEM, página 13.
[1328] IBIDEM, página 14.
[1329] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción de Educación Digital. Bruselas, 17.1.2018. COM(2018) 22 final. Este primer plan 2018-2020 posteriormente dio paso al actual Plan de Educación Digital 2021-2027, recogido en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Plan de Acción de Educación Digital 2021-2027: Adaptar la educación y la formación a la era digital. Bruselas, 30.9.2020. COM(2020) 624 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0022&from=EN https://eur-lex.europa.eu/ES/legal-content/summary/digital-education-action-plan-2021-2027.html (27/08/2024).
[1330] La Lucha contra la desinformación en línea: un enfoque europeo, op.cit., página 16.

Ediciones Universidad de Salamanca | CC BY-NC-ND

5. Impulsar en el marco de actuación del SEAE la comunicación estratégica para contrarrestar la desinformación proveniente tanto del ámbito interno como externo, a través de agentes públicos o privados.

7.2.1.2. El desarrollo de las capacidades frente a la amenaza híbrida y el primer Código de Buenas Prácticas en materia de desinformación

Con este objetivo de combatir la amenaza híbrida y la desinformación como una de sus principales herramientas, la Comisión Europea y la AR/VP firman en junio de 2018 la Comunicación Conjunta titulada *Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas*[1331], donde advierten del desafío que suponen las diversas formas que éstas pueden adaptar, desde los ciberataques contra intereses económicos o instituciones públicas a las operaciones militares hostiles, "pasando por campañas de desinformación con objetivos muy precisos"[1332]. Para contrarrestarlas se entiende prioritaria la labor educacional y de concienciación de la población mediante una adecuada estrategia de comunicación, con el fin de que los ciudadanos aprendan a distinguir entre la información de calidad y la desinformación dañina. En concreto, se refiere la Comisión a las intrusiones y ataques contra las infraestructuras y los sistemas de campaña electoral, así como a las campañas de desinformación con fines políticos para desacreditar a las instituciones y deslegitimar los procesos democráticos[1333], en un contexto de preparación de las elecciones al Parlamento Europeo de 2019 que miraba con inquietud a los precedentes aportados por el despliegue de actividad del Kremlin en la Zona Gris desde la invasión de Crimea en 2014, los resultados de las elecciones presidenciales estadounidenses del 2016 que catapultaron al poder a Donad Trump y la mala gestión de la estrategia comunicativa europea que espoleó el *Brexit* ese mismo año. Ese contexto sirvió para elevar la alerta de la UE ante los posibles efectos que pudieran causar las campañas de desinformación, principalmente las alimentadas por actores externos, en los procesos electorales y democráticos europeos.

Desde este momento se aprecia ya la permanente atención por parte de la Comisión Europea a las campañas desinformativas, de manera que las referencias a dicha amenaza se consolidan como factor común de otros textos normativos que atienden a escenarios estrechamente vinculados con ella, como la Comunicación de septiembre de 2018 denominada *Garantizar unas elecciones europeas libres y justas*, en la que se concluye la inmediata puesta en marcha "de un plan de acción con propuestas concretas encaminadas a una respuesta coordinada de la UE al reto de la desinformación"[1334].

[1331] Comunicación Conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo. Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas. Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 13.6.2018. JOIN(2018) 16 final. Este texto fue ya analizado en el Capítulo 3, apartado 5, al estudiar la estrategia de la UE en el ciberespacio. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0016 (26/08/2024).

[1332] IBIDEM, página 1.

[1333] IBIDEM, página 8.

[1334] Conclusiones, página 10, de la Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Garantizar unas elecciones europeas libres y justas. *Contribución de la Comisión Europea a la reunión de los dirigentes en Salzburgo*

Ediciones Universidad de Salamanca | CC BY-NC-ND

Conscientes de que el problema de la difusión de esta amenaza afecta a múltiples actores que deben comprometerse en su mitigación, la Comisión presenta en octubre de ese mismo año el primer *Código de Buenas Prácticas en materia de desinformación*[1335] sobre los principios de voluntariedad y buena fe de las partes, con el objetivo de involucrar a las plataformas en línea, los anunciantes y el sector de la publicidad, cuya actividad resulta crucial por su capacidad para amplificar y difundir contenidos desinformativos y, al mismo tiempo, por la cadena de valor que representan en la lucha contra ellos. Su triunfo radica en que es la primera vez que la industria de la comunicación y los servicios digitales se compromete, de manera voluntaria, con un conjunto de estándares de autorregulación para combatir la desinformación.

La finalidad de este primer Código de Buenas Prácticas es identificar las acciones que las plataformas en línea firmantes puedan llevar a cabo para mitigar los efectos de la desinformación y, al mismo tiempo, alcanzar una mayor transparencia y la adecuada rendición de cuentas de aquellas mediante la aplicación de estándares de autorregulación para combatir dicha amenaza. Para ello, se incide en la protección contra la desinformación a través de compromisos respecto a los anuncios publicitarios, la promoción de políticas contra las declaraciones falsas y las cuentas asociadas, la priorización de la información auténtica y de contenido fiable o el empoderamiento de los usuarios mediante herramientas que faciliten el acceso a fuentes de información distintas que presenten puntos de vista alternativos.

No obstante, siendo una herramienta pionera, su principal debilidad radica precisamente en la amplitud de opciones de compromiso que ofrece, tal y como recoge su Preámbulo:

> "Given the breadth of the commitments outlined in the Code and the heterogeneous range of stakeholders involved, Signatories will sign up only to commitments which correspond to the product and/or service they offer, their role in the value chain, their technical capabilities and their liability regimes as provided under EU Law, which vary depending on the role they play in the creation and dissemination of the content at stake"[1336].

los días 19 y 20 de septiembre de 2018. Bruselas, 12.9.2018. COM(2018) 637 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2018%3A637%3AFIN (31(08/2024).

[1335] Código de Buenas Prácticas en materia de desinformación, de la Comisión Europea, publicado el 16 de junio de 2018. Conforme indica la página web de la Comisión Europea, el Código de Buenas Prácticas fue firmado en octubre de 2018 por las plataformas en línea Facebook, Google, Twitter y Mozilla, así como por anunciantes y otros actores del sector publicitario. Microsoft se unió al Código en mayo de 2019, mientras que TikTok lo firmó en junio de 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (02/09/2024).

[1336] "Dada la amplitud de los compromisos establecidos en el Código y la naturaleza heterogénea de las partes interesadas, los signatarios solo firmarán los compromisos que correspondan al producto y/o servicio que ofrecen, a su papel en la cadena de valor, a su capacidad técnica y a sus regímenes de responsabilidad según lo dispuesto en el Derecho de la Unión, los cuales varían en función del papel que desempeñen en la creación y difusión del contenido en cuestión". Código de buenas prácticas sobre desinformación, octubre de 2018. Preámbulo, páginas 1 y 2. Disponible en: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (08/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Este amplio marco opcional, la falta de criterios de uniformidad en su aplicación, la inadecuación de algunos de sus conceptos y la falta de concreción a la hora de objetivizar el nivel de cumplimiento de los compromisos por los signatarios hace que se inicie su proceso de revisión[1337], que culminará con la presentación en 2022 de un nuevo *Código Reforzado de Buenas Prácticas contra la Desinformación.*

7.2.1.3. El Plan de Acción contra la Desinformación

Este periodo inicial de concienciación de la gravedad de la amenaza y definición de prioridades culmina en diciembre de 2018 con la presentación de otra propuesta, el *Plan de Acción contra la desinformación*[1338]*,* que la Comisión Europea y la AR/VP anuncian como la punta de lanza de la defensa de la Unión, sus instituciones y sus ciudadanos frente a la amenaza desinformativa, y que se arma en torno a diez acciones coordinadas y organizadas conforme a cuatro pilares:

1. La *mejora de la capacidad de las instituciones* de la Unión para detectar, analizar y exponer la desinformación, mediante dos acciones centradas en el reforzamiento de los avances en comunicación estratégica y la ampliación de los *Grupos de Trabajo StratCom* hacia nuevos frentes a cubrir -Balcanes occidentales y países meridionales-.
2. El *refuerzo de las respuestas europeas coordinadas y conjuntas* a la desinformación, analizada en el marco de la guerra híbrida, desde tres acciones encaminadas a la creación de un *Sistema de Alerta Rápida* (RAS por sus siglas en inglés)[1339] vinculado a la capacidad de respuesta permanente del SEAE, la

[1337] En este sentido debemos referirnos a la propia evaluación de la Comisión Europea del Código de buenas prácticas sobre desinformación, de septiembre de 2020, en la que se concluye que es necesario mejorar el Código proporcionando definiciones compartidas comunes, procedimientos más claros, compromisos más precisos, indicadores clave de rendimiento transparentes y un seguimiento adecuado de estos. Además, debe darse entrada a la participación de otras partes interesadas, como el sector publicitario. Igualmente se señala la dependencia de la Comisión y del resto de instituciones de la Unión a la hora de acceder a la información y los datos propiedad de las plataformas, lo cual impide una evaluación independiente de la realidad de la amenaza desinformativa, así como de la eficacia de la acción de las plataformas para contrarrestarla. Para ello debe avanzarse en un modelo de colaboración más adecuado entre estas, los verificadores y el resto de la comunidad investigadora.
Commission Staff Working Document. Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement. Brussels, 10.9.2020. SWD(2020) 180 final. Conclusiones, página 19. Disponible en: https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement (08/09/2024).

[1338] Comunicación Conjunta de la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción contra la desinformación. Bruselas 5.12.2018. JOIN(2018) 36 final. Disponible en: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036 (31/08/2024).

[1339] El *Sistema de Alerta Rápida* de la UE (RAS, Rapid Alert System) contra la amenaza desinformativa es un elemento relevante en la estrategia europea para abordar esta amenaza, que se articula en marzo de 2019 a través de puntos de contacto nacionales los cuales, en el momento en que detectan una campaña de este tipo, ponen en marcha el procedimiento de contacto con sus homólogos del resto de Estados Miembros a través de una infraestructura técnica específica para intercambiar información al respecto y, de manera coordinada, determinar las posibles medidas de respuesta que procedan. Amplio seguimiento en prensa. Disponible en: https://elderecho.com/la-ue-lanza-este-semana-sistema-alerta-rapida-la-desinformacion

Ediciones Universidad de Salamanca | CC BY-NC-ND

intensificación de la labor de proyección de los valores y políticas de la Unión -sobre todo con vistas a los procesos electorales europeos- y el reforzamiento de las comunicaciones estratégicas europeas en los países vecinos.

3. La *movilización del sector privado* para combatir la desinformación, cuyo seguimiento se arbitra a través de una acción de la Comisión centrada en la puesta en marcha de un *Código de Buenas Prácticas* a modo de código de autorregulación voluntariamente aceptado por las plataformas en línea y la industria publicitaria en el que, si no están todas, al menos sí lo estén las principales[1340].
4. El *aumento de la sensibilización* sobre los efectos negativos de la desinformación y la capacidad de respuesta de la sociedad, mediante cuatro acciones orientadas al impulso de campañas específicas para el público en general y el apoyo a los medios de comunicación independientes y el periodismo de calidad, la potenciación de la labor de los equipos de verificadores de datos e investigadores multidisciplinares, la promoción de la cooperación transfronteriza entre profesionales de la alfabetización mediática y la puesta en marcha de herramientas prácticas que la fomenten y, finalmente, la garantía de la aplicación efectiva por los Estados miembros del conjunto de medidas concebidas por la Unión para garantizar unas elecciones europeas libres y justas[1341].

Merece ser destacado, dentro de este cuarto Pilar, la mención a los verificadores de datos e investigadores privados, por cuanto que:

> "Los verificadores de datos y los investigadores independientes desempeñan un papel clave a la hora de fomentar la comprensión de las estructuras que apoyan la desinformación y los mecanismos que determinan cómo se difunde en línea. Además, a través de sus actividades, sensibilizan sobre diversos tipos de amenazas de desinformación y pueden contribuir a mitigar su impacto negativo. Es necesario reforzar su capacidad para detectar y exponer las amenazas de la desinformación y facilitar la cooperación transfronteriza"[1342].

---

https://www.eitb.eus/es/noticias/sociedad/detalle/6275323/la-ue-lanza-su-sistema-alerta-rapida-desinformacion-18-marzo/ (01/09/2024).

[1340] El *Código de Buenas Prácticas contra la desinformación*, puesto en marcha en septiembre de 2018, supone el primer caso de éxito en el que las plataformas en línea y la industria de la publicidad aceptan autorregularse para evitar la propagación de la desinformación y las noticias falsas a través de sus servicios digitales en red. Inicialmente lo suscriben Facebook (Meta a partir de octubre de 2021), Google, Twitter y Mozilla. En mayo de 2019 lo hace Microsoft y Tik Tok en junio de 2020. Tras la llegada de Elon Musk a Twitter la red social no solo cambia su nombre comercial a X sino que, también, en mayo de 2023, se retira del compromiso con el Código Reforzado de Buenas Prácticas. Seguimiento en prensa de esta decisión de la plataforma. Disponible en: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation
https://www.europapress.es/portaltic/socialmedia/noticia-twitter-retira-codigo-buenas-practicas-materia-desinformacion-ue-20230529102243.html (01/09/2024)

[1341] Esta última acción está específicamente orientada a la protección del desarrollo de las elecciones europeas de mayo de 2019, próximas a celebrarse cuando se publica el Plan de Acción contra la Desinformación en diciembre de 2018.

[1342] Comunicación Conjunta de la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción contra la desinformación. Bruselas

Ediciones Universidad de Salamanca | CC BY-NC-ND

La promoción de esta importante labor de verificación, que algunos autores incluso llegan a considerar como una *nueva institución democrática* (GRAVES & CHERUBINI, 2016, pág. 6), comienza en EE.UU. durante la primera década del siglo XXI con iniciativas como *Politifact*[1343], aunque es a partir del año 2015 con la fundación de la *International Fact-Checking Network* (IFCN)[1344], la llegada al poder de líderes como Donald Trump en 2017 en EE.UU. y Jair Bolsonaro en 2019 en Brasil y, finalmente, la eclosión desinformadora y conspiranoica vinculada a la pandemia del COVID-19 (MORENO-GIL & SALGADO DE DIOS, 2023, pág. 294), cuando definitivamente despega el *fact checking*[1345] y la visión de la necesidad de coordinar el esfuerzo de los verificadores de todo el mundo. Para coadyuvar a ello, la IFCN unifica la metodología y acuerda un *Código de Principios*, con cinco compromisos que toda plataforma de verificadores debe cumplir: 1) la imparcialidad y la equidad; 2) la transparencia de las fuentes; 3) la transparencia en la financiación y la organización; 4) la transparencia de la metodología utilizada; 5) y el compromiso con las correcciones abiertas y honestas[1346].

Este puede ser considerado el inicio de la profesionalización de los verificadores y su concienciación sobre la tarea global que deben asumir para contribuir, si no a acabar con la desinformación puesto que se trata de una amenaza prácticamente inabarcable, sí a mitigar sus efectos. Para ello resulta clave, por un lado, sacar a la luz y desmontar aquella información falsa o inexacta que circule por los canales de comunicación con una metodología vinculada a los compromisos de exactitud, imparcialidad, objetividad, independencia, exhaustividad y transparencia, y por otro, ayudar a la alfabetización mediática de las audiencias para sensibilizarlas ante el problema y que vayan adquiriendo competencia crítica y ética con la que conformar sus opiniones y aprender a defenderse de la manipulación informativa (MORENO-GIL & SALGADO DE DIOS, 2023, pág. 296). Por esta razón, el *Plan de Acción contra la desinformación* de la Comisión Europea se refiere a los verificadores como uno de los mecanismos claves para conformar el frente de respuesta ante las narrativas desinformadoras.

5.12.2018. JOIN(2018) 36 final. Página 11. Disponible en: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036 (12/11/2024).

[1343] Politifact se crea en 2007 para verificar las afirmaciones, mensajes y datos lanzados por los políticos y sus equipos durante la campaña presidencial de los EE.UU. y, posteriormente, se amplía su cometido a la verificación de los mensajes del Congreso y la Casa Blanca. Obtuvo el Premio Pulitzer de Periodismo en 2009 por su labor durante la campaña estadounidense del 2008, utilizando periodistas del St. Petersburg Times. Disponible en: https://www.politifact.com/ (12/10/2024).

[1344] Red Internacional de Verificación de Datos (IFCN por sus siglas en inglés), fundada por el Instituto Poynter, que es una organización internacional "que fortalece la democracia mejorando la relevancia, la práctica ética y el valor del periodismo". Disponible en: https://www.poynter.org/about/ (12/10/2024).

[1345] El *fact checking* (verificación de datos) es un proceso por el cual se analizan las noticias y mensajes en el ámbito público y se examina su veracidad recurriendo a fuentes de información contrastadas, para concluir su falsedad o veracidad, con el objetivo de promover la transparencia y la verdad en la comunicación de las sociedades democráticas y empoderar a los ciudadanos para que puedan tomar decisiones informadas y con bases de certeza. Muy unido al anterior está el *debunking* (desenmascarar/desacreditar), que consiste en el desmentido de noticias falsas transmitidas por las redes sociales, y que también forma parte de la labor de los verificadores.

[1346] El Código de Principios puede consultarse en la página web de Poynter. Disponible en: https://www.poynter.org/fact-checking/2018/a-new-home-for-the-ifcn-code-of-principles/ (12/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Consciente de ello, en la presentación del Plan, la AR/VP Federica Mogherini lanza un mensaje claro y contundente que avisa de los objetivos perseguidos:

> "Una democracia sana depende de un debate público abierto, libre y justo. Es nuestro deber proteger este espacio y no permitir que nadie difunda desinformación que alimente el odio, la división y la desconfianza en la democracia […]. Como UE, hemos decidido actuar juntos y reforzar nuestra respuesta para apoyar la resiliencia de nuestras sociedades, dentro de nuestras fronteras y en la vecindad. Es la manera europea de responder a uno de los principales desafíos de nuestro tiempo"[1347].

De esta manera, el año 2018 se cierra como uno de los más prolijos respecto a la acción normativa de la Unión frente a la amenaza desinformativa y la creación de capacidades para darle respuesta.

7.2.2. Las evaluaciones de impacto, la definición del marco normativo y la elaboración de herramientas específicas (2019-2024)

7.2.2.1. La Agenda Estratégica de la UE y la infodemia de la COVID-19

Tras las elecciones europeas de mayo de 2019 el Consejo aprueba la *Agenda Estratégica de la UE 2019-2024*[1348], fijando cuatro ámbitos prioritarios de actuación[1349] entre los que destacamos el orientado a proteger a los europeos y sus libertades frente a las actividades cibernéticas maliciosas, las amenazas híbridas y la desinformación procedente de agentes estatales y no estatales hostiles. Acorde con esta línea directriz, la Presidenta de la Comisión, Úrsula von der Leyen, elabora seis *prioridades políticas*[1350] para dicho mandato, señalando expresamente que "necesitamos un enfoque integrado y general de nuestra seguridad"[1351] así como "hacer más para protegernos de interferencias externas"[1352], siendo que para ello "debemos desarrollar un enfoque

[1347] Nota de prensa del SEAE en su página web oficial, de 05.12.2018. Intensificar la respuesta europea coordinada a la desinformación. Disponible en: https://www.eeas.europa.eu/node/54897_en (08/09/2024).
[1348] Una nueva agenda estratégica para la UE 2019-2024. Documento del Consejo Europeo, de 20 de junio de 2019. Disponible en: https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/ (25/08/2024).
[1349] Las cuatro prioridades de actuación de la UE que se fijan para el periodo 2019-2024 son: 1) Proteger a los ciudadanos y las libertades; 2) desarrollar una base económica sólida y dinámica; 3) construir una Europa climáticamente neutra, ecológica, justa y social; 4) promover los intereses y valores europeos en el mundo.
[1350] Una Unión que se esfuerza por lograr más resultados. Mi agenda para Europa. Orientaciones políticas para la próxima Comisión Europea 2019-2024. Úrsula von der Leyen. Las seis prioridades políticas que establece son: 1) Un Pacto Verde Europeo; 2) Una economía que funcione en pro de las personas; 3) Una Europa adaptada a la era digital; 4) La protección de nuestro estilo de vida europeo; 5) Una Europa más fuerte en el mundo; 6) Un nuevo impulso a la democracia europea. Disponible en: https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_es?filename=political-guidelines-next-commission_es.pdf (25/08/2024).
[1351] IBIDEM, página 21.
[1352] IBIDEM, página 23.

Ediciones Universidad de Salamanca | CC BY-NC-ND

común y normas comunes para abordar cuestiones como la desinformación y los mensajes en línea de incitación al odio"[1353].

En junio de 2020 la Comisión Europea, consciente de que la responsabilidad de combatir la desinformación estriba en la acción de los Estados Miembros y que el impulso de una visión común y catalizadora de acciones que permitan responder desde la coordinación y la adecuada gestión de la comunicación es competencia de la UE, presenta su Comunicación conjunta titulada *La lucha contra la desinformación acerca de la COVID-19: contrastando los datos*[1354], en la que se examinan las acciones concretas ya adoptadas y las pendientes de implementar para contrarrestar la *infodemia*[1355] generada en Internet sobre el brote infeccioso, reconociendo la *necesidad de acordar un sistema de publicación de informes periódicos sobe la evolución de estas medidas*[1356].

El fenómeno de la *infodemia* se identifica como un elemento disruptivo nunca antes visto en tales magnitudes e incluye diversas facetas como la información sanitaria engañosa[1357], las teorías conspirativas que ponen en peligro la salud de las personas, las campañas desinformadoras acusando a grupos étnicos o religiosos de ser los causantes de la propagación de la COVID-19 con la consiguiente secuela de incitación al odio, el fraude a los consumidores a través de la venta de productos *milagrosos*, la ciberdelincuencia asociada a múltiples formatos -*phising*[1358], ransomware, etc.- o, incluso, las operaciones de influencia extranjera -en particular Rusia y China- para, aprovechando la pandemia, desacreditar el sistema democrático y tratar de mejorar su propia imagen de país.

Este contexto desinformativo, parasitario de la situación de crisis sanitaria mundial, obliga a la Unión a evaluar la eficacia e idoneidad de su respuesta acorde a la magnitud de las posibles repercusiones en la salud de las personas y la estabilidad de la sociedad

[1353] IBIDEM, página 23.

[1354] Comisión Europea. Comunicación conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La lucha contra la desinformación acerca de la COVID-19: contrastando los datos. JOIN(2020) 8 final. Bruselas, 10.6.2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020JC0008 (01/09/2024).

[1355] Este término es empleado por la OMS para referirse a la disponibilidad de una cantidad desmesurada de información sobre un determinado problema, llegando incluso a dificultar la búsqueda de una solución por saturación del receptor. La infodemia puede consistir en la difusión de simple información errónea, de desinformación interesada o de rumores durante una situación de emergencia sanitaria, como fue el caso de la COVID-19 que, alimentándose de los temores humanos más primarios, entorpece la adecuada respuesta de la sanidad pública y, al tiempo, genera a los ciudadanos confusión y desconfianza en las instituciones. Disponible en: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4 (07/09/2024).

[1356] La lucha contra la desinformación acerca de la COVID-19: contrastando los datos, Op. Cit., página 7.

[1357] Hay estudios académicos como "Cable news and COVID-19 vaccine uptake" que analizan y fundamentan la relación causal entre ver una determinada cadena de televisión -Fox News en este caso- y la baja tasa de vacunación de los espectadores, llegando así a vincularse la identificación partidista con la probabilidad de morir por coronavirus. Disponible en: Matteo Pinna, Léo Picard y Christoph Goessmann. Cable news and COVID-19 vaccine uptake. Sci Rep 12, 16804 (2022). https://doi.org/10.1038/s41598-022-20350-0 (07/09/2024)

[1358] El *phishing* es una técnica utilizada por los ciberdelincuentes que consiste en el envío masivo de correos electrónicos para *pescar* toda la información privada de las víctimas que, atraídas por el cebo del engaño, caigan en el fraude urdido o hagan clic en el enlace malicioso que se adjunta a la comunicación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

y sus propias instituciones, refiriendo a tal efecto las formas de combatir los distintos aspectos de la amenaza. En este sentido, se refiere la Comisión al refuerzo de la comunicación estratégica, a la mejora de la cooperación interna y externa de la UE para garantizar la coherencia y consistencia de su respuesta, al compromiso de las plataformas de redes sociales como elemento clave de la eficacia de dicha respuesta y el apoyo a los verificadores de datos como pilar del acceso a información fiable, entre otras.

Por ello, en la idea de ese decidido impulso a los verificadores de datos, se crea de manera simultánea el *European Digital Media Observatory* (EDMO)[1359], que se articula desde una red europea de centros de coordinación de verificadores de la que dependen distintos observatorios nacionales e internacionales, conformando un frente para la detección de campañas desinformadoras basado en el intercambio fluido de información, la identificación coordinada de narrativas y noticias falsas en cualquier tipo de canal, sin restricciones territoriales, y la puesta en común de las conclusiones de las investigaciones efectuadas para ello. De esta manera, el EDMO apoya a la comunidad de actores involucrados en la lucha contra la desinformación en línea, sobre la base de cuatro áreas principales de actividad contra la desinformación: 1) la verificación de datos; 2) la alfabetización mediática de los ciudadanos; 3) la investigación de la amenaza desinformativa por parte de profesionales independientes; 4) y el análisis de las políticas de los EEMM y de la UE para combatirla.

Concluye la Comisión Europea aludiendo a la puesta en marcha de todas estas medidas "allanando el camino para un planteamiento a más largo plazo enmarcado en el Plan de Acción para la Democracia Europea, que en principio se presentará hacia el final de este año, al igual que la futura Ley de Servicios Digitales"[1360], dando de esta manera entrada a dos iniciativas orientadas, respectivamente, a reforzar la resiliencia de las democracias de la UE frente a la desinformación y a la creación de un marco reglamentario en el que encuadrar la rendición de cuentas y la transparencia de todos aquellos actores que interactúan en el ciberespacio.

7.2.2.2. El Plan de Acción para la Democracia Europea

De acuerdo a la propuesta manifestada en la *Agenda Estratégica de la UE*, la Comisión presenta el 4 de diciembre de 2020 el *Plan de Acción para la Democracia Europea*[1361]

[1359] El Observatorio Europeo de Medios Digitales (EDMO por sus siglas en inglés) se constituye en la red europea de verificadores para contrarrestar la desinformación. Cuenta con 14 centros distribuidos en los 27 EEMM de la UE, Noruega y EE.UU. En España y Portugal es IBERIFIER (Iberian Digital Media Observatory) el observatorio de medios digitales vinculado al EDMO, coordinado por la Universidad de Navarra e integrado por universidades españolas y portuguesas -entre ellas el Instituto Universitário de Lisboa, la Universidad de Granada, la Universidad Politécnica de Madrid y la Universidad Politécnica de Valencia-, verificadores de ambos países como EFE Verifica, Maldita.es, Newtral, Polígrafo y Verificat, entre otros, y centros de investigación multidisciplinar -entre ellos el Real Instituto Elcano-. Disponible en: https://edmo.eu/
https://iberifier.eu/ (12/10/2024).

[1360] IBIDEM, página 18.

[1361] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción para la Democracia Europea. COM(2020) 790

Ediciones Universidad de Salamanca | CC BY-NC-ND

que, en su conjunto, supone un paquete de medidas con especial atención al empoderamiento de los ciudadanos y la participación social como mejor garantía para la resiliencia del modelo político del Estado de Derecho, por cuanto "la democracia no puede darse por sentada. Necesita ser cuidada y protegida de forma activa"[1362].

El *Plan de Acción para la Democracia Europea* pone encima de la mesa la afectación que la revolución digital supone para la política democrática, sus actores, sus procedimientos y sus garantías[1363], y propone una serie de medidas para impulsar la respuesta frente a estos retos digitales en base a tres pilares:

1. El *fomento de unas elecciones íntegras, libres y justas*, a través de la implementación de estándares de transparencia de la publicidad política con el objeto de poderla distinguir del resto de mensajes que no lo son, la revisión de la normativa aplicada a la financiación de los partidos políticos para combatir la financiación extranjera y sus sesgados intereses, el refuerzo de la cooperación entre los Estados Miembros y la UE para garantizar los procesos electorales y el fomento de la implicación ciudadana activa con la democracia día a día, más allá de las elecciones.
2. El *refuerzo de la libertad y el pluralismo de los medios de comunicación*, cuestión esencial para el funcionamiento de la democracia, actuando sobre la debida protección de la seguridad de los periodistas frente al acoso, la intimidación, el odio o la difamación, el apoyo frente a las demandas estratégicas contra la participación pública[1364], el decidido impulso de iniciativas de autorregulación en favor de los códigos deontológicos y profesionales del periodismo, y la vigilancia de la transparencia de la propiedad de los prestadores de servicios de comunicación.
3. La *lucha contra la desinformación* desde una estrategia de cooperación aún más estrecha entre los distintos actores involucrados -instituciones, sociedad civil, academia, industria privada, aliados internacionales-, la mejora y el continuo desarrollo de la gama de herramientas para contrarrestar la injerencia extranjera y las operaciones de influencia, el establecimiento de nuevas obligaciones a las plataformas en línea para la mejora de la transparencia en el uso de sus algoritmos y la rendición de cuentas a través de la Ley de Servicios Digitales y un Código Reforzado de Buenas Prácticas contra la Desinformación, la divulgación efectiva de datos para su análisis por los verificadores en el marco del

final. Bruselas, 3.12.2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423 (07/09/2024).

[1362] Plan de Acción para la Democracia Europea, Op. Cit., página 1.

[1363] En concreto, el Plan de Acción para la Democracia Europea se refiere a las nuevas posibilidades que la digitalización abre respecto a las formas de financiación no controladas para las campañas políticas, la vulnerabilidad de las infraestructuras electorales frente a los ciberataques, las redes sociales como factor polarizador de opinión y de incitación al odio, la manipulación de opinión mediante información falsa y, desde luego, las campañas desinformativas coordinadas por agentes externos, de carácter estatal o no. Plan de Acción para la Democracia Europea, Op. Cit., página 2.

[1364] Estas demandas contra la participación pública, SLAPP por sus siglas en inglés (*strategic lawsuit against public participation*), hacen referencia a pleitos infundados cuya verdadera intención es intimidar y silenciar a periodistas, activistas u opositores políticos críticos con los postulados del demandante, el cual busca que desistan de su postura ante la presión jurídica, el elevado coste de la defensa legal y la desgate social y para su credibilidad que supone mantener un pleito abierto. El objetivo no es otro que el demandado acabe abandonando su postura crítica o contraria al interés del demandante.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> Observatorio Europeo de los Medios de Comunicación Digitales (EDMO), y la alfabetización digital de los ciudadanos para que puedan interactuar en el ciberespacio guiados por un pensamiento crítico que les permita actuar de forma juiciosa, orientada, segura y ética.

Nuevamente se incide en la relevancia de los verificadores como parte de los mecanismos para luchar contra la desinformación cuando el Plan de Acción para la Democracia Europea, en su apartado 4.2., se refiere a la necesidad de:

> "[…] garantizar la divulgación efectiva de datos para la investigación sobre desinformación, desarrollando un marco acorde con los requisitos reglamentarios aplicables y basado en la participación de todas las partes interesadas (e independiente de la influencia política). El Observatorio Europeo de los Medios de Comunicación Digitales (EDMO) puede facilitar el desarrollo de dicho marco. La Comisión señala que, a priori y de forma generalizada, el RGPD no prohíbe a las plataformas que se compartan datos personales con los investigadores"[1365].

El Plan de Acción, que se publica prácticamente al mismo tiempo que se alcanza el Acuerdo definitivo entre la UE y el Reino Unido para regular la relación entre ambos a partir del Brexit, trata de ir más allá de los principales responsables de garantizar el buen funcionamiento de la democracia -las instituciones, los parlamentos y gobiernos nacionales-, buscando la corresponsabilidad y el compromiso del resto de actores involucrados en la defensa del modelo político como los partidos, los medios de comunicación, la sociedad civil y las plataformas en línea, por el relevante papel que cada uno de ellos está llamado a desempeñar en la lucha contra la desinformación.

7.2.2.3. La evaluación del Plan de Acción contra la Desinformación

Todo este esfuerzo para combatir los intentos de manipulación de la opinión pública y salvaguardar los pilares democráticos que sostienen la legitimidad de la Unión, llevan a sus instituciones a concluir que es preciso revisar periódicamente los instrumentos utilizados y actualizarlos en caso necesario para garantizar su eficacia a largo plazo[1366], toda vez que la desinformación es una amenaza en constante evolución que se adapta rápidamente a cualquier cambio que pueda beneficiarle en la consecución de sus objetivos desestabilizadores.

Es por ello que, el 27 de abril de 2021, el Tribunal de Cuentas Europeo presenta su Informe Especial titulado *El impacto de la desinformación en la UE: una cuestión*

[1365] Plan de Acción para la Democracia Europea. Op. Clt., páginas 27 y 28. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423 (12/10/2024).

[1366] Sirva como ejemplo lo apuntado por el Consejo de la Unión Europea en el considerando 30 de sus Conclusiones sobre las acciones complementarias para aumentar la resiliencia y luchar contras las amenazas híbridas. Bruselas, 10 de diciembre de 2019. 14972/19. Disponible en: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/es/pdf (08/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

abordada, pero no atajada [1367] que supone la primera evaluación del *Plan de Acción contra la desinformación* de 2018. Sus conclusiones son relevantes por cuanto sacan a la luz los resultados sobre la pertinencia e implantación práctica de las diez acciones propuestas en el referido Plan, declarando al respecto que:

> "[…] el Plan de Acción de la UE resultó pertinente, pero incompleto y, a pesar de que su aplicación se ajusta en gran medida a las previsiones y de que existen pruebas que demuestran que se están produciendo avances positivos, determinados resultados no se han alcanzado según lo previsto"[1368].

En su auditoría del *Plan de Acción contra la desinformación* el Tribunal de Cuentas Europeo señala como principales cuestiones a mejorar las siguientes:

1. El Plan de Acción no se ha actualizado desde su presentación en diciembre de 2018, cuando nació con un enfoque adecuado para abordar la desinformación de ese momento conforme al criterio de expertos y partes interesadas. Sin embargo, pese a la rápida y permanente evolución de dicha amenaza, el Plan no siguió esa misma dinámica adaptativa y fue por ello rápidamente superado.
2. El Plan no contiene mecanismos específicos apoyados en un procedimiento *ad hoc* para articular de manera eficaz y efectiva la coordinación de la respuesta europea contra la desinformación, cuyo nivel de amenaza puede variar sensiblemente en cuanto a tipología, alcance y dimensión.
3. Tampoco contempla el Plan de Acción un marco de seguimiento con objetivos claros, de evaluación mediante indicadores medibles y de readaptación continua a través de las *lecciones aprendidas*, que se corresponda con la evolución del entorno geopolítico, el cambio de la amenaza y las respuestas ofrecidas por la Unión. A ello hay que sumar la falta de presupuesto específico y estable a largo plazo para poder acometer las funciones y tareas que, de manera recurrente, hay que atender para combatir la desinformación conforme dispone el propio Plan.
4. El compromiso de las plataformas en línea con el *Código de Buenas Prácticas* de 2018 no ha sido el esperado, habiéndose quedado en el ámbito meramente informal. El propio carácter autorregulatorio y discrecional del Código, unido a la ausencia de uniformidad en su aplicación y la falta de claridad de algunos de sus conceptos, entre otras cuestiones, han resultado claves para no haber conseguido que las plataformas mejoraran en cuanto a la transparencia del funcionamiento de sus algoritmos y rindieran cuentas de su gestión activa contra la desinformación.
5. La falta de una auténtica estrategia de comunicación y alfabetización mediática[1369] para el estímulo de la resiliencia y la concienciación social frente a la desinformación y sus graves efectos.

[1367] Tribunal de Cuentas Europeo. Informe Especial 9/2021 El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada. 2021/C 215/06. Disponible en: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_ES.pdf (01/09/2024).

[1368] IBIDEM, página 4.

[1369] Como ejemplo de ello se refiere el Informe del Tribunal de Cuentas Europeo a la falta de interés que ha despertado entre los actores afectados el Observatorio Europeo de Medios Digitales (EDMO), concebido punto de encuentro entre verificadores de datos, expertos en alfabetización mediática, investigadores académicos, plataformas en línea y medios de comunicación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Con esta evaluación el Tribunal de Cuentas pone en valor el esfuerzo realizado por la UE y sus EEMM para responder frente a la desinformación como amenaza para su seguridad y la del modelo democrático de organización social, mediante la implementación de medidas y acciones que mitiguen su impacto y protejan de sus efectos, las cuales deben estar en permanente estado de revisión para poder adaptarse de manera rápida y flexible a la naturaleza cambiante de esta amenaza.

Sin embargo, parece obviarse el hecho de que este frente de acción contra la amenaza desinformativa, para ser realmente efectivo, debe trascender el ámbito de las propias instituciones comunitarias y nacionales por cuanto que, más allá de estas, existen diferentes actores y organismos que si bien no pertenecen *stricto sensu* a la UE, sí actúan como socios preferentes en materia de seguridad y defensa, desarrollando políticas de cooperación y respuesta conjunta ante las amenazas híbridas en general. En este sentido, quedan fuera de este análisis las iniciativas desarrolladas por el Hybrid CoE, paradigma de la colaboración en esta materia entre la UE y la OTAN, por las entidades privadas, como IBERIFIER respecto a las dedicadas a la verificación de contenidos, y la sociedad civil, presente en foros y grupos de trabajo interdisciplinares, lo cual supone la pérdida de visión sobre una parte importante de las capacidades reales de actuación (SABATER QUINTO, BELMONTE MARTÍN, & LLORET IRLES, 2025, págs. 13-14).

7.2.2.4. La Caja de Herramientas Híbrida de la Brújula Estratégica

En esta demanda de una línea europea de acción conjunta ante la desinformación se presenta en marzo de 2022 la *Brújula Estratégica para la Seguridad y la Defensa*[1370] que, en el marco de la PCSD y de la obligada reacción ante la nueva bofetada de Rusia a Europa a través de la invasión de Ucrania, es muy consciente de que debe poder implementarse de manera realista. Por ello, la nueva estrategia integra esta visión a través de la creación de la *EU Hybrid Toolbox* (EUHT)[1371], un conjunto de herramientas -civiles y militares- que la Unión ofrece a los Estados miembros para complementar su respuesta ante un ataque de carácter híbrido, de manera proporcional, integral y coordinada. Y es precisamente este último elemento el que suscita su valor diferencial, por cuanto:

> "The main added value of the EUHT is perhaps less in assisting individual member states with their national response, than in responding in the spirit of «a hybrid attack against one is a hybrid attack against all». One of the objectives of the Toolbox is to make the EU and its members more resilient, in order to strengthen deterrence by making them less easy targets. The other is to provide a doctrine to actively respond to and push back hybrid threat actors" (LASOEN, 2022, pág. 3)[1372].

El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada, Op. Cit., página 46.

[1370] Ver Capítulo 3, apartado 3.3.3.

[1371] Ver Capítulo 3, apartado 3.3.3. y apartado 5, donde se cita la Caja de Herramientas Híbridas de la UE.

[1372] "El principal valor añadido de la EUHT probablemente consista no tanto en ayudar a los Estados miembros individuales en su respuesta nacional como en responder con el espíritu de «un ataque híbrido contra uno es un ataque híbrido contra todos». Uno de los objetivos de la Caja de Herramientas es hacer a la UE y sus miembros más resilientes, con el fin de reforzar la disuasión convirtiéndolos en objetivos

Ediciones Universidad de Salamanca | CC BY-NC-ND

Asimismo, los propios Estados miembros coinciden en que otro de los valores añadidos de la EUHT es que proporciona un marco de aplicación coherente de estas herramientas de respuesta -internas y externas- que, enfocado a su adaptación al caso concreto, integraría cinco tipos de medidas (LASOEN, 2022, pág. 7):

1. Las medidas preventivas, orientadas al desarrollo de capacidades.
2. Las medidas de cooperación y coordinación con países aliados y la OTAN.
3. Las medidas de estabilidad, a través de la utilización de mecanismos de diplomacia, misiones y operaciones de PCSD o de comunicación estratégica, entre otras).
4. Las medidas restrictivas, entre las que se encuentran las encaminadas a la atribución del ataque y la determinación de las sanciones aplicables.
5. Las medidas de asistencia y solidaridad entre Estados.

Entre estas herramientas están los informes del SEAE relativos a la amenaza de *Manipulación de la Información e Interferencia Extranjera*[1373] con los que, a través del análisis de caso específicos, se desarrollan taxonomías y procedimientos estandarizados para interpretar la amenaza y determinar el marco de respuesta adecuado, con especial incidencia en la cooperación entre los Estados miembros y el resto de las partes interesadas.

Aprovechando este entorno propicio, en octubre de 2022 los verificadores de datos europeos se unen en torno al European Fact-Checking Standards Network (EFCSN) con los objetivos de unificar procedimientos, promover unos elevados estándares de calidad en la verificación de datos y contribuir a la educación mediática, ofreciendo al público información contrastada y confiable. Para llevar a cabo este compromiso redactan el Código Europeo de Estándares de verificación, entendido como.

> "[…] conjunto de criterios diseñados para garantizar que las organizaciones que verifican información errónea y desinformación cumplan con los más altos estándares de metodología, ética y transparencia para servir mejor al interés público"[1374].

Sin embargo, como señala Kenneth Lasoen, no resulta sencillo conjugar una respuesta europea rápida y coherente a través de la aplicación del conjunto de herramientas híbridas y de ciberdiplomacia entre las diferentes opciones nacionales de ámbito político y de seguridad -interna y externa-, entre otras. Hay que tener presente no solo el alto nivel de ambición de la *Brújula Estratégica*, sino también la dificultad que entraña diseñar un procedimiento de toma de decisiones ágil e inequívoco que case con las diferentes posiciones nacionales ante la aplicabilidad de la EUHT y su marco

menos fáciles. La otra es proporcionar una doctrina para responder activamente y hacer retroceder a los actores de amenazas híbridas" (Traducción propia).

[1373] Ver Capítulo 6, apartado 6.2.3. donde se estudian los tres Informes de amenaza FIMI del SEAE que se han publicado por ahora.

[1374] La Red Europea de Normas de Verificación de Datos (EFCSN por sus siglas en inglés) es una asociación sin ánimo de lucro, con sede en París, que aglutina a 49 organizaciones a día de la fecha de consulta, entre las que se encuentran las españolas Maldita.es, Verificat, Newtral, Infoveritas y EFE Verifica. Disponible en: https://efcsn.com/ (12/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

terminológico de referencia. Si este reto llega a alcanzarse, el beneficio será para todos aquellos que se unan para contrarrestar de manera conjunta la amenaza y, al tiempo, la Unión logrará dar un importante paso adelante en su ansiada autonomía estratégica y de defensa, por cuanto se consolidaría:

> "[…] as a comprehensive and powerful actor to deal with those complex crises which are beyond the capabilities of individual states, and improve the chances of countering the hybrid attempts undermining international order" (LASOEN, 2022, pág. 10)[1375].

Por ese convencimiento en el beneficio del desarrollo conjunto y colaborativo de capacidades bajo una dirección única orientada a la seguridad de todos los EEMM, el Libro Blanco de la Defensa Europea, presentado en marzo de 2025, se refiere a la desinformación como una de las principales amenazas híbridas consustanciales al actual entorno de competencia sistémica que requiere una respuesta estratégica. Uno de los pilares de ésta habrá de ser, indefectiblemente, ser capaces de mantener, atraer y desarrollar el talento con el que liderar la innovación disruptiva en campos de aplicación directa a la seguridad como la IA, factor clave para la implementación de herramientas que pueden ayudar a mitigar los efectos de las campañas desinformativas.

7.2.2.5. El Código Reforzado de Buenas Prácticas contra la Desinformación

Alineado con esta estrategia de involucrar a todos los actores, en junio de 2022 se publica el *Código Reforzado de Buenas Prácticas contra la Desinformación*[1376] que, como principal avance, busca integrar el compromiso de las grandes plataformas en línea para la mayor calidad de sus servicios con el marco de protección de los usuarios que establece la Ley de Servicios Digitales[1377], siendo su principal objetivo afrontar los riesgos derivados de estas relaciones, entre ellos el de la desinformación, fenómeno en el que también se incluyen la información errónea o no contrastada, las operaciones de influencia y la injerencia extranjera en el espacio de la información[1378].

Otras novedades sobre el anterior Código de 2018 son:

1. La posibilidad que se brinda a aquellos otros sectores -como el de la publicidad o el comercio electrónico- y a las plataformas en línea de menor tamaño e implantación en el mercado, de suscribir un compromiso flexible y dimensionado

[1375] La UE se consolidaría "como un actor integral y poderoso para hacer frente a esas crisis complejas que están más allá de las capacidades de los Estados individuales, y mejorar así las posibilidades de contrarrestar los intentos de ataque híbridos que socavan el orden internacional" (Traducción propia).

[1376] Código Reforzado de Buenas Prácticas contra la Desinformación. Junio 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (14/09/2024).

[1377] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). DOUE L 277/1, de fecha 27.10.2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065 (14/09/2024).

[1378] Código Reforzado de Buenas Prácticas contra la Desinformación, Op. Cit., página 1.
En este sentido, debemos llamar la atención sobre el hecho de que la desinformación no engloba la sátira, la parodia ni los errores de cita, como corresponde a un modelo jurídico que vela por la libertad de expresión y el pluralismo de los medios de comunicación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

de acuerdo a sus recursos, su volumen de negocio y la naturaleza de sus servicios[1379].

2. El compromiso de los firmantes para impedir el uso de la publicidad como herramienta desinformadora, mediante el control financiero de los anuncios y sus patrocinadores y la mejora de la transparencia entre los diferentes actores de la cadena publicitaria con el objetivo final de desmonetizar dicha amenaza[1380].
3. Respecto a los anuncios políticos y temáticos, se considera prioritaria una armonización de conceptos y de enfoque a nivel de plataformas[1381] para evitar asimetrías en la aplicación de los parámetros de control y etiquetado de la publicidad de cara a la protección de los usuarios. Se trata, en definitiva, de ofrecer a estos una información transparente y comprensible sobre las razones por las cuales ven un determinado anuncio político o temático[1382].
4. Se señala el compromiso de las plataformas para mejorar la alfabetización mediática y dotar a los usuarios de herramientas para detectar contenidos falsos o engañosos, marcarlos y denunciarlos fácilmente a través de sus servicios[1383].
5. El nuevo Código Reforzado también establece un compromiso de las plataformas para facilitar el acceso a sus datos por parte de la comunidad investigadora de la desinformación y el apoyo a sus actividades, como vector de eficacia de la estrategia contra dicha amenaza[1384].
6. Igualmente, se señala el compromiso de las plataformas con los verificadores de datos a través de un marco colaborativo transparente, abierto, igualitario y financieramente sostenible, fruto del cual las empresas firmantes integrarán los resultados de aquellos en sus procesos y contenidos para mejorar la calidad de sus servicios y medir el impacto real de la verificación de datos aplicada[1385].
7. La creación de un Centro de Transparencia a disposición de los ciudadanos para garantizar la claridad de los procesos -de inserción de anuncios, de gestión de datos personales, etc.- y la rendición de cuentas en cuanto a la aplicación del Código[1386].
8. Muy novedosa también es la constitución de un Grupo de Trabajo Permanente con el objeto de evolucionar el Código Reforzado para mantenerlo adaptado a la realidad social determinada por los avances técnicos y legislativos para, conforme a ello, poder actualizar los compromisos de los firmantes[1387].
9. Y, en último lugar, la definición de un marco de seguimiento específico para valorar la aplicación del Código Reforzado y su impacto en la reducción efectiva de la desinformación, mediante informes periódicos de evaluación de la implementación de los compromisos firmados y la medición de indicadores de servicio[1388].

[1379] IBIDEM, página 2.
[1380] IBIDEM, página 5.
[1381] Ciertamente sería también necesaria una unificación de los criterios de los Estados de la UE a la hora de definir los contenidos a los que no deben estar asociados los anuncios.
[1382] Código Reforzado de Buenas Prácticas contra la Desinformación, Op. Cit., página 10.
[1383] IBIDEM, página 18.
[1384] IBIDEM, página 26.
[1385] IBIDEM, página 31.
[1386] IBIDEM, página 35.
[1387] IBIDEM, página 36.
[1388] IBIDEM, página 39.

Ediciones Universidad de Salamanca | CC BY-NC-ND

El nuevo Código Reforzado viene así a consolidar una forma de entender la estrategia contra la desinformación que no se limita exclusivamente a la lucha contra los comportamientos ilegítimos, sino que abarca un amplio espectro de acción para defender los derechos y valores de la democracia, para lo cual necesita el compromiso de los ciudadanos y de todos los actores involucrados, en este caso las plataformas y suministradores de servicios en línea[1389], en proporción a la naturaleza de sus prestaciones y su dimensión operacional. Además, consciente de la necesidad de poder evaluar los progresos y su impacto para tener una visión real de los objetivos alcanzados en la respuesta a la desinformación en línea, el Código Reforzado acuerda la utilización de indicadores clave de desempeño[1390] que permitan dicho control, al tiempo que instaura la obligación de reportar a través de informes periódicos los resultados del análisis de seguimiento de los compromisos de cada signatario en cada Estado miembro.

7.2.3. La recuperación del tiempo perdido: la Ley de Servicios Digitales

Este ecosistema europeo de plataformas de servicios en línea, empresas de publicidad y mercantiles digitales, de instituciones de observación como el EDMO, de verificadores de datos y de normativa reguladora *ad hoc* para la lucha contra la desinformación no se puede entender sin referirnos al *Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales*, también llamado *Ley de Servicios Digitales* (DSA)[1391], norma de referencia de la Unión que trata de *recuperar el tiempo perdido* en lo relativo a la regulación del ciberespacio y la delimitación del poder que han consolidado las grandes plataformas a través de las redes sociales y la intermediación de servicios en línea. En este contexto hay que entender este marco normativo armonizador que provee de garantías jurídicas tanto a los consumidores[1392] como a los propios prestadores de servicios intermediarios[1393] en

[1389] Las plataformas que participan y han firmado el Código Reforzado de Buenas Prácticas contra la Desinformación se ha ampliado respecto a las que lo hicieron en el 2018, con la posibilidad de que sigan incorporándose nuevos signatarios. En junio de 2022 firmaron las grandes como Adobe, Google, Meta (Facebook, Instagram y WhatsApp), Microsoft y Tik Tok, pero también otras compañías como la verificadora Maldita.es. Disponible en: https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation (14/09/2024).

[1390] Estos indicadores son de dos tipos: los indicadores de nivel de servicio (SLI) y los de información cualitativa (QRE). Como ejemplos podemos citar el número de denuncias de informaciones falsas, la cantidad de contenidos comprobados por verificadores independientes, la cuantía de acciones de mitigación y respuesta de la plataforma en la protección de la integridad de sus servicios o el número de medidas de transparencia puestas en marcha por la plataforma.
Código Reforzado de Buenas Prácticas contra la Desinformación, Op. Cit., página 39.

[1391] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). Diario Oficial de la Unión Europea L 277/1, de 27.10.2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065 (12/10/2024).

[1392] El artículo 3.c) de la DSA define *consumidor* como "toda persona física que actúe con fines ajenos a su actividad comercial, negocio, oficio o profesión". Por otra parte, los *destinatarios del servicio* se conceptualizan en el apartado b) como "toda persona física o jurídica que utilice un servicio intermediario, en particular para buscar información o para hacerla accesible".

[1393] Conforme al artículo 3.g) de la DSA los *servicios intermediarios* en la sociedad de la información pueden ser de tres tipos: de "mera transmisión", de "memoria caché" o de "alojamiento de datos".

Ediciones Universidad de Salamanca | CC BY-NC-ND

la UE, con independencia de su lugar de establecimiento o ubicación[1394], a través de un conjunto de obligaciones, responsabilidades y medidas orientadas, entre otras, a abordar la difusión de contenidos ilícitos en línea[1395] y los riesgos para la sociedad derivados de la desinformación[1396] con el fin de alcanzar un ciberespacio seguro, predecible y confiable.

Con este objetivo, la DSA ofrece un marco conceptual preciso para interpretar las relaciones entre estos nuevos modelos de negocio y servicios en línea tan importantes para la sociedad de la información, las normas y condiciones que regulan la prestación de servicios en el mercado interior europeo y la defensa de los derechos garantizados en la Carta de Derechos Fundamentales de la Unión, especialmente la libertad de expresión y de información, la libertad de empresa, el derecho a la no discriminación y la protección de los consumidores[1397].

Así, se define la responsabilidad y las obligaciones de diligencia debida para favorecer la transparencia de las plataformas, luchar contra los contenidos delictivos y, en definitiva, poder trazar la actividad de prestación de servicios en línea[1398] con la finalidad de identificar al proveedor de este tipo de contenidos y actuar contra él en caso de ser necesario para la defensa de los derechos del consumidor. En este mismo sentido, y con la idea de graduar proporcionalmente el nivel de exigencia para las pequeñas y grandes empresas, se establecen obligaciones adicionales para las plataformas en línea *de muy gran tamaño*[1399] como la de llevar a cabo evaluaciones de riesgo anuales para evitar abusos de sus sistemas [1400], adoptar las correspondientes medidas para mitigarlos[1401], someterse a auditorias independientes para evaluar el cumplimiento de sus obligaciones[1402], ofrecer a los usuarios información suplementaria sobre la publicidad en línea que presentan[1403] y otras obligaciones de transparencia informativa[1404].

Supone un avance importante por parte de la DSA el señalamiento impositivo de una *tasa de supervisión anual*[1405], que la Comisión cobrará a estas plataformas en línea *de muy gran tamaño* para cubrir los costes derivados del cumplimiento de las funciones supervisoras que ésta tiene, así como también el establecimiento de estructuras específicas para hacer valer su acatamiento, como los *coordinadores de servicios*

[1394] IBIDEM, Considerando (7) y artículo 2.
[1395] El concepto de *contenido ilícito* se define de manera amplia en el artículo 3.h) de la DSA, como "toda información que, por sí sola o en relación con una actividad, incluida la venta de productos o la prestación de servicios, incumpla el Derecho de la Unión o el Derecho de cualquier Estado miembro que cumpla el Derecho de la Unión, sea cual sea el objeto o carácter concreto de ese Derecho".
[1396] IBIDEM, Considerando (9).
[1397] IBIDEM, Considerando (3) y artículo 2.
[1398] IBIDEM, artículo 30.
[1399] Conforme al artículo 33 de la DSA son aquellas que "tengan un promedio mensual de destinatarios del servicio activos en la Unión igual o superior a cuarenta y cinco millones".
[1400] IBIDEM, artículo 34.
[1401] IBIDEM, artículo 35.
[1402] IBIDEM, artículo 37.
[1403] IBIDEM, artículo 39.
[1404] IBIDEM, artículo 42.
[1405] IBIDEM, artículo 43.

Ediciones Universidad de Salamanca | CC BY-NC-ND

digitales[1406] o la *Junta Europea de Servicios Digitales*[1407]. Igualmente es obligado reseñar el impulso que se pretende del *voluntario cumplimiento de la norma* por parte de las plataformas, el cual se busca a través de la elaboración de *códigos de conducta voluntarios*[1408] a través de los que fijar compromisos de adopción de medidas específicas para la reducción de riesgos, el control de la publicidad en línea[1409] o la mejora del acceso a los servicios[1410]. En este punto tiene especial cabida la firma por estos intermediarios digitales del *Código Reforzado de Buenas Prácticas contra la Desinformación,* que puede operar perfectamente como uno de estos códigos de conducta voluntarios que dan cuerpo a la iniciativa para contribuir a la debida aplicación de la DSA, dando cuerpo así a la visión holística de la UE con la que afrontar la amenaza desinformativa.

Una cuestión que nos parece de especial notoriedad y que pone de relieve la preocupación de la Unión por mantener su capacidad efectiva de adaptación frente a la naturaleza cambiante de la amenaza, es el mecanismo de respuesta a situaciones de crisis que puede conllevar la exigencia a las plataformas en línea *de muy gran tamaño* de la adopción, en un breve plazo temporal, de determinadas medidas entre las que se encuentren, por ejemplo, la moderación de contenidos y el aumento de recursos dedicados a dicha tarea, la adaptación de los algoritmos pertinentes y los sistemas publicitarios, o la adopción de medidas de concienciación, entre otras[1411].

Para hacer efectivo este conjunto de garantías, obligaciones y responsabilidades se prevén mecanismos para la moderación de contenidos y vías para que los usuarios defiendan sus derechos[1412], así como la posibilidad de imponer sanciones efectivas, proporcionadas y disuasorias a estas grandes empresas, siendo ejemplo de ello las multas por cuantías de hasta el 6% de su volumen de negocios mundial[1413], para cuya aplicación se valorará el carácter sistemático o recurrente de la infracción, su naturaleza intencionada o negligente y el ámbito de actuación territorial del prestador del servicio[1414].

[1406] Los coordinadores de servicios digitales son los responsables, conforme al artículo 49 de la DSA, de "todas las materias relacionadas con la supervisión y garantía del cumplimiento del presente Reglamento" en cada uno de los Estados miembros, y están obligados a cooperar entre ellos para dar respuesta a las infracciones de un prestador de servicio con implicaciones transfronterizas para los derechos de los ciudadanos, tal y como señala el artículo 58, de manera que puedan hacer efectiva su encomienda para adoptar medidas eficaces y proporcionadas con las que corregir aquellas infracciones particularmente graves y persistentes.

[1407] La Junta Europea de Servicios Digitales es, según el artículo 61 de la DSA, "un grupo consultivo independiente integrado por coordinadores de servicios digitales para la supervisión de los prestadores de servicios intermediarios".

[1408] IBIDEM, artículo 45.

[1409] IBIDEM, artículo 46.

[1410] IBIDEM, artículo 47.

[1411] El artículo 36 de la DSA considera que se ha producido una *crisis* "cuando se produzcan circunstancias extraordinarias que den lugar a una amenaza grave para la seguridad pública o la salud pública en la Unión o en partes significativas de esta". Por su parte, el Considerando (91) señala que estas crisis pueden derivarse de conflictos armados -en clara referencia a la guerra de Ucrania-, actos de terrorismo, catástrofes naturales, pandemias u cualquier otra amenaza transfronteriza grave para la salud pública.

[1412] IBIDEM, artículos 53 y 54.

[1413] IBIDEM, artículos 52 y 74.

[1414] IBIDEM, Considerando (117).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Al mismo tiempo, debemos señalar que la DSA tiene su complemento esencial en un grupo de normas entre las que se encuentran la Ley de Mercados Digitales (DMA)[1415] y la Directiva para garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS 2)[1416] que, entre otras cuestiones, abordan la seguridad de los usuarios en línea y el impacto de las plataformas en sus derechos fundamentales, estableciendo un marco de gobernanza para la gestión del ciberespacio de manera justa y abierta en todo el territorio de la UE, creándose al efecto estructuras como la Red Europea de Organizaciones de Enlace para la Cibercrisis (EU-CyCLONe)[1417], que refuerza la resiliencia de los sistemas de información y la capacidad de respuesta ante incidentes críticos de ciberseguridad.

Por todo ello, podemos concluir que la DSA es la respuesta -un poco tardía- de la UE ante la realidad de los nuevos modelos de negocio y servicios digitales que mueve la sociedad de la información que permite a los ciudadanos, en su rutina diaria, compartir noticias, acceder a datos, efectuar transacciones y relacionarse entre ellos a través de una novedosa dimensión digital y cibernética que, aunque privilegiada con claras ventajas y oportunidades, también entraña destacables riesgos y desafíos de seguridad para la sociedad en su conjunto que deben ser afrontados desde una estrategia europea integradora y, al tiempo, respetuosa con sus principios.

[1415] El Reglamento de Mercados Digitales (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828. Diario Oficial de la Unión Europea L 265/1, de 12.10.2022. Su artículo 1.1. establece que "La finalidad del presente Reglamento es contribuir al correcto funcionamiento del mercado interior estableciendo normas armonizadas que garanticen a todas las empresas, en toda la Unión, la equidad y la disputabilidad de los mercados en el sector digital donde haya guardianes de acceso, en beneficio de los usuarios profesionales y los usuarios finales". Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A265%3ATOC&uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG (20/10/2024).

[1416] La Directiva NIS 2 (UE) 2022/2555 del Parlamento Europeo y del Consejo, del 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148. DOL L 333 de 27.12.2022, p.80. En su artículo 1.2. señala que para llevar a cabo las medidas destinadas a lograr ese elevado nivel común de ciberseguridad en toda la Unión, con vistas a mejorar el funcionamiento del mercado interior, esta Directiva NIS 2 establece "(a) obligaciones que exigen a los Estados miembros adoptar estrategias nacionales de ciberseguridad y designar o establecer autoridades competentes, autoridades de gestión de crisis cibernéticas, puntos de contacto únicos en materia de ciberseguridad (puntos de contacto únicos) y equipos de respuesta a incidentes de seguridad informática (CSIRT); (b) medidas de gestión de riesgos de ciberseguridad y obligaciones de información para las entidades de un tipo mencionado en el anexo I o II, así como para las entidades identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557; (c) normas y obligaciones sobre el intercambio de información en materia de ciberseguridad; (d) obligaciones de supervisión y ejecución de los Estados miembros". Disponible en: https://eur-lex.europa.eu/eli/dir/2022/2555 (20/10/2024).

[1417] El artículo 16 de la NIS 2 es la base de esta Red Europea de Organizaciones de Enlace para la Cibercrisis (EU-CyCLONe), integrada por representantes de las autoridades de gestión de crisis cibernéticas de los Estados miembros y, también, de la Comisión en caso de incidente que pueda tener un impacto significativo en los servicios y actividades incluidos en el ámbito de aplicación de la NIS 2. Su objetivo es fomentar la colaboración y el intercambio de información para obtener un conocimiento acertado del estado de situación de la ciberamenaza basado en las herramientas y el apoyo que ofrece la Agencia de Ciberseguridad de la UE. Disponible en: https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone (22/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

7.3. La injerencia extranjera en las democracias europeas

La injerencia de un Estado extranjero en el proceso de elecciones democráticas de otro a través de ciberoperaciones maliciosas enmarcadas en una campaña de influencia, desprestigio o desinformación, con el objetivo de apoyar a determinadas opciones políticas o candidatos para obtener algún tipo de ventaja o, simplemente, generar dudas sobre la legitimidad del proceso o sus instituciones, supone para países como, por ejemplo, Alemania y Dinamarca, una violación de su soberanía y constituye un hecho ilícito internacional equiparable, en el plano físico, al apoyo a la insurgencia que, tradicionalmente, se interpreta como coerción desde el Derecho Internacional, tal y como vimos en el Capítulo 5 al estudiar el uso de las operaciones cibernéticas maliciosas en las relaciones entre Estados[1418].

En este contexto europeo de preocupación institucional -y social- por la salud de la democracia y la amenaza desinformativa que la constriñe, es necesario disponer de datos y variables medibles que permitan tomar el pulso a la opinión pública para poder adoptar soluciones adecuadas. Es por ello que en 2023 la Comisión Europea encarga una encuesta[1419] para monitorizar el sentir de los ciudadanos en cuanto a, por un lado, el estado de la democracia en la UE y sus Estados miembros y, por otro, la percepción de la amenaza para las instituciones sobre las que se sustenta.

Respecto a la primera de las cuestiones, el 47% de los europeos se sienten entre *muy* y *algo satisfechos* con el funcionamiento de la democracia en su país, frente al 51% que se declara *no muy* o *nada satisfechos*. Es un resultado equilibrado, aunque con un amplio margen de mejora para alcanzar mejores niveles de satisfacción, sobre todo teniendo en cuenta que se trata de un parámetro esencial, como es la percepción de la base del sistema político europeo por parte de sus ciudadanos. Sobre los elementos que caracterizan a unas elecciones libres y justas, los encuestados valoran como principal el acceso a información precisa y veraz para que los votantes puedan decidir en base a un criterio bien formado (51%), que la administración electoral sea imparcial e independiente (47%) y que su infraestructura está protegida frente a amenazas como los ciberataques (36%). Lo más valorado del *fair play* en los debates y campañas electorales es la evitación del discurso de odio, la manipulación y la mentira (46%). Conforme a estos datos, podemos decir que los ciudadanos europeos señalan a la desinformación y a la ciberamenaza como principales factores desestabilizadores para los procesos electorales de sus países y de la propia UE.

En cuanto a los resultados que ofrece la encuesta sobre el segundo asunto, la percepción sobre la amenaza a las instituciones democráticas europeas, muestran un estado de opinión claramente preocupada, de igual manera, por la información falsa y la posible

[1418] Ver Apartado 5.3.2.2.

[1419] Se trata del Eurobarómetro Flash 522 - Democracia, cuyo estudio de campo se hizo en marzo de 2023 y la publicación de resultados en diciembre del mismo año. Este tipo de encuestas *flash* tienen una temática concreta y relevante, y se realizan *ad hoc* en un breve periodo de tiempo, utilizando como método de trabajo principal las entrevistas telefónicas o en línea. Disponible en: https://data.europa.eu/data/datasets/s2966_fl522_eng?locale=en (22/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

afectación a los procesos electorales. En este sentido, se recogen datos que advierten sobre el hecho de que el 38% de los encuestados consideran que la amenaza más grave para la democracia en Europa es la información falsa o engañosa en general que circula por Internet o en el ámbito físico tradicional, seguida por la desconfianza y el escepticismo hacia las instituciones democráticas (32%), y la falta de compromiso o interés por parte de los ciudadanos con la política y las elecciones (26%). Asimismo, resulta paradigmático que, en el periodo de la última semana, el 68% de los encuestados se consideren de alguna forma expuestos a la desinformación y las *fake news* (el 33% *a veces*, el 22% *a menudo* y el 13% *muy a menudo*), así como que sean las redes sociales las que concentren la mayor probabilidad de difundirlas (un 64%, frente al segundo de los medios considerados como desinformativos, la televisión, con un 36%). Por último, en cuanto a las plataformas digitales y su vínculo con la difusión de información falsa o engañosa, un 52% de los europeos encuestados consideran que éstas deberían hacer más para prevenirla y atajarla, siendo por ello que el 42% opina que los usuarios deben asumir el rol de autoverificadores de la información antes de compartirla con otras personas, y un 39% señala que habría que aprender a distinguir mejor entre la información *veraz y confiable* de la *falsa o engañosa*.

7.3.1. Una respuesta conjunta ante una amenaza diversificada

Un ejemplo de la materialización de esta estrategia europea coordinada y multinivel contra la manipulación de la información y los nuevos desafíos, cada vez más controvertidos y sistémicos, es el reforzamiento de la implicación del Parlamento Europeo que se refleja en la creación de la primera *Comisión Especial sobre la Injerencia Extranjera en todos los Procesos Democráticos de la Unión Europea, incluida la Desinformación* (INGE 1)[1420], de cuyo trabajo emana la *Resolución del Parlamento Europeo de 9 de marzo de 2022 sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación*[1421], en la que, pese a haberse elaborado con anterioridad a la invasión rusa de Ucrania, aboga por una estrategia coordinada frente a esta, al tiempo que:

> "Expresa su profunda preocupación por la creciente incidencia y la naturaleza cada vez más sofisticada de las injerencias extranjeras y los intentos de manipulación de la información dirigidos contra todos los ámbitos del funcionamiento democrático de la Unión Europea y sus Estados miembros, llevados a cabo mayoritariamente por Rusia y China"[1422].

[1420] La INGE 1 se constituye tras la Decisión del Parlamento Europeo de, 18 de junio de 2020, sobre la constitución, competencias, composición numérica y duración del mandato de la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación (2020/2683(RSO)). Esta Comisión Especial debía elaborar un informe con conclusiones y recomendaciones sobre las medidas e iniciativas a adoptar para luchar contra la injerencia extranjera y la desinformación en el ámbito de la UE. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020DP0161 (24/10/2024).

[1421] Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2020/2268(INI)). P9_TA(2022)0064. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022IP0064 (28/08/2024).

[1422] IBIDEM, Considerando 1, página 347/73.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Esta Resolución identifica y describe la amenaza de la interferencia extranjera en todas sus formas y aporta un diagnóstico de las vulnerabilidades de la UE, así como las recomendaciones para hacerles frente. Por ello se crea la INGE 2[1423], una nueva Comisión Especial con mandato modernizado para, desde la cooperación y el diálogo interinstitucional[1424], contribuir a la resiliencia de la Unión frente a la amenaza híbrida y la desinformación en la fase previa a las elecciones europeas de 2024. Esta Comisión Especial eleva *Propuesta de Resolución* al Parlamento Europeo en mayo de 2023[1425], pidiendo a los Estados miembros "que reconozcan que la injerencia extranjera, incluida la desinformación, es una amenaza para la seguridad nacional y transfronteriza"[1426].

Dicha propuesta cristaliza un mes más tarde en la *Resolución del Parlamento Europeo sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación*[1427], donde se hace eco de la anterior propuesta de 2022 que propugnaba la adopción de una estrategia coordinada de prevención ante la influencia de terceros países y la desinformación. Al respecto se entiende que la Unión está ya construyendo dicha estrategia desde hace tiempo con el apoyo de iniciativas innovadoras para combatir esta amenaza[1428], con la coordinación interinstitucional pública y privada[1429], a través de la participación de las organizaciones de la sociedad civil (OSC) y con el compromiso de los medios de comunicación. Asimismo, también contribuye a esta estrategia de defensa europea frente a la injerencia foránea la *Ley de Servicios Digitales*[1430] que, como ya hemos visto en el apartado anterior de este Capítulo,

[1423] La INGE 2 se crea por la Decisión del Parlamento Europeo, de 10 de marzo de 2022, sobre la constitución, competencias, composición numérica y duración del mandato de la Comisión Especial sobre Injerencias Extranjeras en todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación (INGE 2) (2022/2585(RSO)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0070_ES.html (24/10/2024).

[1424] Para poder alcanzar sus objetivos la ING 2 ha establecido líneas de cooperación con el StratCom de la OTAN, el Hybrid CoE y las NNUU, entre otros.

[1425] Informe INGE 2 sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación, de 15 de mayo de 2023 (Informe A9-0187/2023; relatora Sandra Kalniete). Disponible en: https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html#_section2 (24/10/2024).

[1426] IBIDEM, párrafo 11.

[1427] Resolución del Parlamento Europeo, de 1 de junio de 2023, sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2022/2075(INI)). DOUE C, C/2023/1226 de 21.12.2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C_202301226 (13/05/2024).

[1428] Sirvan como ejemplo los proyectos financiados por la UE a través de los fondos Horizonte 2020, como SOMA, PROVENANCE, SocialTruth o WeVerify, para educar y concienciar a los ciudadanos frente a las noticias falsas y la desinformación como amenazas para la democracia, la economía y la sociedad. Disponible en: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_es#proyectos-existentes (14/05/2024).

[1429] En este punto debe citarse a organizaciones independientes como EU Disinfo Lab, cuyo objetivo es la monitorización permanente en las principales plataformas de comunicación, para detectar tendencias, identificar narrativas y generar alertas que se comparten con la comunidad de investigadores e instituciones que velan por la integridad de la información que llega a los ciudadanos europeos y sus derechos y valores democráticos. Disponible en: https://www.disinfo.eu/ (14/05/2024).

[1430] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). DOUE L 277/1, de 27.10.2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065 (14/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

armoniza la normativa aplicable a los prestadores de servicios intermediarios en relación con las condiciones de sus servicios, la diligencia debida en el control de contenidos y la obligación de cooperar con las autoridades competentes en situaciones de crisis híbridas complejas, entre las que cabe incluir las consecuencias negativas generadas por la desinformación y la manipulación de las elecciones, ambas consideradas como riesgos sistémicos en la referida DSA[1431].

Continúa la Resolución del Parlamento Europeo de 2023 sobre la injerencia extranjera manifestando el profundo valor democrático que inspira la lucha por garantizar procesos electorales independientes y transparentes, y preservar el derecho de los ciudadanos a una información veraz y libre de condicionamientos espurios, al afirmar que:

> "[…] la desinformación y otros tipos de manipulación de la información vician el debate público en torno a las elecciones y otros procesos democráticos y pueden impedir la toma de decisiones informadas por parte de los ciudadanos o desalentarlos por completo de participar en la política; […] las elecciones europeas son fundamentales para el funcionamiento de los procesos democráticos de la Unión Europea, ya que promueven su estabilidad y legitimidad; que, por lo tanto, debe defenderse la integridad democrática de la Unión, en particular evitando la difusión de desinformación y la influencia extranjera indebida en las elecciones europeas"[1432].

De igual forma se menciona la instrumentalización de los migrantes, las minorías y los movimientos antigénero como parte de las estrategias híbridas, cuyo objetivo es la polarización de la sociedad y el menoscabo de sus valores y derechos fundamentales. A todo lo anterior se suma el hecho de que la injerencia no se encuentra tipificada penalmente en la UE, lo que significa que los autores no se exponen a ninguna pena o sanción, salvo que la conducta encuentre acomodo en algún tipo penal preexistente.

Es tal la preocupación de la UE ante las implicaciones que puede conllevar la injerencia extranjera que, expresamente, la asume como amenaza directa a la seguridad nacional de sus Estados miembros, llegando incluso a proponer la reforma del artículo 222 TFUE[1433] para darle cabida, junto a la desinformación, como causa de activación de la cláusula de solidaridad y, con ello, a la movilización de todos los instrumentos de que

[1431] En los párrafos 82, 83 y 84 del Reglamento de Servicios Digitales se hace referencia a los riesgos que afecten a los procesos democráticos, el discurso cívico y los procesos electorales, así como la seguridad pública, haciendo mención expresa a la desinformación y la amplificación de contenidos engañosos o incorrectos, entre otros.

[1432] Resolución del Parlamento Europeo sobre la injerencia extranjera, Op. Cit., párrafos AW y AX. Página 9/34.

[1433] La cláusula de solidaridad recogida en el artículo 222 TFUE fue concebida para dotar a la Unión de una herramienta útil para la lucha contra la amenaza del terrorismo de carácter internacional, estando por ello ubicada dentro del apartado dedicado a la acción exterior y, como tal, es un instrumento más de la PESC para la movilización de todos los instrumentos de que disponga, incluidos los medios militares puestos a su disposición, para prestar asistencia a un socio en su territorio en caso de ataque terrorista, catástrofe natural o humana, que desborde claramente las capacidades de respuesta de que dispone. Ver apartado 3.3.2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

disponga la Unión para asistir a aquel socio que, habiendo sido atacado, sea desbordado en sus capacidades de respuesta por las graves consecuencias de este ataque:

> "Pide a los Estados miembros que reconozcan que la injerencia extranjera, incluida la desinformación, es una amenaza para la seguridad nacional y transfronteriza; pone de relieve la necesidad de que haya solidaridad entre los Estados miembros para poder luchar de manera eficaz contra este tipo de actividades; pie que se modifique el artículo 222 del TFUE con el fin de incorporar en él la injerencia extranjera"[1434].

Este planteamiento que hace el Parlamento Europeo de la influencia externa y de la desinformación es una declaración de intenciones de mucha relevancia y enlaza directamente con el objetivo de nuestro estudio, al catalogarlas como fuente de amenaza para la seguridad nacional de los Estados miembros.

Por esta trascendencia que tienen la injerencia y la desinformación para la seguridad común europea y la nacional de sus socios, la Resolución del Parlamento de 2023 establece *once líneas de actuación* para construir un marco de respuesta integral y coordinado de la Unión frente a esta grave amenaza.

1. *Estrategia coordinada de la UE contra las injerencias extranjeras*

El Parlamento comienza subrayando la necesidad de avanzar en la autonomía estratégica de la Unión para reducir la vulnerabilidad que supone nuestra dependencia en sectores esenciales como la energía o la tecnología digital.

A partir de este presupuesto, define la estrategia para abordar las injerencias extranjeras como coordinada y adaptada a la multidimensionalidad de la amenaza; sensible a la financiación para el desarrollo de nuevas capacidades y el impulso de las OSC y agencias europeas; creadora de sinergias a todos los niveles; potenciadora del intercambio de información; impulsora de nueva legislación europea para contener la amenaza; promotora del empleo de una amplia *caja de herramientas* contra la injerencia diseñada *ad hoc*; y centrada en la mejora de las capacidades de *prebunking*[1435] de la Unión.

Para llevarlo a cabo es esencial la acción frente a la desinformación que desempeña el StratCom[1436] del SEAE con el objetivo de detectar, analizar y documentar los intentos de

[1434] Resolución del Parlamento Europeo sobre la injerencia extranjera, Op. Cit., párrafo 11, página 15/34.
[1435] Campañas de comunicación estratégica para preparar a la ciudadanía para refutar la información falsa antes de que se difunda, complementada por la amplia difusión de las operaciones en curso y las narrativas detectadas a medida que se van produciendo. Este término deriva de las estrategias sobre la lucha contra la desinformación de EE.UU. y de UK.
[1436] Como ya expusimos en el apartado 7.2.1., el StratCom (Strategic Communication) es un grupo de trabajo del SEAE dedicado específicamente al análisis de información para la identificación de posibles narrativas manipuladoras y desinformativas, instrumentalizadas para la injerencia extranjera, que ha creado un marco analítico y una metodología para detectar, analizar y clasificar la desinformación y la injerencia extranjera, conocido como FIMI (Foreign Information Manipulation and Interference) y poder evaluar los comportamientos, las técnicas, las narrativas y los objetivos de la campaña desinformativa, así como medir el impacto generado por las mismas. Asimismo, elabora informes específicos como el primer

Ediciones Universidad de Salamanca | CC BY-NC-ND

manipulación o injerencia provenientes de actores externos, y medir el impacto alcanzado para generar la respuesta adecuada.

2. *Resiliencia*

Sobre la base de que la resiliencia es "la capacidad de los Estados y las sociedades para reformarse, resistir y recuperarse de las crisis internas y externas" y que, por ello, la esencia de un Estado y una sociedad resilientes se conforma "por la democracia, la confianza en las instituciones y el desarrollo sostenible"[1437], la segunda línea de acción para construir un marco de respuesta integral de la Unión incide en el fortalecimiento del pensamiento crítico de los ciudadanos, de su alfabetización mediática y digital y de la resiliencia frente a la manipulación de la información[1438].

Igualmente relevante será la labor de detección y análisis de campañas desinformativas por parte de verificadores e investigadores académicos, así como el necesario compromiso de la prensa y los medios de comunicación tradicionales -independientes, plurales y de calidad-. La labor de investigación de estos medios de comunicación y equipos de verificación para la detección de publicaciones falsas es, también, objeto de ataque por los Estados injerentes, principalmente Rusia, a través de campañas masivas en las que, mediante avisos de ciudadanos o de entidades suplantadas, dan cuenta de contenidos falsos en redes sociales para colapsar los recursos dedicados a esta tarea y, al tiempo, desviar la atención sobre las auténticas narrativas de desinformación[1439].

De esta manera, se antoja también necesaria la formación específica de los funcionarios públicos para identificar y combatir dicha amenaza, junto con la financiación de

y segundo EEAS Report on Foreign Information Manipulation and Interference Threats, de febrero de 2023 y enero de 2024, respectivamente. Nos permitimos recordar que en el primero de ellos se explica el método analítico del FIMI y, en el segundo, se presenta la *EU Hybrid Toolbox* que complementa al FIMI. Disponibles en: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf
https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (14/05/2024).

[1437] Shared Vision, Common Action: A Stonger Europe. A Global Strategy for the European Union´s Foreign And Securtiy Policy. Junio 2016. Páginas 23 y 24. Disponible en: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (14/05/2024).

[1438] En este sentido citar el Proyecto FANDANGO (FAke News Discovery and propagation from big Data ANalysis and artificial intelliGence Operations), 2018-2021, cuyo objetivo es abordar el problema de las noticias falsas y la posverdad, mediante la utilización de tecnología Big Data para analizar múltiples fuentes de datos provenientes de medios de comunicación, redes sociales, datos abiertos, etc., para detectar la falsedad y poder proporcionar en tiempo oportuno información veraz y verificada a los ciudadanos europeos. Disponible en: https://cordis.europa.eu/project/id/780355/es (14/05/2024).

[1439] Esta dinámica se detectó precisamente en mayo de 2024, en la campaña bautizada por el equipo especializado en el análisis de operaciones de influencia rusas Antibot4Navalny como *Operación Matrioska*, referida a la estrategia prorrusa dirigida contra verificadores de todo el mundo -EFE, BBC, CCN, Check First- para colapsar sus recursos con falsos avisos y peticiones de investigación sobre publicaciones falsas pero sin relevancia, con el objetivo de distraerlos de la verdadera amenaza. Disponible en: https://verifica.efe.com/operacion-matrioska-prorrusa-manipular-verificadores-alertas-falsas/ (23/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

programas específicos[1440] para la defensa de la democracia y el establecimiento de *cláusulas espejo:*

> "[…] para impedir que las empresas de medios de comunicación que estén bajo el control editorial de Gobiernos extranjeros o sean propiedad de países extranjeros de alto riesgo adquieran empresas europeas de medios de comunicación; considera que este sistema debe aplicarse principalmente a los países no democráticos o de alto riesgo en los que no se permite a las organizaciones europeas de medios de comunicación operar libremente, o se las presiona para que sesguen su cobertura en favor de los Gobiernos nacionales"[1441].

3. *Injerencias mediante el uso de plataformas en línea*

Para que la respuesta europea ante la amenaza de la injerencia y la desinformación extranjera sea verdaderamente efectiva se necesita el compromiso de las grandes plataformas en línea[1442], cuyo modelo actual de negocio se basa en el volumen de participación de sus clientes y los ingresos publicitarios derivados, utilizando para ello "algoritmos que premian las opiniones polarizadas y extremas en detrimento de la información basada en los hechos"[1443], lo cual va en contra de la estrategia europea de lucha contra la desinformación.

Por ello, se propone el desarrollo de soluciones normativas y tecnológicas propias, junto con la mayor colaboración de las plataformas para el control de narrativas, la retirada de contenidos y la facilitación del acceso a los datos que necesiten las autoridades europeas -Gobiernos, Policía, investigadores autorizados- para combatir esta amenaza en el marco de la legislación existente[1444].

4. *Infraestructuras críticas y sectores estratégicos*

[1440] Uno de estos programas es el denominado paquete de Defensa de la Democracia (diciembre 2023), con el que la Comisión busca mejorar la transparencia en cuanto a la representación de intereses extranjeros y el refuerzo de los procesos electorales en la Unión. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6453 (15/05/2024).

[1441] Resolución del Parlamento Europeo sobre la injerencia extranjera, Op. Cit., párrafo 37, página 19/34.

[1442] La Resolución aquí cita expresamente a Meta, Google, YouTube, TikTok y Twitter. En este mismo sentido, la Resolución del Parlamento Europeo, de 17 de enero de 2024, sobre las implicaciones en materia de seguridad y defensa de la influencia de China en las infraestructuras críticas en la Unión Europea P9_TA(2024)0028 (2023/2072(INI)), en su apartado 15) considera "que la aplicación TikTok, propiedad del grupo chino ByteDance, incumple el marco europeo sobre la privacidad de los datos, lo que la convierte en un riesgo potencial y una fuente de desinformación respaldada por China; acoge con satisfacción la decisión de las instituciones de la Unión y de varios Estados miembros de suspender el uso de la aplicación TikTok en dispositivos corporativos, así como en los dispositivos personales registrados en los servicios de dispositivos móviles de las instituciones". Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_ES.html#def_1_14 (25/10/2024).

[1443] Resolución del Parlamento Europeo sobre la injerencia extranjera, Op. Cit., párrafo 42, página 19/34.

[1444] Principalmente el Reglamento (UE) 2016/679 General de Protección de Datos, el Reglamento (UE) 2022/2065 de Servicios Digitales, el Reglamento (UE) 2024/900 sobre transparencia y segmentación en la publicidad política, y el Código de Buenas Prácticas en materia de Desinformación (reforzado de 2022).

Ediciones Universidad de Salamanca | CC BY-NC-ND

La cuarta línea de acción se basa en el reforzamiento de la seguridad de las infraestructuras críticas y estratégicas[1445], incluidas las de soporte de los procesos electorales[1446], para proteger su seguridad, resiliencia y fiabilidad. En este sentido, preocupa la dependencia tecnológica de la Unión en cuanto a los bienes de equipo, sistemas y programas informáticos[1447], y se alerta sobre la adquisición de empresas de sectores esenciales y de medios de comunicación por países de riesgo[1448], como parte de su estrategia geopolítica para alcanzar capacidad de influencia a nivel global.

La solución propuesta pasa por reforzar las capacidades industriales de Europa en los ámbitos tecnológicos clave[1449], como la IA, la computación cuántica o las materias primas críticas[1450].

[1445] En este sentido, la Resolución del Parlamento Europeo, de 17 de enero de 2024, sobre las implicaciones en materia de seguridad y defensa de la influencia de China en las infraestructuras críticas en la Unión Europea P9_TA(2024)0028 (2023/2072(INI)), en su apartado 19) pide "que se amplíen los instrumentos actuales que abordan la inversión extranjera directa y las subvenciones extranjeras para incluir procedimientos de control generalizados para todas las partes interesadas que participan en proyectos de infraestructuras críticas de la Unión que cubran todas las modalidades de participación en esfuerzos relacionados con infraestructuras críticas, incluidos los proyectos de colaboración, las asociaciones y las transferencias de tecnología". Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_ES.html#def_1_14 (25/10/2024).

[1446] En esta infraestructura electoral se encuentran los sistemas informáticos de soporte, los equipos de votación, los nodos de comunicación, los procedimientos de las oficinas y colegios electorales, las bases de datos de respaldo y las páginas web de comunicación de información y resultados.

[1447] Expresamente se menciona a fabricantes de países de alto riesgo -China y Rusia- como Tik Tok, ByteDance, Huawei, ZTE, Kaspersky, NtechLab o Nuctech, ya que la política de seguridad nacional de estos países puede llegar a implicar una amenaza para la confidencialidad, la integridad y la disponibilidad de los datos personales de sus clientes, por cuanto dichas empresas están obligadas a compartirlos con el Estado como medio para obtener información y conocimiento para favorecer la consecución de sus objetivos económicos, políticos, estratégicos y militares.

[1448] En Georgia, país candidato a la adhesión a la UE desde diciembre de 2023, se planteó un proyecto de ley sobre *agentes extranjeros* que, finalmente, no fue aprobado por su afectación a la libertad de expresión e ideológica, por cuanto obligaba a los medios de comunicación que recibieran más del 20% de su financiación del exterior a registrarse como *defensores de los intereses de una potencia extranjera*. Este es el dilema que se plantea: articular mecanismos de respuesta frente a la amenaza de las maniobras de Estados autocráticos y revisionistas mientras se defienden los derechos y los principios que conforman la democracia. Disponible en: https://es.euronews.com/2024/05/18/la-presidenta-de-georgia-veta-la-ley-de-agentes-extranjeros-o-ley-rusa
https://cnnespanol.cnn.com/2024/05/19/presidenta-georgia-veta-controversia-proyecto-ley-agentes-extranjeros-rusia-trax/ (19/05/2024).

[1449] Respecto a los semiconductores, la Resolución del Parlamento Europeo, de 17 de enero de 2024, sobre las implicaciones en materia de seguridad y defensa de la influencia de China en las infraestructuras críticas en la Unión Europea P9_TA(2024)0028 (2023/2072(INI)), en su apartado 26) se refiere a la Ley Europea de Chips "que aumentará la capacidad de la Unión para producir semiconductores y creará un mapa estratégico de, entre otras cosas, las carencias de capacidad en la cadena de valor de los semiconductores en la Unión, limitando así la dependencia de la Unión de terceros países como China". Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_ES.html#def_1_14 (25/10/2024).

[1450] Al respecto debemos citar la Ley Europea de Materias Primas Fundamentales, clave para desarrollar las capacidades industriales y tecnológicas de la UE, consolidar las cadenas de suministro estratégicas y reforzar la resiliencia del sistema frente a posibles perturbaciones globales. Reglamento del Parlamento Europeo y del Consejo por el que se establece un marco para garantizar el suministro seguro y sostenible de materias primas fundamentales. Bruselas, 16.3.2023. COM(2023) 160 final. 2023/0079 (COD).

Ediciones Universidad de Salamanca | CC BY-NC-ND

5. *Injerencias durante los procesos electorales*

El Parlamento Europeo apuesta por la decidida protección frente a la injerencia extranjera en los procesos electorales ante la gravedad de sus consecuencias, destacando la labor de la *Autoridad para los Partidos Políticos Europeos y las Fundaciones Políticas Europeas* (AAPF)[1451], y de la *Red Europea de Cooperación Electoral*[1452] que es el modelo a seguir en los Estados miembros para el establecimiento de redes nacionales similares[1453] que trabajen cooperativamente para prevenir y atajar la manipulación de la información en los procesos electorales.

En este mismo sentido, y orientado a los representantes públicos y autoridades, se considera necesario elaborar un Código de buenas prácticas en las redes sociales por cuanto es un hecho que tanto los políticos como los gobiernos "a veces recurren a la desinformación para fomentar la hostilidad ideológica"[1454], infausta constatación de que la amenaza no sólo proviene del exterior sino que, en ocasiones, crece en las grietas del propio ecosistema político europeo y nacional, generando un ambiente de crispación social y odio que lleva a la polarización, fruto del cual se pueden llegar a cometer ataques como los vistos, en el marco de las elecciones europeas de junio de 2024, contra

Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0160 (15/05/2023).

[1451] La Authority for European Political Parties and European Political Foundations (APPF) es la responsable de verificar, registrar y controlar la financiación del sistema político europeo, estando particularmente alerta frente a la financiación indirecta por parte de terceros países de riesgo o no pertenecientes a la UE. También es la encargada de aplicar las sanciones y de garantizar la visibilidad y la transparencia de la documentación de partidos y fundaciones políticas. Disponible en: https://www.appf.europa.eu/appf/en/home/the-authority (15/05/2024).

[1452] La Red Europea de Cooperación Electoral celebra su primera reunión el 21 de enero de 2019, en el marco de las elecciones al Parlamento Europeo de dicho año. Esta Red reúne a representantes de los EEMM con competencia en los procesos electorales, y su objetivo es generar sinergias a través del intercambio de información y de buenas prácticas sobre la protección de datos, la ciberseguridad o la transparencia para garantizar unas elecciones libres y seguras. Disponible en: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship-and-democracy/democracy-and-electoral-rights/european-cooperation-network-elections_en?prefLang=es (14/05/2024).

[1453] Estas redes nacionales de cooperación electoral se han creado en Alemania, Austria, Bélgica, Bulgaria, Chequia, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Rumanía, Suecia. Disponible en: https://elections.europa.eu/es/free-fair-elections/

En España, en abril de 2019, el Consejo de Seguridad Nacional crea la Red de Coordinación para la Seguridad en Procesos Electorales. Disponible en: https://www.europapress.es/nacional/noticia-interior-crea-red-coordinacion-seguridad-procesos-electorales-20190412204535.html (14/05/2024).

Como ejemplo de su funcionamiento, para las elecciones al Parlamento Europeo del 9 de junio de 2024, el Ministro del Interior activa el 6 de mayo la Red de Coordinación para la Seguridad en Procesos Electorales, como parte del dispositivo de seguridad nacional para garantizar las citadas elecciones. Disponible en: https://www.dsn.gob.es/gl/actualidad/sala-prensa/activaci%C3%B3n-red-coordinaci%C3%B3n-para-seguridad-procesos-electorales-ante-9j (14/05/2024).

[1454] Resolución del Parlamento Europeo sobre la injerencia extranjera, Op. Cit., párrafo 70, página 23/34.

Ediciones Universidad de Salamanca | CC BY-NC-ND

representantes públicos como el primer ministro eslovaco Robert Fico[1455] o al eurodiputado alemán y candidato socialista por Sajonia, Matthias Ecke[1456].

6. *Financiación encubierta de actividades políticas por agentes y donantes extranjeros*

La sexta línea de acción para la gestión de la respuesta de la Unión ante la injerencia y la desinformación se centra en la alerta ante la financiación encubierta de actividades políticas en el seno de la UE por parte de agentes y benefactores económicos extranjeros para ganar influencia, refiriéndose en concreto a la financiación rusa de políticos, partidos y funcionarios, así como sus conexiones con movimientos secesionistas como el de Cataluña.

7. *Ciberseguridad y resiliencia frente a ciberataques relacionados con procesos democráticos*

El Parlamento también muestra su preocupación por el incremento de los ciberataques a infraestructuras electorales consideradas críticas, así como a sitios web de instituciones europeas[1457] y de partidos políticos.

Para ello, la mejora de las medidas de ciberseguridad y resiliencia frente a los ciberataques en los procesos electorales requiere la coordinación institucional a través del CERT-UE y el resto de los CERT nacionales de referencia, junto con la ENISA.

[1455] El día 15/05/2024, el primer ministro de Eslovaquia, Robert Fico, recibió hasta cinco disparos a corta distancia por parte de un ciudadano eslovaco de 71 años de edad, cuando salía de una reunión con su gabinete y se disponía a saludar a simpatizantes que aguardaban en la ciudad de Handlova. Disponible en: https://www.elmundo.es/internacional/2024/05/16/66459542e4d4d867308b45a6.html https://www.bbc.com/mundo/articles/cjmkmw3g0ppo (18/05/2024).

[1456] En Alemania el escenario de violencia ejercida contra representantes políticos se agudiza a la vista de las elecciones europeas de junio de 2024, con hechos como la agresión sufrida el 8 de mayo por la exalcaldesa de Berlín y actual responsable de Economía en el Gobierno de la ciudad, la socialdemócrata Franziska Giffey, o la sufrida un día después por la política Yvonne Mosler, afiliada a Los Verdes y atacada en Dresde, misma ciudad donde el eurodiputado socialdemócrata alemán Matthias Ecke fue víctima de una paliza cuando, en el desarrollo de la campaña electoral europea, pegaba carteles junto con otros compañeros de partido el 3 de mayo. Disponible en: https://es.euronews.com/my-europe/2024/05/08/golpean-a-una-politica-alemana-durante-un-acto-oficial-en-berlin-esta-atacando-nuestra-dem https://elpais.com/internacional/2024-05-08/dos-nuevas-agresiones-agravan-la-preocupacion-en-alemania-por-la-violencia-contra-los-politicos.html https://es.euronews.com/my-europe/2024/05/04/agreden-en-plena-calle-a-un-candidato-aleman-para-las-elecciones-europeas https://elpais.com/internacional/2024-05-12/la-oleada-de-agresiones-a-politicos-desata-la-alarma-en-europa-me-atacaron-de-forma-repentina-e-inesperada.html (18/05/2024).

[1457] El 22 de noviembre de 2022, horas después de la aprobación de una resolución que declaraba a Rusia *Estado patrocinador del terrorismo*, la página web oficial del Parlamento Europeo sufrió un ataque de denegación de servicio atribuida a un grupo pro-Kremlin. Disponible en: https://es.euronews.com/my-europe/2022/11/23/cae-la-web-del-parlamento-europeo-tras-aprobar-una-resolucion-contra-rusia https://www.elmundo.es/internacional/2022/11/23/637e3186fc6c837b508b45d5.html (18/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

8. *Impacto de las injerencias en los derechos de las minorías y otros grupos vulnerables*

Otra de las líneas de acción de la estrategia europea frente a la desinformación se centra en el análisis y la evaluación del impacto de las injerencias en los derechos de las minorías y grupos vulnerables, a través de la instrumentalización de narrativas vinculadas a la migración, la cuestión de género o el discurso del odio, siempre con objetivos políticos encubiertos contrarios a la UE y sus valores democráticos.

9. *Injerencias por medio de agentes mundiales a través de la captación de élites, las diásporas nacionales, las universidades y actos culturales*

Igualmente preocupantes son las injerencias extranjeras a través de la captación de las élites, la entrada en las universidades[1458], el patrocinio de actos culturales y la financiación de proyectos y actividades investigativas a través de maniobras de corrupción, manipulación, tráfico de influencias y aproximación a objetivos de referencia como medio para lograr filtraciones de conocimiento y alcanzar capacidad de influencia con las que conseguir ventaja competitiva industrial o militar[1459].

10. *Disuasión, atribución y contramedidas colectivas, incluidas sanciones*

La respuesta integral que busca la Unión frente a la injerencia y la desinformación exige la adopción de contramedidas y sanciones colectivas bajo un patrón común construido en torno al artículo 29 TUE y el 215 TFUE. Dicho esquema debe basarse en la rapidez de actuación y en la efectividad de las medidas adoptadas, incluyendo para ello la imposición de costes a los agentes -estatales y no estatales- hostiles condenados, el uso

[1458] La creciente presencia de estudiantes chinos en las universidades y centros de investigación europeos ha hecho saltar las alarmas por la fuga del *know how* que, a través del regreso a su país de estos estudiantes y la aplicación de tecnologías de doble uso a las capacidades de Pekín tanto en el plano civil como militar, alimenta la estrategia modernizadora de su ejército y la competencia industrial de sus marcas automovilísticas y tecnológicas, entre otras. Esta realidad ha hecho que surjan iniciativas como la web MapInfluenceCE (https://mapinfluence.eu) o China Observers in Central and Eastern Europe CHOICE (https://chinaobservers.eu), conformadas por expertos de distintos ámbitos y países que analizan y emiten informes sobre la creciente influencia de China y Rusia en Europa para identificar sus estrategias de penetración en el ámbito académico y la influencia en las élites políticas. También la prensa se hace eco de estas tácticas de espionaje. Disponible en: https://www.abc.es/sociedad/china-infiltra-agentes-universidades-europeas-20221202183650-nt.html (25/10/2024).

[1459] La Resolución del Parlamento Europeo, de 17 de enero de 2024, sobre las implicaciones en materia de seguridad y defensa de la influencia de China en las infraestructuras críticas en la Unión Europea P9_TA(2024)0028 (2023/2072(INI)), en su apartado 13) sobre las herramientas para responder a las preocupaciones en materia de seguridad y defensa, sostiene "que un ámbito clave de las infraestructuras básicas de la Unión es también su red de institutos de investigación y entidades de investigación y desarrollo, que desempeñan un papel importante en la capacidad de la Unión para cumplir sus compromisos en materia de transición ecológica y digital, junto con áreas clave como el espacio de defensa; recuerda las vulnerabilidades en materia de seguridad relacionadas con las transferencias forzosas de tecnología, el robo de propiedad intelectual y las filtraciones de conocimientos, tanto en la Unión como fuera de ella; pide una mayor vigilancia a la hora de tener en cuenta estas amenazas a la capacidad de la Unión para innovar y fomentar el crecimiento". Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_ES.html (25/10/2024)

Ediciones Universidad de Salamanca | CC BY-NC-ND

de la *EU Hybrid Toolbox*[1460] del SEAE, su aplicación conformada en los diferentes Estados miembros y el desarrollo de una base jurídica que permita sancionar este tipo de amenazas en toda la UE, para cuya consecución la DSA desempeña un papel decisivo.

Un ejemplo de este tipo de sanción con un enfoque coordinado de la Unión es la sentencia del Tribunal General (Gran Sala) de 27 de julio de 2022 -RT France contra el Consejo de la Unión Europea-[1461], por la que se confirma la prohibición temporal de emisión y suspensión de las autorizaciones en Europa para difundir contenidos por RT France, por haberse demostrado que se trata de un medio de comunicación bajo el control permanente de la Federación de Rusia y, como tal, constituyente de una amenaza importante y directa para el orden público y la seguridad de la Unión en el marco de la agresión militar a Ucrania.

11. *Vecindad, cooperación mundial y multilateralismo*

Las narrativas desinformativas propagadas por actores Estatales extranjeros, principalmente Rusia y China, contra los intereses y la seguridad de la Unión tienen también una amplia repercusión en América Latina y África -muchas veces utilizadas como plataformas de lanzamiento de mensajes para su entrada en Europa-, por lo que es precisa una comunicación estratégica proactiva, eficaz y transparente para generar confianza en el modelo europeo y contrarrestar la influencia de estos países revisionistas de alto riesgo.

Esta línea de defensa europea conlleva una apuesta firme y decidida por contribuir a crear una conciencia común sobre los retos mundiales y la necesidad de reforzar la cooperación internacional en el marco de las Naciones Unidas, proponiendo el desarrollo de respuestas internacionales frente a la manipulación de la información y la injerencia por parte de agentes extranjeros.

Asimismo, desde el SEAE se lidera la intensificación de la cooperación multilateral con otros socios de la UE[1462], las OSC, los verificadores, los medios de comunicación y la industria para el desarrollo de mecanismos conjuntos tendentes a combatir la injerencia en los procesos electorales y la cooperación en el intercambio de información que permita aprovechar las lecciones aprendidas, con el objetivo de mejorar la resiliencia conjunta frente a las estrategias híbridas.

La última consideración a destacar de la *Resolución del Parlamento Europeo sobre la injerencia extranjera* es que, más allá de presentar un marco de respuesta integral de la Unión frente a esta amenaza que afecta a la esencia misma de la democracia y la seguridad de los europeos, lanza un mensaje de compromiso y colaboración con la comunidad internacional proponiendo la necesidad de alcanzar, en el marco de las NNUU, estrategias de respuesta conjuntas frente a la desinformación y la intervención de terceros Estados de riesgo, para lo cual es necesario que:

[1460] Ver apartado 3.3.3.

[1461] Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62022TJ0125 (13/05/2024).

[1462] Con países aliados como EE.UU., Canadá, Australia, Brasil y Taiwán, entre otros.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "[…] abandonen su enfoque neutral en cuanto a países y adopten un enfoque centrado en los Estados de alto riesgo, y que no vacilen en identificar y nombrar en los foros internacionales, como las Naciones Unidas, a los países que han intentado llevar a cabo injerencias extranjeras, a fin de que otros países tomen conciencia de los riesgos que entraña este problema"[1463].

7.3.2. La estrategia de defensa común europea frente a la desinformación aplicada a los pilares de la democracia: la vulnerabilidad de los procesos electorales

Mejorar la participación de los ciudadanos europeos en la vida democrática[1464] y, para ello, enfrentar las estrategias en la Zona Gris que la amenazan, se ha convertido en objetivo prioritario para la UE y sus Estados miembros, los cuales han sufrido graves injerencias en procesos tan relevantes como el referéndum sobre la pertenencia de Reino Unido a la UE de junio de 2016 -el *Brexit*-, las elecciones presidenciales francesas de mayo de 2017[1465] o la crisis por el referéndum secesionista catalán de octubre del mismo año[1466], aparte de las habituales campañas de influencia extranjera -principalmente rusas- detectadas con ocasión de las elecciones europeas de mayo del 2019 o de junio de 2024.

[1463] Resolución del Parlamento Europeo sobre la injerencia extranjera, Op. Cit., párrafo 139, página 34/34.
[1464] En este sentido, las Conclusiones del Consejo relativas al Informe sobre la Ciudadanía de la Unión de 2017, adoptada el 11 de mayo, recoge expresamente como prioridad *aumentar y mejorar la participación ciudadana en la vida democrática de la UE*. Documento 9080/17. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9080-2017-INIT/es/pdf (13/05/2024).
[1465] En mayo de 2017, al cierre de la campaña electoral y a menos de 48 horas de la jornada para la elección presidencial, se publicaron en Pastebin, sitio web para compartir archivos, 14.5 gigabytes de correos electrónicos y otra documentación personal del candidato Emmanuel Macron, mezclando documentos falsos con otros auténticos con el objetivo de crear confusión y desinformación. Disponible en: https://cnnespanol.cnn.com/2017/05/06/hackean-la-campana-de-emmanuel-macron-en-francia/ (13/05/2024).
[1466] El 6 de septiembre de 2017 el Parlamento de Cataluña aprobó la convocatoria de un referéndum vinculante sobre su independencia que, recurrido por el Gobierno de España, fue suspendido por el Tribunal Constitucional. A pesar de ello, dicho consulta se celebró, sin ninguna garantía legal y con numerosas irregularidades, el 1 de octubre de 2017, consiguiendo según la Generalitat de Cataluña un 90% de votos favorables a la independencia con un 43% de participación, resultado que nunca se reconoció internacionalmente, como tampoco la declaración unilateral e inmediata suspensión de la independencia de Cataluña que hizo el Presidente de la Generalitat, Carles Puigdemont, días después y que motivó la activación del artículo 155 de la Constitución por parte del Gobierno de la nación. Posteriormente, el Parlamento Europeo advierte de la injerencia rusa en este proceso independentista catalán. Disponible en: https://www.elmundo.es/cataluna/2021/11/09/61896962e4d4d840138b458a.html https://www.elperiodico.com/es/politica/20240207/parlamento-europeo-injerencia-rusia-cataluna-proces-97875532 https://elpais.com/espana/2024-02-06/bruselas-advierte-contra-la-injerencia-rusa-en-el-proces-y-pide-investigar-si-el-kremlin-infiltro-agentes-en-la-ue.html https://elpais.com/espana/2024-02-26/un-informe-de-la-inteligencia-europea-traza-vinculos-entre-el-independentismo-catalan-y-el-kremlin.html (13/05/2024)

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por esta razón, en febrero de 2019 el Consejo de la UE adopta unas Conclusiones en este sentido[1467], subrayando la necesidad de favorecer un enfoque holístico e integral para contrarrestar de manera efectiva el profundo embate que las amenazas híbridas representan para los procesos democráticos y, por ende, para la seguridad de la Unión y sus Estados miembros:

> "[…] las amenazas que se ciernen sobre nuestros procesos electorales pueden adoptar varias formas, por ejemplo las amenazas híbridas y cibernéticas y la desinformación. Por lo tanto, son necesarios un planteamiento global y exhaustivo y una actuación decidida para neutralizar dichas amenazas antagonistas y subversivas"[1468].

Como ya hemos estudiado, el origen de este complejo y grave riesgo para la seguridad y la transparencia de las elecciones puede provenir tanto de un actor externo como interno, a través de diversas formas, directas o indirectas, compartiendo en todo caso los objetivos de socavar la confianza de la ciudadanía en sus instituciones de gobierno y representación y, al tiempo, deslegitimar el propio funcionamiento de los procesos democráticos[1469]. Conscientes de ello, se vertebran distintas líneas de trabajo con el objetivo de desarrollar un enfoque global y coherente para garantizar que los procesos electorales europeos sean lo más estancos posible ante la desinformación y las campañas manipuladoras.

En esta línea recordamos que, en diciembre de 2020, la Comisión adoptó el *Plan de Acción para la Democracia Europea*[1470] con la finalidad de construir democracias más resilientes en toda la UE mediante la promoción de elecciones libres y justas, el refuerzo de la libertad de los medios de comunicación y la lucha contra la desinformación, fijando entre sus prioridades de carácter transversal el impulso del compromiso y la participación ciudadana en la defensa de la democracia.

Cuando estudiamos en el Capítulo anterior el apartado referido al contexto y las principales causas de la desinformación[1471], proponíamos una *quinta oleada de la era moderna de la desinformación*, la por nosotros denominada *era de la competencia cognitiva* que, iniciando en el 2016, llegaría hasta el momento actual y se caracterizaría por una nueva dimensión de la amenaza favorecida por, entre otras, el uso de la IA.

Las indudables ventajas referidas a parámetros de eficacia, economía de recursos, desarrollo de soluciones o bienestar humano que pueden conllevar el empleo de

---

[1467] Conclusiones del Consejo y de los Estados miembros sobre «garantizar unas elecciones europeas libres e imparciales». Bruselas, 19 de febrero de 2019. 6573/1/19. REV 1. Disponible en: https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/es/pdf https://www.consilium.europa.eu/en/press/press-releases/2019/02/19/securing-free-and-fair-european-elections-council-adopts-conclusions/ (13/05/2024).

[1468] IBIDEM, pág. 2.

[1469] Ver Capítulo 6.2.

[1470] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción para la Democracia Europea. COM(2020) 790 final. Bruselas, 3.12.2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423 (20/10/2024).

[1471] Ver Capítulo 6, apartado 6.2.2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

herramientas y sistemas de IA, a través de decisiones automatizadas basadas en algoritmos o en redes neuronales, no deben hacernos rehuir la realidad que suponen los riesgos que:

> "[…] estos usos conllevan para los derechos e intereses de la ciudadanía y que requieren contar con una regulación adecuada para garantizar la protección de la privacidad y los datos personales, el uso ético y responsable de la inteligencia artificial, la ciberseguridad o la protección de la propiedad intelectual, así como la gobernanza en internet" (ABA CATOIRA, 2024, pág. 189).

La cada vez más profunda integración de la IA en los distintos contextos de la vida de los ciudadanos requiere, como señala Castellanos Claramunt, un tratamiento regulatorio singular y exhaustivo, basado en el evidente componente ético del manejo de los datos generados por la actividad de las personas, "con el fin de garantizar su compatibilidad con los derechos fundamentales y promover su uso responsable y sostenible" (CASTELLANOS CLARAMUNT, 2023, pág. 266).

En este contexto podemos decir que el uso de la IA en los procesos electorales es una realidad con mediáticas muestras a nivel global -Pakistán, Paraguay, EE.UU., Argentina- que ponen de manifiesto la capacidad de la tecnología actual para personalizar los mensajes políticos, con el objetivo de maximizar la efectividad de las campañas e influir de forma larvada en los votantes "potenciando la persuasión y, en muchos casos, distorsionando la percepción de la realidad política y social" (RUBIO NUÑEZ, FRANCO ALVIM, & DE ANDRADE MONTEIRO, 2024, pág. 19).

En la moderna sociedad digital y altamente conectada que reclama una democracia igualmente avanzada con procesos e instituciones tecnologizadas, las elecciones se ven inmersas en un novedoso y complejo contexto de comunicación que se ha trasladado al ciberespacio, donde el debate público se distorsiona en el reflejo que produce la amenaza desinformativa a través de la intolerancia y la polarización ideológica, la injerencia extranjera, la pérdida del poder intermediador de los medios tradicionales, la profunda fractura social y la desafección política, entre otros. Fruto de ello, las elecciones se *deshumanizan* y pierden las referencias clásicas, pudiendo concluir que:

> "Las campañas electorales, en este ambiente, se desarrollan en un espacio en el que la información y opinión se funden en beneficio de esta última, donde las emociones conforman una conversación pública cada vez más superficial, más anecdótica, polémica, truculenta y estridente […]. Las disputas simbólicas actuales dependen menos del acceso a la información que de la capacidad de difundirla y reiterarla eficazmente en bucles interminables" (RUBIO NUÑEZ, FRANCO ALVIM, & DE ANDRADE MONTEIRO, 2024, págs. 58-59).

Un claro ejemplo de la percepción social de esta amenaza son los resultados que ofrece el *Eurobarómetro Flash 528 – Ciudadanía y democracia*[1472], donde en torno al 80% de los europeos manifiestan su preocupación por las diversas formas de interferencia en

[1472] Eurobarómetro Flash 528 – Ciudadanía y democracia. Trabajo de campo realizado entre abril y mayo de 2023, siendo publicado en diciembre de 2023. Disponible en:https://europa.eu/eurobarometer/surveys/detail/2971 (26/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

las elecciones de la UE y, en concreto, de la desinformación y la injerencia extranjera como piezas clave de influencia en la conformación de voto de los ciudadanos, representando un grave problema que debe abordarse[1473]. Siendo este el sentir de la población e instada por la previsión de posibles contingencias en los comicios europeos de 2024, sabedora del valor que representan unas elecciones libres, justas y resilientes, la Comisión Europea adopta en diciembre de 2023 un paquete de medidas legislativas para la *Defensa de la Democracia*[1474], que se apoya en tres pilares:

1. La mejora de la transparencia y la rendición de cuentas para arrojar luz sobre la influencia extranjera encubierta y la representación de intereses de terceros países en dichos procesos[1475]. Ante la evidencia de que los gobiernos de determinados países -mayormente de riesgo, como Rusia o China- utilizan cada vez más en sus estrategias de proyección política las actividades de representación de intereses, sin desdeñar por ello los canales formales clásicos, la Comisión establece tres obligaciones de control de estos *movimientos laterales*, claramente emplazados en la Zona Gris: la inscripción en un registro de transparencia, el libre acceso público a los datos referidos a esas actividades de representación de intereses de terceros países, y el necesario archivo documental durante cuatro años desde la finalización de dicha actividad.
2. El refuerzo de los procesos electorales en la Unión[1476], con el objetivo de promover la alta participación en los comicios y proteger, frente a la ciberamenaza, a las infraestructuras vinculadas con el desarrollo de estos procesos esenciales para la buena salud de las democracias. Igualmente, propone medidas para minimizar el riesgo de injerencia extranjera a través de la financiación de partidos políticos, candidatos y campañas electorales, que pudieran ser utilizados como instrumento de presión.
3. El fomento de un entorno propicio para la participación inclusiva de los ciudadanos y las OSC en la elaboración de políticas públicas orientadas a proteger la democracia y los valores comunes, a través de marcos accesibles, transparentes e inclusivos[1477].

[1473] IBIDEM, páginas 27 a 33.

[1474] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Defensa de la Democracia. Estrasburgo, 12.12.2023. COM(2023) 630 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52023DC0630 (26/10/2024).

[1475] Propuesta de la Comisión Europea de una Directiva del Parlamento Europeo y del Consejo por la que se establecen requisitos armonizados en el mercado interior en materia de transparencia de la representación de intereses realizada en nombre de terceros países y se modifica la Directiva (UE) 2019/1937. Estrasburgo 12.12.2023. COM(2023) 637 final. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A637%3AFIN (26/10/2024).

[1476] Recomendación (UE) 2023/2829 de la Comisión, de 12 de diciembre de 2023, sobre procesos electorales inclusivos y resilientes en la Unión y con vistas a reforzar el carácter europeo y el desarrollo eficiente de las elecciones al Parlamento Europeo. Diario Oficial de la Unión Europea 2023/2829, de fecha 20.12.2023. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H2829 (26/10/2024).

[1477] Recomendación de la Comisión Europea sobre la promoción del compromiso y la participación efectiva de los ciudadanos y las organizaciones de la sociedad civil en los procesos de elaboración de políticas públicas. Bruselas, 12.12.2023. C(2023) 8627 final. Disponible en: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=PI_COM%3AC%282023%298627 (26/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Este ecosistema de riesgo y nuevas amenazas en el que se ven inmersos los procesos electorales provocado en gran medida por la aplicación de la tecnología, y en concreto de la IA, al entorno de comunicación y relaciones en campaña, hace que algunos autores como Rubio Núñez, Franco Alvim y De Andrade Montero se refieran a las *elecciones algorítmicas* como una nueva época caracterizada por la sutil selección de los mensajes políticos, la categórica segmentación de los destinatarios y la retroalimentación permanente de este proceso en base a sus efectos y resultados, que sustenta lo que estos autores denominan el proceso de *deshumanización de las elecciones:*

> "[…] evidenciado por la incisiva ruptura de la intimidad, la sobreexplotación de narrativas atrayentes, la normalización de la intolerancia y la ostentosa falta de respeto que los candidatos de la anti política muestran hacia las instituciones, así como el uso creciente de la extracción de datos, el poder algorítmico y la propaganda informática en estrategias de persuasión masiva […]" (RUBIO NUÑEZ, FRANCO ALVIM, & DE ANDRADE MONTEIRO, 2024, págs. 53-57).

Este contexto es determinante para que, en enero de 2024, el SEAE publique su *2nd Report on Foreign Information Manipulation and Interference Threats: a framework for networked defence*[1478], con una visión práctica del Marco de Respuesta a las Amenazas FIMI aplicado a los procesos electorales que, por un lado, se integra en la *EU Hybrid Toolbox* como parte esencial de la estrategia de lucha contra la desinformación y, por otro, materializa la propuesta del Plan de Acción para la Democracia Europea de responder de manera estructurada y colectiva frente a la manipulación de la información tanto interna como externa.

En lo que se refiere a la interferencia extranjera en los procesos electorales, como venimos viendo, supone una preocupación trascendental para la UE y se caracteriza por el recurso a una amplia variedad de métodos, todos ellos orquestados en torno al objetivo principal de la desestabilización de las sociedades democráticas, a las que los Estados autoritarios consideran una permanente amenaza a sus deseos de supervivencia y anhelos de expansión. Con el punto de mira en las elecciones europeas de junio de 2024, este Segundo Informe FIMI del SEAE presenta las conclusiones de su análisis de campo sobre diferentes incidentes de este tipo relacionados con elecciones en países europeos y de EE.UU. durante el periodo 2022-2023[1479], distinguiendo cinco categorías en base a los objetivos del ataque, las TTP características del autor y los riesgos generados por la amenaza:

1. Amenaza FIMI orientada al control de la información y de los temas clave debatidos durante el período electoral, a través de la cual los actores tratan de

[1478] Ver el Capítulo 6, apartado 6.2.3.3. donde se analiza el Segundo informe del SEAE sobre Amenazas de Manipulación e Interferencia de Información Extranjera: un marco para la defensa en red. European Union External Action. Enero de 2024.
Disponible en: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (29/09/2024).

[1479] La muestra de casos de incidentes FIMI están relacionados con las elecciones en EE.UU. (elecciones de mitad de período 2022), Italia (elecciones generales 2022), Kosovo (elecciones locales 2023), Montenegro (elecciones parlamentarias 2023), España (elecciones generales 2023), Liberia (elecciones generales 2023), Polonia (elecciones parlamentarias 2023), Países Bajos (elecciones parlamentarias 2023) y República Democrática del Congo (elecciones presidenciales 2023). IBIDEM, página 23.

Ediciones Universidad de Salamanca | CC BY-NC-ND

ocupar espacio en los canales de comunicación alternativos y redes sociales con el fin de interactuar con las audiencias para, poco a poco, ir adquiriendo credibilidad y legitimidad, al tiempo que se desacredita el cauce de comunicación convencional. Ello conlleva el riesgo de desconfianza en las fuentes oficiales y la consolidación de las no verificadas.

2. Amenaza FIMI que trata de fomentar el absentismo y la no participación de los ciudadanos en el proceso de votación, con el objetivo de reducir la representatividad de los resultados electorales y, con ello, debilitar la democracia. Se utilizan para ello las falsas alertas de seguridad en el entorno de los colegios electorales o la confusión sobre los requisitos establecidos para ejercer el derecho al voto, entre otros. El riesgo subyacente es la falta de aceptación de los resultados electorales como legítimos, con las posibles consecuencias de orden público y seguridad ciudadana.
3. Amenaza FIMI que apunta de manera particular a partidos y candidatos individuales buscando polarizar la opinión de los votantes respecto a ellos, para posicionar o desmejorar una opción política conforme a los intereses particulares del actor. A veces se aprovechan narrativas ya existentes que se alimentan de teorías conspirativas o extremistas, con las que dañar la imagen de un candidato y, con ello, agrietar sus aspiraciones políticas para desalentar que se presente a las elecciones o acabe haciendo declaraciones que, definitivamente, le saquen de las opciones de alcanzar su objetivo.
4. Amenaza FIMI que directamente busca socavar la confianza en la democracia como sistema político y el apoyo de la sociedad a sus instituciones, a través de falsas acusaciones de fraude electoral, resultados manipulados, irregularidades en el proceso de votación o de recuento de votos, con el riesgo de que los ciudadanos no acudan a las urnas y las posibles protestas derivadas, consiguiendo de esta manera enturbiar las elecciones y transmitir una imagen de falsa democracia.
5. Amenaza FIMI que, principalmente a través de ciberataques, acomete contra las infraestructuras críticas que dan soporte a los procesos electorales, con la idea de interrumpir el normal desarrollo del proceso de votación y lanzar el mensaje de que es un sistema inseguro y de fácil acceso para su manipulación, independientemente del éxito real alcanzado por el ataque.

Esta categorización de la amenaza se complementa con un marco cronológico que fija la relación entre el periodo temporal del proceso de elecciones y las características del ataque FIMI[1480]:

1. El *período preelectoral*, que llega hasta un año antes de la fecha de la votación, donde los actores de la amenaza crean la infraestructura para influir en el consumo de información por parte de sus audiencias objetivo, mediante la creación de narrativas críticas o, incluso, el aprovechamiento de las existentes en el seno de la sociedad, para polarizar, socavar la confianza en el sistema electoral y falsear el entorno comunicativo que rodea a las elecciones. En esta fase los ataques ciber buscan penetrar en los sistemas sin ser detectados para

[1480] IBIDEM, páginas 25 a 29.

Ediciones Universidad de Salamanca | CC BY-NC-ND

hacerse persistentes y escalar privilegios que les permitan activarse en fases posteriores.

2. Durante el *mes previo* a la cita electoral, momento de intensificación del discurso político público, la actividad FIMI también aumenta tratando de legitimar y dar mayor voz a los canales de comunicación social previamente establecidos y poder lanzar ataques que socaven la reputación de candidatos y partidos. El objetivo es generar desconfianza en el electorado sobre la integridad del proceso democrático y las instituciones encargadas de preservarlo.
3. Las últimas *72 horas previas* a la votación son cruciales y, por ello, los actores FIMI aprovechan para activar sus estrategias desinformativas con la idea de influir en la disposición de los ciudadanos a votar o en el sentido de su elección. En este momento se desalienta la participación, se presentan falsas pruebas que *castiguen* la imagen de los candidatos objetivos -sabiendo que no hay tiempo posible de respuesta- y se intensifican las acciones orientadas a sembrar la desconfianza en la integridad y legitimidad del proceso de elecciones.
4. La última fase se corresponde con el periodo temporal que abarca desde el *cierre de los colegios electorales hasta la presentación oficial de los resultados*. En este momento los ataques FIMI se enfocan hacia la llamada a la acción ciudadana violenta y reivindicativa para, desde la acusación de fraude electoral y manipulación de los resultados, tratar de sabotear la democracia *desde dentro*, utilizando para ello a la propia sociedad que ha sido llamada a votar.

De esta forma, el Marco de Respuesta FIMI del SEAE ofrece una panoplia de herramientas desde la que diseñar estrategias de protección y defensa, con cuatro niveles de gradación: 1) la identificación del riesgo y de las posibles vulnerabilidades, 2) la detección de la amenaza FIMI, 3) la activación de la respuesta efectiva, y 4) la integración de la información para perfeccionar el proceso[1481].

Abundando en este enfoque integral y cooperativo que refuerza el Parlamento Europeo, orientado a la seguridad e integridad de los procesos democráticos frente a las injerencias extranjeras, en marzo de 2024, el Hybrid CoE[1482] publica el informe *Countering hybrid threats to elections: From updating legislation to establishing collaboration networks*[1483], en el que realiza un análisis específico de las amenazas híbridas con afectación a los procesos electorales democráticos, en concreto las que se han materializado en Europa y EE.UU. a través de ataques físicos, cibernéticos y campañas desinformativas.

El informe clasifica la afectación de estas amenazas a los procesos electorales en razón del área perjudicada, distinguiendo tres posibles formas de hacerlo: a través de la

[1481] IBIDEM, páginas 30 a 33.

[1482] European Centre of Excellence for Countering Hybrid Threats (Centro Europeo de Excelencia para la lucha contra las amenazas híbridas). Vid. supra. apartado 3.5.

[1483] Informe nº 12 de investigación del Consejo de Europa, de 19 de marzo de 2024. Contrarrestar las amenazas híbridas a las elecciones: de la actualización normativa al establecimiento de redes de colaboración. Disponible en https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/ (13/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

interferencia en el funcionamiento del propio proceso de elecciones[1484], socavando la confianza de la ciudadanía en la transparencia del proceso[1485] y, por último, influyendo en la voluntad y la capacidad de los ciudadanos para ejercer su derecho al voto[1486].

En lo referente a la amplia gama de actores, el Hybrid CoE menciona a Estados, a entidades interpuestas patrocinadas por estos, a hackers independientes, activistas, organizaciones y grupos extremistas que buscan la imposición de su particular ideología o, incluso, actores políticos de carácter nacional que trascienden el límite de la *mentira noble* platoniana.

Los actores externos, por su parte, tienen un marcado carácter revisionista, estando liderados por el habitual triunvirato de alto riesgo conformado por Rusia, Irán y China, que comparten el objetivo común de tratar de quebrantar la integridad de las instituciones que sustentan la democracia, a través de la influencia en la opinión pública ciudadana mediante la propaganda y la desinformación, buscando además generar narrativas globales que favorezcan sus propios intereses estratégicos a medio y largo plazo, aprovechando así los procesos electorales como propicio campo de acción de su política exterior para apoyar candidatos afines a sus políticas o desprestigiar a los elegidos sembrando la sospecha de la duda (RUBIO NUÑEZ, 2024).

Respecto a los actores nacionales o internos, suponen una amenaza creciente para las elecciones porque, a menudo, sus acciones caen en el espacio difuso de las zonas legales y éticas no definidas, lo cual dificulta su catalogación y, al mismo tiempo, poder ser contrarrestadas, proponiéndose para ello la mejora de la concienciación pública sobre la amenaza y la mejora de los marcos legales en los que encuadrar dichas actuaciones (BAY, 2024, pág. 14).

Ante este complejo panorama de permanente desafío para las democracias a través de la amenaza a sus procesos electorales, clave de la defensa de sus principios y valores, el informe del Hybrid CoE señala que la protección electoral se basa en la gestión de riesgos, el fortalecimiento de la resiliencia y la gestión de crisis:

> "Risk management involves creating procedures to identify and prevent potential negative events that an organization may face. Building resilience focuses on strengthening an organization or system to sustain operations during times of

[1484] Por ejemplo, saboteando actos de campaña o el desempeño de las mesas electorales impidiendo el acceso al lugar donde se constituyen, o incluso amenazando a funcionarios con responsabilidades en el desarrollo del proceso. También entrarían en este supuesto los ciberataques a las infraestructuras de soporte de los sistemas del proceso electoral, el ataque a las bases de datos del censo electoral, o un ataque de denegación de servicio a la página web oficial encargada de ir reflejando los resultados del recuento de votos. Disponible en: https://www.elconfidencial.com/espana/2023-07-23/elecciones-23j-hackers-prorrusos-atacan-interior-votacion_3706141/ (14/05/2024).

[1485] Por ejemplo, a través de la difusión de teorías conspirativas en las que se ponga en duda el sistema de recuento de votos o directamente se aluda al fraude, para erosionar así la confianza en el proceso.

[1486] Por ejemplo, el transporte coercitivo de personas a colegios electorales para ejercer el voto dirigido, o mediante la compra de votos por correo. Disponible en: https://elpais.com/espana/2023-05-23/al-menos-seis-detenidos-por-la-compra-de-votos-en-melilla.html https://www.elconfidencial.com/espana/2023-05-18/melilla-duplica-record-voto-correo-acusaciones-fraude-masivo_3631502/ (14/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> stress and shocks resulting from the risks that do materialize. In contrast, crisis management is mainly concerned with recovering from disruptions and re-establishing normalcy after a crisis"[1487] (BAY, 2024, pág. 15).

Consecuentemente, la propuesta planteada para mejorar la capacidad de hacer frente a las amenazas híbridas dirigidas a las elecciones se consigna en torno a nueve esferas de actuación:

1. La permanente adaptación normativa para conseguir un marco jurídico nacional sólido, con el cual ir articulando la respuesta legislativa a las diferentes modalidades evolutivas de la amenaza para los procesos electorales.
2. El adecuado análisis de contingencias negativas para la identificación de vulnerabilidades del proceso electoral, con el objetivo de componer un mapa de riesgos que nos permita definir la estrategia integral para mitigar la amenaza.
3. La implementación de medidas de fortalecimiento del sistema electoral en el ámbito de la prevención de riesgos, la detección del ataque y la gestión de la respuesta, que coadyuven al enfoque unificado de la seguridad y la resiliencia del conjunto del proceso.
4. La adecuada gestión de la comunicación estratégica por los organismos implicados, con el objetivo de inspirar en los ciudadanos un espíritu de confianza en las campañas políticas y los procesos electorales. Para ello, se propone la difusión de información precisa y confiable que desmonte las narrativas desinformadoras -*prebunking*-, junto con la alfabetización digital y mediática que ayude a los electores a evaluar convenientemente la información a la que acceden a través de los medios de comunicación y las redes sociales, para formarse su propia opinión y tomar conciencia sobre la gravedad de la amenaza híbrida.
5. La cooperación entre las autoridades estatales y las entidades públicas y privadas para garantizar la seguridad y la integridad de las elecciones, apostando por la creación de *redes nacionales de cooperación electoral*, siguiendo el ejemplo de la *Red Europea de Cooperación Electoral* que, a su vez, interactúa con aquellas.
6. La programación y desarrollo de ejercicios tipo *Red Team* para probar la consistencia del sistema, evaluar la eficacia de las medidas de seguridad, valorar la eficacia de los protocolos de respuesta y descubrir las debilidades del procedimiento.
7. El establecimiento de mecanismos de detección y alerta temprana para incidentes de seguridad en las elecciones que posibiliten una respuesta rápida, eficaz y coordinada entre las empresas de ciberseguridad, las Fuerzas y Cuerpos de Seguridad y los órganos electorales centrales.
8. La construcción de la respuesta unificada y coordinada a todos los niveles del Estado, integrando el esfuerzo de instituciones, organismos y empresas implicadas en el proceso de elecciones, tanto en el ámbito físico como digital.

[1487] "La gestión de riesgos implica la creación de procedimientos para identificar y prevenir posibles eventos negativos a los que se puede enfrentar una organización. El desarrollo de la resiliencia se centra en el fortalecimiento de una organización o sistema para mantener las operaciones en tiempos de estrés y perturbaciones resultantes de los riesgos que se materializan. Por el contrario, la gestión de crisis se ocupa principalmente de recuperarse de las perturbaciones y restablecer la normalidad después de una crisis" (Traducción propia).

Ediciones Universidad de Salamanca | CC BY-NC-ND

9. Trabajar en la capacidad de recuperación de la normalidad del proceso electoral una vez que se haya sufrido el impacto de un ataque. Para ello será determinante la evaluación exhaustiva del incidente y de las medidas adoptadas, así como la posterior integración de las lecciones aprendidas.

Esta amplia panoplia normativa vertebra la organización de recursos y medios que la Unión ha activado para responder con contundencia tanto a la amenaza desinformativa como a los intentos de injerencia extranjera en sus procesos electorales, que no buscan sino deteriorar la confianza en el modelo de Estado democrático como garante de libertades y derechos fundamentales, buscando fomentar la aparición de movimientos *antidemocráticos*, que la desprecian como destino político deseable, o movimientos *hiperdemocráticos*, para quienes "la dosis de democracia de los regímenes actuales es insuficiente y debe ser ampliada" (SANSÓ-RUBERT PASCUAL, 2024, pág. 44).

Prueba de ello son las operaciones que el SEAE en colaboración con las autoridades nacionales ha llevado a cabo, en la fase previa a las elecciones europeas de junio de 2024, para sacar a la luz narrativas pro Kremlin que buscaban quebrantar el apoyo de los aliados a Ucrania desde sitios web que se hacían pasar por medios de comunicación occidentales[1488], difundir de forma masiva las publicaciones de cuentas de redes sociales de agencias de prensa e instituciones oficiales rusas ensalzando la *operación militar especial* con el objetivo de polarizar el debate público en Europa[1489], generar descontento en la ciudadanía alemana respecto a las instituciones del Gobierno Federal a través de más de 50.000 cuentas falsas de usuario en la plataforma X[1490] o, también, el intento de colapsar a más de 800 verificadores de datos en más de 75 países para derivar sus recursos y esfuerzos hacia piezas de información simulada o inexistente[1491].

A partir de aquí, las elecciones europeas de 2024 se afrontan desde las instituciones con una estrategia basada en tres pilares fundamentales:

1. La prevención desde la detección temprana de las narrativas desinformadoras, para comenzar a actuar antes de que se materialice la amenaza a partir de los parámetros de la *FIMI toolbox*.
2. La mitigación mediante la acción proactiva, a través de una comunicación positiva de información de calidad, buscando *ocupar el espacio* para impedir o, al menos, dificultar la libre expansión de la desinformación. En esta tarea resulta

[1488] Se trata de la *Operación False Facade,* de mayo de 2024. Disponible en: https://euvsdisinfo.eu/building-a-false-facade/ (27/10/2024).

[1489] *Operación Portal Kombat* que lideró el servicio francés VIGINUM desde finales de 2023 y hasta febrero de 2024, a través del análisis de una red de supuestas webs de información que difundían contenidos prorrusos a nivel internacional. Disponible en: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2024/article/foreign-digital-interference-result-of-investigations-into-the-russian (27/10/2024).

[1490] Se trata de la Operación Doppelgänger. Disponible en: https://euvsdisinfo.eu/es/la-campana-doppelganger-de-nuevo-en-accion-destapando-actividades-de-fimi-dirigidas-en-contra-de-las-elecciones-europeas-de-2024/
https://www.dw.com/de/ausw%C3%A4rtiges-amt-prorussische-desinformationskampagne-auf-x-aufgedeckt/a-68096288 (27/10/2024).

[1491] *Operación Overload* de la compañía Check First. Disponible en: https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf (27/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

de máxima utilidad la experiencia acumulada y los canales de comunicación de los verificadores.

3. Fomentar la resiliencia social e implicar a toda la sociedad civil a través de actividades de sensibilización frente a la desinformación, la alfabetización mediática y el fomento del espíritu crítico individual para la evaluación de la información que se recibe, entre otros. La idea es clara: la cooperación multiplica la capacidad de resistir a la desinformación.

Posteriormente, a principios de diciembre de 2024, el Tribunal Constitucional de Rumanía anula las elecciones presidenciales a menos de 72 horas de la celebración de la segunda vuelta del proceso[1492], basándose en datos que demostrarían una campaña de injerencia rusa que habría favorecido al candidato de extrema derecha y posiciones nacionalistas, Calin Georgescu, ganador de la primera vuelta de los citados comicios. La posición crítica de Georgescu hacia el apoyo militar a Ucrania y sus postulados fuertemente conservadores y proteccionistas evidenciaban que un nuevo resultado favorable para él en segunda vuelta supondría un cambio en la política interna del país y, también, un reforzamiento en la línea de tendencia en Europa hacia gobiernos nacionalistas que desafían la cohesión de la UE y complican la respuesta cohesionada a la guerra. Como señala el profesor Rubio Nuñez, los motivos alegados por el alto Tribunal, a la sazón la ventaja obtenida por uno de los candidatos mediante las redes sociales, la opacidad de los algoritmos subyacentes que lo permiten y las sospechas de financiación irregular, no pueden obviar el hecho de que *la decisión se adopta sin un marco normativo previo adecuado*. Esta actuación del Tribunal Constitucional de Rumanía genera, cuando menos, una percepción de *falta de respeto por la voluntad popular* manifestada en las urnas puesto que, para la mayoría de los ciudadanos ajenos a la gravedad de la injerencia, su voto emitido refleja *fidedignamente* su opinión, para ellos conformada de manera libre y sin condicionamientos. Inevitablemente, esta situación puede tener efectos en posteriores llamamientos electorales, aparte de generar inestabilidad en el país a costa de la duda vinculada a la transparencia y el propio carácter democrático del proceso (RUBIO NUÑEZ, 2024).

Por todo lo dicho, podemos sostener que el pensamiento racional, crítico y orientado que sustenta la sociedad inclusiva que caracteriza a la democracia es prácticamente imposible en un contexto desinformativo, por lo cual:

> "[…] la detección de la manipulación informativa […] es el primer nivel que hay que activar para contrarrestar la desinformación […]. La verificación es necesaria primero para después proceder a refutar falsedades. Identificar y detectar la manipulación es algo perentorio ante campañas de desinformación por el enorme

[1492] El seguimiento en prensa de esta decisión del Tribunal Constitucional de Rumanía ante la campaña híbrida rusa en plataformas sociales, principalmente TikTok. Disponible en: https://elpais.com/internacional/2024-12-06/el-constitucional-de-rumania-anula-la-primera-vuelta-de-las-presidenciales-tras-revelarse-la-campana-de-ataques-hibridos-rusos.html https://es.euronews.com/my-europe/2024/12/08/anulan-las-elecciones-presidenciales-en-rumania-tras-las-denuncias-de-interferencia-extran https://www.newtral.es/rumania-anula-elecciones/20241206/ https://efe.com/mundo/2024-12-06/rumania-elecciones-presidenciales-anulacion-justicia/ (14/12/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

> potencial negativo que conllevan, mucho mayor que *fake news* aisladas y puntuales" (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 139).

En este contexto, la noticia publicada en enero de 2025 relativa al cierre del programa de verificación profesional e independiente en Meta, en la cartera de servicios prestados en EE.UU., y su sustitución por el modelo de verificación alternativo conocido como *community notes*[1493], supone un punto de inflexión en la verificación profesional de contenidos en la red. Al amparo de argumentos como el que señala que los verificadores profesiones también tienen sesgos, se abre una línea paralela de interpretación de la función de velar por la seguridad y la información veraz en el ciberespacio ya avanzada por X, en la que es la propia comunidad de usuarios la encargada de identificar y señalar las publicaciones potencialmente engañosas o desinformadoras. La UE, por su parte, se mantiene firme en la efectividad y utilidad del sistema de verificación profesional e independiente y advierte a Meta que deberá cumplir con la DSA en el ámbito de soberanía digital europea[1494].

En definitiva, podemos colegir que las elecciones democráticas son hoy día vistas por los Estados autocráticos como una oportunidad para promover sus intereses desde la Zona Gris, recurriendo a la desinformación y la manipulación de la información para desprestigiar a las figuras políticas no afines a sus ideas, apoyar a los candidatos que más les favorezcan, instrumentalizar la problemática social y política existente en el Estado objetivo o, en definitiva, minar la credibilidad de las democracias y sus instituciones. Por ello, hay que avanzar en la forma de medir y valorar los efectos de la desinformación superando cajones de clasificación como los de actor externo-interno o estatal-privado, en la idea de conseguir que dicha evaluación sea un eje transversal para la mejor gobernanza democrática.

7.4. Conclusiones

Como ya pudimos comprobar en el Capítulo 6, la Zona Gris se presenta como un entorno de confrontación *pacífica* y de proyección de influencia *soterrada* entre Estados que obliga a las sociedades democráticas, como las europeas, a unirse en la defensa de sus principios fundamentales a través de un firme y decidido compromiso que les permita articular una estrategia de respuesta unificada frente a los riesgos compartidos.

Desde 2015 la amenaza híbrida manifestada, principalmente, a través de las campañas desinformativas y la injerencia extranjera, ha sido entendida por la Unión como un asunto de defensa y seguridad nacional que, como tal, requiere el compromiso

[1493] Puede traducirse como *notas de la comunidad.*

[1494] Amplia repercusión en prensa. Disponible en: https://efe.com/ciencia-y-tecnologia/2025-01-07/meta-verificacion-notas-comunidad-x/
https://www.bbc.com/mundo/articles/clyjlp66q2po
https://www.rtve.es/noticias/20250108/meta-elimina-verificacion-profesional-whatsapp-facebook-instagram-para-pasarse-a-notas-comunidad/16399446.shtml
https://www.swissinfo.ch/spa/ce-avisa-a-meta-que-tiene-que-respetar-normativa-sobre-moderaci%C3%B3n-de-contenidos-en-la-ue/88688106
https://elmon.cat/es/mundo/bruselas-advierte-a-meta-sobre-la-eliminacion-de-verificadores-de-datos-949634/ (11/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

individual de cada Estado pero, al mismo tiempo, exige un enfoque integral basado en la solidaridad y la asistencia mutua, con el objetivo añadido de generar sinergias asociativas con sus aliados para poder afrontar con éxito los nuevos desafíos planteados.

Esta estrategia colaborativa se operativiza a través de un cuerpo normativo extenso y complejo que se apoya en herramientas de diversa naturaleza -protocolos de actuación, estructuras de supervisión y apoyo, grupos de trabajo, acciones multidimensionales, elaboración de informes, etc.- cuyos objetivos se sintetizan en dos: la protección de la democracia como sistema de gobierno y la garantía del acceso libre de los ciudadanos a la información para participar en la defensa de la misma.

Resulta éste un punto nuclear de la cuestión por cuanto la base de la democracia representativa no es otra que la participación política del pueblo, a través de su *voto consciente*, el cual "supone una decisión político-electoral bien informada, deliberada y alineada con las convicciones e intereses del votante" conforme a la adecuada comprensión de tres parámetros: 1) las necesidades del país, 2) las opciones más adecuadas para atenderlas, y 3) los candidatos más idóneos para liderar su aplicación (RUBIO NUÑEZ, FRANCO ALVIM, & DE ANDRADE MONTEIRO, 2024, págs. 76-77). Y es por ello que disponer de un entorno social y comunicativo *limpio*, que permita a las personas discernir entre las fuentes de información fiables y las falsas o tendenciosas, se erige en elemento fundamental para preservar la seguridad de la democracia constitucional que, inexorablemente, "lleva al Estado a creer en la responsabilidad de sus propios ciudadanos" (RUBIO NUÑEZ, FRANCO ALVIM, & DE ANDRADE MONTEIRO, 2024, pág. 78)

Es este elemento de responsabilidad ciudadana imbricado con el libre acceso a la información veraz el que determina la importancia de preservar la seguridad de los procesos electorales, máxima expresión de la voluntad popular en democracia. De ahí la atención prestada por la UE al impacto que la desinformación y la influencia de terceros Estados, potenciado por el elevado nivel de digitalización y tecnologización de las campañas políticas, pueda tener en la base de organización del sistema democrático y, a la postre, en su propia subsistencia.

Ediciones Universidad de Salamanca | CC BY-NC-ND

CAPÍTULO 8. LA RESPUESTA ESPAÑOLA FRENTE A LA AMENAZA DESINFORMATIVA CON AFECTACIÓN A LA SEGURIDAD NACIONAL

Cada vez existen más evidencias de la instrumentalización de vectores de inseguridad tradicionales por parte de actores estatales o paraestatales con el objetivo de llevar a cabo campañas de influencia con potencial capacidad de afectación al orden público[1495] o, también, de desestabilizar el normal funcionamiento institucional de sus adversarios, con manifiestas repercusiones en la seguridad nacional de estos.

El firme asentamiento de bandas de crimen organizado en el norte de Europa, la penetración de las mafias transnacionales en Países Bajos, los violentos enfrentamientos entre grupos delincuenciales en Francia, la irrupción de brotes de radicalismo violento islamista en Alemania o las estructuras de tráfico de personas que dirigen los flujos migratorios que parten del Continente Africano hacia el Viejo Continente, plantean serios desafíos de seguridad que repercuten directamente en la desestabilización de las sociedades democráticas europeas, las cuales, como ya hemos analizado en capítulos anteriores, se ven abocadas a enfrentar un horizonte de riesgos híbridos que exigen un firme compromiso político y social que no resulta fácil de alcanzar en el actual contexto de polarización y extremismo ideológico.

Las estructuras criminales han entrado por propia iniciativa en una dinámica colaboracionista con actores estatales que pueden ayudarles a desarrollar o, incluso, ampliar sus ya de por sí extraordinarias capacidades para obstaculizar, colapsar o parasitar el entramado institucional de un Estado, generando una amenaza grave y sostenida en el tiempo que puede llegar a causar metástasis sistémica en sus órganos de gobierno.

De otra parte, los Estados iliberales y autocráticos, hostiles al orden internacional, tratan de aprovechar los movimientos sociales antisistema y las problemáticas delincuenciales más graves en el marco del conflicto híbrido para, desde posiciones asociativas o de actores interpuestos tipo *proxies*, desplegar sus acciones ofensivas en el ciberespacio o de injerencia en los procesos democráticos de sus oponentes con el afán de desacreditarlos y de "instaurar un equilibrio de poder en la esfera internacional acorde con sus intereses estratégicos" (SANSÓ-RUBERT PASCUAL, 2024, pág. 32)

[1495] En este sentido, sirva como ejemplo la acusación que en septiembre de 2024 sostiene la Fiscalía sueca contra el servicio de inteligencia de Irán de piratear un operador de SMS en 2023 para lanzar una campaña de influencia con potencial afectación al orden público, a través de mensajes que incitaban a la acción contra los manifestantes que habían protagonizado la quema de libros del Corán. Disponible en: https://es.euronews.com/2024/09/24/suecia-acusa-a-iran-de-piratear-su-servicio-de-mensajeria-tras-los-incidentes-de-la-quema-
https://www.swissinfo.ch/spa/suecia-acusa-a-ir%C3%A1n-de-ciberataque-para-provocar-reacciones-a-las-quemas-del-cor%C3%A1n/87605518
https://apnews.com/world-news/general-news-3e78ea8cbd3ff27bb0edd4975c5d8dd0 (27/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Es producto de todo ello que, en los últimos años, las sociedades libres y democráticas que protegen entornos plurales y abiertos hayan observado anonadadas campañas de desinformación, orquestadas por actores revisionistas con objetivos claramente interesados, que han causado un profundo impacto en sus pilares constitutivos. Un ejemplo fue la pandemia del COVID del año 2020, pero también fueron del todo ilustrativos respecto a su capacidad de influencia el proceso de elecciones a la Presidencia de los Estados Unidos del año 2016 y la consulta plebiscitaria del Reino Unido, en el mismo año, para decidir su salida de la Unión Europea -el conocido popularmente como *Brexit*-. Los tres constituyen un manifiesto ejemplo de la eficacia destructiva que alcanza la orquestación de una estrategia que utilice, por un lado, la desinformación como uno de sus vectores de ataque y, por otro, a los ciudadanos como medio para desgastar al propio sistema de gobierno democrático, que claramente sucumbe si la sociedad no puede confiar en las instituciones, en las campañas políticas, en los medios de comunicación o en sus representantes electos (VAN HEEMSTRA FERNÁNDEZ, 2023, pág. 14).

Y esta eficacia es un relevante aspecto a considerar porque, ante la superioridad del instrumento militar en un potencial conflicto convencional, los estados revisionistas han llegado a la conclusión, por la vía de los hechos, de que las estrategias híbridas con fuerte carga de desinformación son plenamente eficaces para lograr sus objetivos políticos. En el actual escenario multipolar y competitivo, donde la mente se convierte en uno de los principales campos de batalla, la confrontación cognitiva entre Estados a través de la instrumentalización de las narrativas resulta esencial, siendo así que la alteración de la realidad mediante los procesos de desinformación va dirigida a las percepciones, los sentimientos, los afectos, las voluntades y las opiniones que terminan por afectar a los procesos de toma de decisiones, aprovechando la desigual combinación de razón y emoción.

En este punto nos permitimos recordar que la UE viene considerando la lucha contra las amenazas híbridas y la desinformación un asunto de defensa y de seguridad nacional cuya responsabilidad principal compete, como tal, a sus Estados miembros si bien, al tratarse de una amenaza común a todos ellos, debe afrontarse desde una estrategia coordinada europea que permita una respuesta unificada de mayor eficacia[1496], que a

[1496] Sirvan como ejemplos de esta política que vincula la amenaza híbrida y la desinformación con la seguridad nacional, con la consiguiente responsabilidad directa de los Estados miembros para la defensa de sus propios intereses, aunque bajo la actuación coordinada y conjunta de toda la Unión con el ánimo de hacer más efectiva la respuesta a dicha amenaza, lo establecido por la Comunicación conjunta al Parlamento Europeo y al Consejo, sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea. Bruselas, 6.4.2016. JOIN(2016) 18 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52016JC0018.
También en este sentido el Informe INGE 2 sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación, de 15 de mayo de 2023 (Informe A9-0187/2023; relatora Sandra Kalniete). Disponible en: https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html#_section2.
De igual manera se pronuncia la Resolución del Parlamento Europeo, de 1 de junio de 2023, sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2022/2075(INI)). DOUE C, C/2023/1226 de 21.12.2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C_202301226 (27/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

su vez mira hacia los aliados con el ánimo de fomentar la cooperación internacional para un reforzamiento mutuo que, también, recurre a la coordinación público-privada, tal y como señala Guilló:

> "En la actualidad, los tres documentos estratégicos de Seguridad y Defensa de la OTAN, la UE y España, esto es «el Nuevo Concepto Estratégico», la «Brújula Estratégica» y la citada «ESN21», respectivamente, presentan tres puntos de encuentro respecto de las campañas de desinformación. Primeramente, la gran importancia que están apreciando en estos desafíos a la política de seguridad aliada. En segundo lugar, la coincidencia en identificar a Rusia y China como los actores hostiles más activos en este ámbito. Para finalizar, el modo en que esta amenaza se debe afrontar: a través de la cooperación internacional y de la coordinación entre organismos públicos y privados" (GUILLÓ ROT , 2024, pág. 8) .

8.1. El reto: la identificación de la amenaza desinformativa como ámbito de interés para la seguridad nacional española

Podemos comenzar señalando que España identifica la desinformación como parte de la amenaza a partir de la experiencia de otros países de su entorno y, principalmente, a través de las iniciativas europeas del Consejo, el Parlamento y el SEAE, analizadas en el capítulo anterior. La convicción de que el uso de la información falsa ha llegado para quedarse se gesta a partir de dos hechos destacados en este sentido: la invasión rusa de Crimea en el año 2014, como primera referencia de conflicto híbrido donde la información opera como eje vertebral, y las elecciones presidenciales de EE.UU. del 2016, que demuestran el uso combinado de ciberataques y narrativas desinformativas en el marco de una estrategia híbrida superior, orquestada desde Rusia (BADILLO & ARTEAGA, 2024, pág. 9). Desde luego, no parece casual que el común denominador de ambas acciones sea el actor que las impulsa.

Es en este contexto en el que, como vimos en el Capítulo 4 al estudiar el modelo español[1497], la Ley de Seguridad Nacional (LSN) del año 2015[1498] refleja la capacidad de adaptación a la permanente evolución de la amenaza y define como ámbitos de especial interés la ciberseguridad y las crisis sanitarias, al tiempo que identifica al Sistema de Seguridad Nacional como clave de acción, en el que se integra la implicación activa de toda la sociedad desde un enfoque holístico y colaborativo de la seguridad y la defensa de la nación.

Tal y como señala el Preámbulo de la citada LSN, "la seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones", de donde dimana la encomienda a los poderes públicos para, bajo su responsabilidad, puesto que de una política de Estado se trata, construir la estructura normativa,

[1497] Ver Capítulo 4, apartados 4 y 5.

[1498] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. BOE núm. 233, de 29 de septiembre de 2015. BOE-A-2015-10389. Disponible en: https://www.boe.es/eli/es/l/2015/09/28/36/con (07/12/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

procedimental y de recursos que permita responder con eficacia a las amenazas que la desafíen.

En este sentido, resulta clave para el objeto de nuestro estudio referirnos al artículo 3 LSN, que dispone:

> "A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos".

Se configura de esta manera una definición integral de las tres dimensiones de la seguridad nacional:

1. Primeramente, la *individual*, referida a la protección de las personas, sus derechos y libertades.
2. En segundo lugar, la esfera *colectiva*, representada por la garantía de la defensa de España como nación y los principios y valores constitucionales que se han dado todos los españoles para vivir en sociedad.
3. En tercer lugar, el aspecto *global* de la seguridad, manifestado a través del compromiso, junto a nuestros socios y aliados, con el Derecho Internacional y las obligaciones que conlleva.

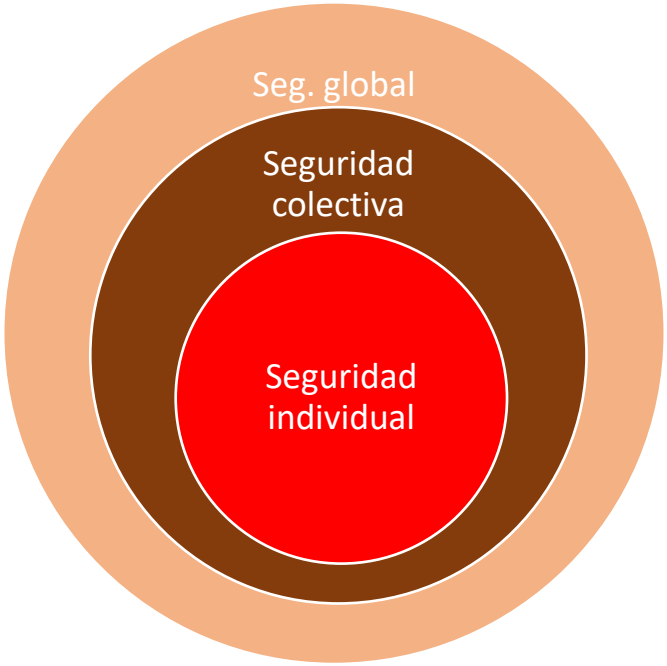


Gráfico 8.1.
Los tres círculos de la seguridad nacional española
Fuente: propia

Esta definición supera la concepción tradicional de seguridad nacional y camina hacia una seguridad ampliada que señala a la persona como centro del esquema de protección

Ediciones Universidad de Salamanca | CC BY-NC-ND

que, a su vez, se ve fortalecido a través de la cooperación con nuestros socios y aliados para, de esta manera, contribuir a la paz y la estabilidad internacionales. Así, a través de esta visión de la seguridad nacional, no solo se garantiza la respuesta frente a los riesgos y amenazas que atacan al Estado, sino también la defensa de los derechos, las libertades y el bienestar ciudadano, para que ningún desafío de seguridad dañe la vida en comunidad y el normal desarrollo personal en el marco del Estado social y democrático de Derecho[1499].

Con esta perspectiva tridimensional de la seguridad nacional, la LSN pretende atender al amplio espectro que presenta la amenaza en el actual contexto geoestratégico internacional, en el que la Zona Gris cada vez ocupa más espacio en las relaciones entre Estados que, por ello, recurren a los conflictos híbridos para articular sus estrategias defensivas y ofensivas. Es así que la desinformación deba centrar nuestra atención al estudiar las implicaciones de estos nuevos desafíos para la seguridad nacional española.

8.1.1. El señalamiento de la desinformación como amenaza y el inicio de la configuración de la respuesta

Conforme a lo ya estudiado en capítulos anteriores, el marco regulatorio español y las políticas públicas desarrolladas en esta materia se encuadran en el contexto normativo europeo y en las líneas de acción en él definidas[1500]. Partiendo de este presupuesto, España se incorpora en julio de 2017 al por entonces recién creado *Hybrid CoE*[1501] como parte de su compromiso con la estrategia de respuesta coordinada europea frente a las amenazas híbridas[1502]. De manera consecuente y, en cierta medida, alentados por los indicios de injerencia rusa en el contexto del referéndum de independencia de Cataluña de octubre de ese mismo año (BADILLO & ARTEAGA, 2024, págs. 77-79), los redactores de la Estrategia de Seguridad Nacional (ESN) del 2017 se refieren a la desinformación como parte de los riesgos tecnológicos asociados a la repercusión de la actividad del ciberespacio en la seguridad nacional, no como una amenaza específica (BADILLO MATOS, et al., 2023, p. 27), señalando que su utilización:

> "[…] como medio para la realización de actividades ilícitas, acciones de desinformación, propaganda o financiación terrorista y actividades de crimen organizado, entre otras, impacta en la Seguridad Nacional, amplificando la complejidad y la incertidumbre, y también pone en riesgo la propia privacidad de los ciudadanos"[1503].

[1499] Concepto de Seguridad Nacional que señala el artículo 3 de la Orden PCM/575/2021, de 8 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 25 de mayo de 2021, por el que se aprueba el Plan Integral de Cultura de Seguridad Nacional. BOE núm. 138, de 10/06/2021. Referencia BOE-A-2021-9631. Disponible en: https://www.boe.es/eli/es/o/2021/06/08/pcm575 (07/12/2024).

[1500] Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). Informe C: Desinformación en la era digital. Página 24/26 (2023). Disponible en: www.doi.org/10.57952/j3p6-9086 (07/12/2024).

[1501] Puede consultarse la lista de integrantes del Hybrid CoE en su página web. Disponible en: https://www.hybridcoe.fi/wp-content/uploads/2024/08/Hybrid_CoE_Participating-states_Albania_240830.pdf (07/12/2024).

[1502] Ver epígrafe 7.1.3. sobre la estrategia de respuesta europea frente a la amenaza híbrida.

[1503] Estrategia de Seguridad Nacional 2017. Op. Cit., página 67.

Ediciones Universidad de Salamanca | CC BY-NC-ND

El año 2019 supone un punto de inflexión en la postura española respecto a la desinformación por cuanto que, en febrero, el Centro Criptológico Nacional (CCN) -estructura dependiente del CNI- elabora la *Guía* sobre *Desinformación en el ciberespacio*[1504] que, por primera vez, se refiere a dicha amenaza en España desde un punto de vista descriptivo, aportando patrones de comportamiento y desgranando la sistemática de las campañas desinformativas, proponiendo "discriminar la influencia legítima de la ilegítima en asuntos donde existía polarización social y política" (BADILLO & ARTEAGA, 2024, pág. 17). Asimismo, ya alerta sobre que la desinformación va minando lentamente la confianza de los ciudadanos en los medios de comunicación tradicionales, en las instituciones públicas e, incluso, en la propia información como elemento fundamental para el libre ejercicio de la decisión democrática, generando de esta manera una sensación de *duda total* que llega a afectar a la propia soberanía del ciudadano. Abundando en este planteamiento y alineado con la Comisión Europea que acababa entonces de publicar su *Comunicación Conjunta para aumentar la resiliencia frente a las amenazas híbridas*[1505], el CCN señala la protección de los ciudadanos como una de las maneras más efectiva de afrontar esta amenaza, proponiendo el acceso a los recursos y las habilidades necesarias que les permitan identificarla, principalmente a través de las redes sociales e Internet. Así, la alfabetización digital de la sociedad española – en el marco de la *cultura de seguridad*- es ya distinguida por el CCN como pieza clave para articular la defensa ante la desinformación: si los usuarios de las redes no son conscientes de la amenaza y, de manera consecuente, no saben identificarla, esta podrá expandirse inadvertidamente e, incluso, llegar a beneficiarse del propio desconocimiento de su existencia para alcanzar sus objetivos.

En esta misma línea, al amparo de lo establecido en el marco de la UE por el *Plan de Acción contra la Desinformación*, en marzo de 2019 el Consejo de Seguridad Nacional (CSN) crea la *Comisión Permanente contra la Desinformación*, orientada a la coordinación interministerial y provista de un marcado carácter técnico. Apenas un mes después, el CSN aprueba la *Estrategia Nacional de Ciberseguridad (ENC)*[1506] en la que, explícitamente, se advierte sobre la peligrosidad de la desinformación en redes sociales por cuanto el ciberespacio, concebido como un vector de comunicación estratégica, influye y modela la realidad a través de la forma de pensar de las personas. Para identificarla y poder contrarrestarla se propone el desarrollo de la *cultura de ciberseguridad* a través de campañas de concienciación ciudadana, el impulso de iniciativas de alfabetización digital, la promoción de la corresponsabilidad y el fomento del espíritu crítico en favor de la información veraz y de calidad[1507].

[1504] Este documento actualmente ya no es accesible desde fuentes abiertas.

[1505] Comunicación Conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo. Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas. Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 13.6.2018. JOIN(2018) 16 final. Este texto fue ya analizado en el Capítulo 3, apartado 5, al estudiar la estrategia de la UE en el ciberespacio, y en Capitulo 7, apartado 7.2.1.2.

[1506] Ver Capítulo 4, apartado 4.7.7.
Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. BOE núm. 103, de 30 de abril de 2019. Referencia BOE-A-2019-6347. Disponible en: https://www.boe.es/eli/es/o/2019/04/26/pci487 (10/12/2024).

[1507] IBIDEM, Capítulo 4 Líneas de acción y medidas.

Ediciones Universidad de Salamanca | CC BY-NC-ND

La ENC igualmente alude a que la explotación de las facilidades que ofrece internet tiene un alto potencial desestabilizador de la sociedad pero que, también, puede emplearse contra Estados, instituciones públicas y privadas, iniciativas políticas o procesos electorales democráticos[1508]. De esta manera, la desinformación en España:

> "[…] queda asignada a los órganos y organismos que forman parte del Sistema de Seguridad Nacional (DSN, Departamento de Seguridad Nacional). El Centro Nacional de Inteligencia (CNI) realiza el seguimiento de los agentes vinculados a las campañas de desinformación y, a nivel interior, también intervienen las Fuerzas y Cuerpos de Seguridad del Estado dentro de sus competencias. El Centro Criptológico Nacional (CCN), dependiente del CNI, crea una unidad sobre desinformación"[1509].

8.1.2. El compromiso español a través del Procedimiento de actuación contra la desinformación y la puerta de entrada de la sociedad civil

Posteriormente, en octubre de 2020, el CSN aprueba el *Procedimiento de actuación contra la desinformación*[1510] que, en su artículo 3, identifica órganos y competencias:

1. El *Consejo de Seguridad Nacional*, con la función de asistir al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.
2. El *Comité de Situación* que lleva a cabo las directrices estratégicas marcadas desde el Consejo de Seguridad Nacional.
3. La *Secretaría de Estado de Comunicación*, responsable de la coordinación de la política informativa del Gobierno, de la política de comunicación institucional del Estado y de la comunicación en situaciones de crisis. Además, actúa como único punto de contacto con la UE en el ámbito de la lucha contra la desinformación.
4. La *Comisión Permanente contra la desinformación*, responsable de la coordinación interministerial a nivel operacional y de la asistencia al CSN sobre aquellos aspectos que requieran la valoración técnica sobre posibles campañas desinformadoras. Está integrada por el DSN, el CNI, la Secretaría de Estado de Seguridad, la Secretaría de Estado de Transformación Digital e Inteligencia Artificial y la Dirección General de Comunicación, Diplomacia Pública y Redes.
5. Las *Autoridades públicas* competentes, entre las que se encuentran los Gabinetes de comunicación de los Ministerios.
6. El *sector privado y la sociedad civil*, con especial referencia a los medios de comunicación, las plataformas digitales, el mundo académico, el sector tecnológico y las organizaciones no gubernamentales, entre otros.

Este *Procedimiento de actuación contra la desinformación*, que básicamente es una norma de estructura y competencias que reparte la responsabilidad entre diferentes actores, cuenta con el respaldo de la Comisión Europea y se adecua a sus parámetros organizativos, facilitando a su vez el intercambio de información con el Sistema de Alerta

[1508] IBIDEM, Capítulo 2 Las amenazas y desafíos en el ciberespacio.
[1509] Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). Informe C: Desinformación en la era digital. Página 24/26 (2023). Disponible en: www.doi.org/10.57952/j3p6-9086 10/12/2024).
[1510] Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. BOE número 292, de 5 de noviembre de 2020. Disponible en: https://www.boe.es/eli/es/o/2020/10/30/pcm1030 (07/12/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Rápida del SEAE, a fin de obtener respuestas coordinadas y conjuntas a las campañas de desinformación. Su desarrollo propone cuatro niveles de activación para la detección y el análisis de las campañas de desinformación y su posible impacto en la seguridad nacional[1511], señalando para cada uno de ellos las funciones concretas que conllevan, los actores involucrados, los mecanismos para el intercambio de información y la forma de comunicación pública a adoptar.

A nuestro parecer, merece la pena llamar la atención sobre dos consideraciones de esta Orden ministerial. La primera de ellas se refiere a una apreciación que figura en su *Contexto*, donde literalmente se señala que:

> "En la lucha contra la desinformación, los ciudadanos consideran que los medios de comunicación, las autoridades públicas y las plataformas de medios sociales son los principales responsables de frenar la divulgación de noticias falsas"[1512].

Conforme a esto, parece desvanecerse el *compromiso de la sociedad* con su propia seguridad, quedando ésta supeditada a la acción del Estado y del resto de actores implicados en la comunicación en el ciberespacio, cuando la experiencia demuestra que la gestión democrática de los riesgos y amenazas requiere contar con el parecer de la sociedad civil, a la que no se puede ni debe excluir del debate sobre una cuestión que afecta a todos (SERRA CRISTÓBAL, 2015, págs. 109-110). Sin embargo, posteriormente, al referirse el *Procedimiento* a la sociedad civil en el apartado de los *Órganos, organismos y autoridades responsables*, ya le confiere un papel esencial en la lucha contra la desinformación mediante el compromiso para su identificación, el freno a su difusión y la promoción de actividades de concienciación sobre la amenaza que representa y la formación que permita evitarla[1513]. Tal vez lo más adecuado habría sido lanzar como idea fuerza, ya desde el *Contexto* que introduce la Orden ministerial, que el compromiso de la sociedad civil con la lucha contra la desinformación es clave para lograr neutralizar los graves efectos que puede llegar a tener sobre la seguridad nacional, la cual no deja de ser *un proyecto compartido de todos y para todos*[1514].

La segunda consideración se refiere al hecho de que, teniendo en cuenta que *la desinformación se vincula a la esfera de la seguridad nacional* al incardinarse *en* el ámbito de actuación del SSN, llama la atención el relevante papel que se le asigna a la Secretaría de Estado de Comunicación en la lucha contra dicha amenaza (CARLÓN RUIZ, 2020). Hubiera parecido más adecuado que fuera el DSN quien asumiera la responsabilidad de la coordinación y la función de punto de contacto con la UE, por razones de coherencia competencial, capacidades relacionadas con la integración de toda la información de seguridad disponible en el panorama nacional y la consiguiente generación de inteligencia para su explotación operativa.

[1511] El artículo 4 del Procedimiento de actuación contra la desinformación señala el Nivel 1 para el nivel técnico de detección y alerta temprana, el Nivel 2 para la coordinación y priorización de esfuerzos contra la amenaza, el Nivel 3 para la adopción de decisiones y el señalamiento de objetivos político-estratégicos, y el Nivel 4 de gestión política en el marco del SSN.
[1512] IBIDEM, página 2.
[1513] IBIDEM, página 4.
[1514] Encabezamiento de la ESN 2017.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En todo caso, podemos decir que la publicación de esta Orden ministerial marca el momento a partir del cual el Gobierno español da muestras fehacientes de su compromiso con la respuesta a la desinformación mediante el diseño de una estructura organizacional propia y la formulación de iniciativas a desarrollar. Sin embargo, aun siendo que la norma no establece medidas concretas sobre la moderación de contenidos, paradójicamente, genera cuando es publicada un amplio debate político y social en torno a su consideración como *el Ministerio de la Verdad*[1515] en base a los *trabajos en la sombra* que, supuestamente, estos órganos del Estado pudieran llevar a cabo con afectación a derechos fundamentales, como la libertad de información del artículo 20 de la CE, por cuanto siendo cierto que aquel debe garantizar la igualdad, la justicia y la seguridad como pilares de la libertad ciudadana, no lo es menos que debe hacerlo dentro del marco del Estado de Derecho, para el que "los derechos de los ciudadanos son un componente esencial de la propia seguridad que se pretende" (SERRA CRISTÓBAL, 2015, pág. 93).

En este sentido, como señalan Badillo y Arteaga, el problema vino derivado de la inadecuada negociación de la *comunicación estratégica* de esta iniciativa con la que el Gobierno, conocedor de la gravedad de la amenaza desinformadora, establecía su plan de respuesta ante una sociedad que, en ese momento, no era plenamente consciente de la misma. A ello hay que añadir que se presentó en medio de un contexto político adverso derivado de las controversias generadas a raíz de la gestión de la crisis sanitaria del COVID-19. Este error de comunicación que puso de relieve la especial sensibilización social en la materia, obligó al DSN a tratar de enmendarlo abriendo la puerta a la constitución de un *espacio de encuentro informal* de la Administración con más de cincuenta expertos de la sociedad civil[1516] con la finalidad de analizar la amenaza y las posibles estrategias para combatirla en los diferentes planos -social, informativo, normativo y tecnológico-, a través de cinco grupos de trabajo[1517] que terminarían conformando un año después el *Foro contra las campañas de desinformación en el ámbito de la seguridad nacional* (BADILLO & ARTEAGA, 2024, págs. 82-83).

[1515] El Tribunal Supremo, en sentencia 1240/2021, de 18 de octubre de 2021, Sala de lo Contencioso, Sección 4, Rec 361/2020, no admite a trámite el recurso de Club Liberal Español contra la citada Orden ministerial. En igual sentido, la sentencia del Tribunal Supremo 1238/2021, de 18 de octubre de 2021, Sala de lo Contencioso, Sección 4, Rec 384/2020. Puede verse la repercusión en prensa de esta cuestión referida al *Ministerio de la Verdad*. Disponible en: https://www.hayderecho.com/2020/12/19/la-orden-contra-la-desinformacion-y-el-ministerio-de-la-verdad/ https://www.abc.es/espana/abci-sanchez-impone-secreto-reuniones-ministerio-verdad-202104160119_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Fespana%2Fabci-sanchez-impone-secreto-reuniones-ministerio-verdad-202104160119_noticia.html https://www.eldebate.com/espana/20211203/ministerio-verdad-sanchez-descubierto.html (10/12/2024).

[1516] El grupo informal de expertos incluía periodistas, académicos, representantes de centros de pensamiento y análisis, organizaciones sociales y plataformas digitales, junto con representantes de la Administración Pública.

[1517] Los cinco grupos de trabajo se constituyen con el mismo esquema organizativo, basado en un coordinador de perfil técnico del ámbito de la Administración, y una serie de expertos en la materia provenientes de diferentes ámbitos de la esfera privada -periodismo, comunicación, universidad, plataformas tecnológicas, verificadores, etc.-, en torno a cinco temáticas principales: definición de conceptos; marco normativo y legislativo; procesos electorales; sensibilización social; estrategia de lucha contra la desinformación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Otra de las puertas de entrada para la iniciativa privada en la lucha contra la desinformación en España es la referida a la verificación de datos, al igual que ocurre en el resto de la Unión. En nuestro caso, está repartida entre proyectos independientes -Maldita.es, Verificat[1518], Newtral, Infoveritas-, y otros vinculados a medios de comunicación de titularidad pública -EFE Verifica, AFP Factual (España), Verifica RTVE- o privada -El Objetivo-[1519].

A este respecto debemos señalar que los verificadores de hechos que pertenecen a grupos o medios de comunicación cuentan con una gran ventaja en términos de rentabilidad, alcance en la audiencia y recursos pero, por el contrario, dependen de las líneas de interés editorial y del apoyo financiero de empleador. Un claro ejemplo supone la cuota de pantalla que tienen los segmentos de verificación de hechos en *El Objetivo*, un programa semanal de la cadena española de televisión La Sexta, que alcanza a entre 1,5 y 2 millones de espectadores cada domingo, probablemente la mayor audiencia regular para un mensaje de verificación en Europa (GRAVES & CHERUBINI, 2016, págs. 8-9), o Verifica RTVE que mantiene una sección diaria en el programa matinal *Las mañanas de RNE* con una cuota del 6.1 del share de las cadenas de radio en 2023 y cerca de 850.000 oyentes[1520]. Por su parte, los proyectos de verificación independientes carecen de los recursos y las audiencias fijas de los anteriores pero, a su favor, están libres de limitaciones editoriales y comerciales y disponen de amplio margen de actuación que les permite adaptarse a la amenaza desinformativa del momento con agilidad y sin condicionamientos (GRAVES & CHERUBINI, 2016, págs. 10-11).

El esfuerzo de esta línea de cooperación público-privada culmina con la publicación del libro *Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil*[1521], que a través de cinco capítulos[1522] analiza

[1518] En noviembre de 2024 el diario La Vanguardia y Verificat firman un acuerdo para, a través de la publicación regular en prensa y redes sociales de las verificaciones de información realizadas, dar mayor publicidad a la detección de bulos y a las narrativas desinformadoras. Disponible en: https://www.lavanguardia.com/vida/20241110/10093363/vanguardia-verificat-alian-desenmascarar-noticias-falsas.html
https://www.verificat.cat/es/verificat-y-la-vanguardia-se-alian-para-hacer-llegar-el-fact-checking-a-nuevas-audiencias/ (17/11/2024)

[1519] Conforme a la guía de verificadores de datos de Reporters´Lab, centro de investigación periodística de la Escuela de Políticas Públicas de Sanford en la Universidad de Duke. Disponible en: https://reporterslab.org/ (13/10/2024).

[1520] Datos estimados por el Marco General de Medios y la página web PRNoticias. Disponible en: https://www.aimc.es/a1mc-c0nt3nt/uploads/2024/01/Marco_General_Medios_2024.pdf
https://prnoticias.com/2024/09/02/rne-despliega-una-bateria-de-novedades-para-superar-la-crisis/#:~:text=847.000%20oyentes%3B%20esa%20es%20la,la%20que%20cuenta%20actualmente%20RNE. (24/10/2024).

[1521] Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil. Catálogo de publicaciones de la Administración General del Estado. Madrid. Septiembre de 2022. El libro fue presentado el 27 de septiembre de 2022 en la sede de la Asociación de la Prensa de Madrid, y puede accederse a él a través del sitio oficial del DSN. Disponible en: https://www.dsn.gob.es/ca/node/18297 (14/12/2024).

[1522] Este libro se compone de cinco capítulos: 1) La desinformación: una amenaza a la democracia; 2) Propuestas de regulación ante la desinformación; 3) La alfabetización mediática, herramienta clave en la lucha contra la desinformación; 4) Propuestas para combatir las campañas de desinformación en procesos electorales; 5) Principios para una estrategia contra la desinformación.

Ediciones Universidad de Salamanca | CC BY-NC-ND

diferentes perspectivas de esta cuestión, entre las que merecen destacarse a nuestra consideración tres de ellas:

1. La plena *vigencia del Derecho Internacional* de manera que, dependiendo de su alcance, naturaleza y efectos, una campaña de desinformación puede constituir una amenaza para la seguridad tanto nacional como internacional y, con ello, implicar el ejercicio de la legítima defensa de acuerdo a las condiciones previstas en la Carta de las Naciones Unidas, el Tratado de la Unión Europea o el Tratado de la OTAN[1523].
2. La *relevancia de la alfabetización mediática*, que debe estar integrada en los planes de educación y que precisa de campañas de información a nivel estatal para concienciar a la sociedad sobre los peligros de este tipo de manipulación. En este sentido, ha de atender a diferentes aspectos como el análisis del exceso de información al que estamos expuestos en nuestra cotidianidad, la comprensión del Derecho como herramienta de protección de los derechos fundamentales, la delimitación conceptual de fenómenos próximos como los bulos y, finalmente, los colectivos a los que debe dirigirse -estudiantes, tercera edad, personas vulnerables, formadores y periodistas-[1524] para hacerlos partícipes en la solución al problema.
3. La *singularidad de España* como lugar especialmente sensible a la difusión de desinformación por su condición de democracia avanzada, la penetración de las redes digitales, el elevado nivel de polarización política, la globalidad del idioma español[1525] y su particular enclave como punto de encuentro multifacético entre América Latina y Europa (BADILLO & ARTEAGA, 2024, pág. 75). Puesto que la relevancia de las campañas de desinformación está directamente relacionada con la capacidad de medir sus efectos e impacto, se propone la redacción de una Estrategia Nacional contra estas que incluya, entre otras, "la identificación de las debilidades actuales, los límites, principios, objetivos y medidas para abordar este tipo de amenazas dentro del Sistema y procedimientos de la Seguridad Nacional"[1526].

8.1.3. El desarrollo del eje de colaboración público-privado: el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional

En paralelo a lo anterior se inicia el proceso de redacción de la ESN 2021[1527] bajo el lema *Un proyecto compartido*, con un innovador enfoque multinivel y de consenso que da entrada a las Comunidades y Ciudades Autónomas de Ceuta y Melilla, así como a los

[1523] Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil. Catálogo de publicaciones de la Administración General del Estado (NIPO 089-22-020-X). Septiembre de 2022. Página 79.
[1524] IBIDEM, páginas 141-154.
[1525] En este sentido, debemos decir que la desinformación se beneficia del idioma español no solo por su carácter global, con más de 600 millones de hispanohablantes, sino que también lo hace del hecho de que las herramientas disponibles en las plataformas para la detección de narrativas desinformadoras están más enfocadas a trabajar con el idioma inglés que con el español.
[1526] IBIDEM, páginas 268-273.
[1527] Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. BOE núm. 314, de 31 de diciembre de 2021 (referencia BOE-A-2021-21884). Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884 (08/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

grupos de trabajo que, liderados por el DSN, recogen las aportaciones de los especialistas institucionales y de la sociedad civil con conocimiento en la materia[1528].

Otra de las novedades cardinales de la ESN 2021 es la inclusión, por primera vez en una ESN española, de las campañas de desinformación y de la injerencia extranjera entre los riesgos que, con alto componente tecnológico e híbrido, amenazan a la seguridad nacional, así como la referencia a la capital importancia de la colaboración público-privada para afrontarla:

> "La colaboración público-privada, especialmente con los medios de comunicación y proveedores de redes sociales, y la sensibilización de la ciudadanía, son aspectos clave a la hora de detectar y hacer frente a las campañas de desinformación"[1529].

Este mismo mensaje destacado, referido a que una sociedad civil concienciada y comprometida con su protección es más segura y resiliente, es el que se proyecta desde el *Plan Integral de Cultura de Seguridad Nacional*[1530], de junio de 2021, que aboga por la *formación* para generar conocimiento y cultura crítica de seguridad, incentiva la divulgación y la comunicación pública a través de los medios y las plataformas digitales, y estimula la participación activa de la ciudadanía y las organizaciones de la sociedad civil en las labores de fomento de la cultura de seguridad nacional, que es una *acción prioritaria* del Gobierno de España.

Con arreglo a esta línea directriz y partiendo de la experiencia aportada por el *grupo informal* de expertos y representantes de la Administración gestado un año antes en el seno del DSN, el 31 de mayo de 2022 el Consejo de Ministros acuerda la creación del *Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional*[1531], como un espacio de colaboración público-privado de *carácter formal* y con fines consultivos, con el objetivo de avanzar en el conocimiento de la amenaza desinformativa y el estudio de las posibles estrategias para abordarla de forma integral y coordinada, así como en la sensibilización de la sociedad para fortalecer su resiliencia ante "los riesgos y amenazas generados por las campañas de desinformación susceptibles de comprometer la Seguridad Nacional"[1532].

Este Foro, presidido por la persona titular del DSN, apoyada en la vicepresidencia por una persona de la Secretaría de Estado de Comunicación, tiene una composición multidisciplinar con representantes de múltiples sectores de la sociedad civil y de la Administración[1533]. Es de destacar que, en su seno, pueden crearse grupos de trabajo *ad*

[1528] Ver Capítulo 4, apartado 4.4.4.
[1529] ESN 2021, Op. Cit., páginas 81-82.
[1530] Ver Capítulo 4, apartado 4.3.3.
[1531] Orden PCM/541/2022, de 10 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 31 de mayo de 2022, por el que se crea el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional y se regula su composición y funcionamiento. BOE núm. 142, de 15 de junio de 2022. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-9965 (14/12/2024).
[1532] IBIDEM, Quinto, punto 4.
[1533] En el Foro se integran 4 representantes de la Administración General del Estado, a través de los Ministerios de Asuntos Exteriores, Unión Europea y Cooperación, Defensa, Interior y Asuntos Económicos y Transformación Digital. Por parte de la sociedad civil, del ámbito académico y privado, 10 representantes elegidos de entre los sectores de la comunicación audiovisual, del periodismo, de los verificadores, de la

Ediciones Universidad de Salamanca | CC BY-NC-ND

hoc para el estudio de temas específicos relacionados con sus fines, incorporando o recabando criterio para ello de personas expertas en la materia. Como señalábamos anteriormente, este nuevo Foro pretende dar continuidad al trabajo conjunto iniciado en el año 2021 bajo el formato de *grupo de expertos informal* coordinado por el DSN[1534], pero con un enfoque de institucionalidad y permanencia que le permita constituirse como el órgano colaborativo de naturaleza pública-privada, referente en la tarea del análisis multidimensional de la amenaza desinformativa y la proposición de marcos de respuesta para combatirla desde puntos de vista heterogéneos.

Siendo el objetivo principal del Foro la lucha contra las campañas de desinformación, se desarrolla a través de dos perspectivas complementarias: una primera, orientada a la promoción de estudios e iniciativas para profundizar en el conocimiento de los riesgos y amenazas causados por la desinformación con afectación a la seguridad nacional y la consiguiente sensibilización de la sociedad al respecto, y una segunda, para comunicar y dar visibilidad a las acciones llevadas a cabo por los actores involucrados del ámbito público y privado para la detección y respuesta frente a esta grave amenaza (ÁLVAREZ ROBLES, 2025, págs. 362-363).

Fruto de esta labor, en diciembre de 2023 se presenta el libro *Trabajos 2023*[1535], como recopilación de las siete iniciativas emprendidas en el Foro que, desde distintas ópticas, abordan el fenómeno de la desinformación y su posible afectación a la seguridad nacional española[1536], de las que destacan las siguientes consideraciones:

1. Son tres las notas esenciales que definen la *naturaleza de la amenaza desinformativa*: su carácter internacional, la magnitud objetivamente inabarcable que ha logrado, y el elevado nivel de eficiencia que alcanza gracias a que "todos somos vulnerables ante ella"[1537].
2. Las democracias deben afrontar esta amenaza desde la firme *defensa de sus principios y valores y la garantía de las libertades de expresión y de prensa*, siendo que la censura nunca debería ser empleada para limitar o controlar la información, so pena de caer en los mismos subterfugios empleados por las

Universidad, de los centros de investigación de la IA, de los centros de análisis jurídicos y sociopolíticos, de los centros de análisis estratégicos de seguridad, de la industria digital, de la publicidad y de las organizaciones de usuarios.

[1534] Creación del Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional. Disponible en: https://www.dsn.gob.es/index.php/en/node/17619 (14/12/2024).

[1535] Foro contra las campañas de desinformación en el ámbito de la seguridad nacional. Trabajos 2023. Catálogo de publicaciones de la Administración General del Estado (NIPO 089-23-041-3). Noviembre 2023. El libro fue presentado el 12 de diciembre de 2023 en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN). Disponible en: https://es.scribd.com/document/694443774/Foro-Campanas-Desinfo-GT-2023-Accesible (20/12/2024).

[1536] El libro de *Trabajos 2023* presenta siete capítulos: 1) Metodología y buenas prácticas para la detección y verificación de la desinformación y para la respuesta en el plano de la comunicación. 2) Estudio de la desinformación rusa a nivel internacional. 3) Efectos psicológicos, radicalización y amplificación de los conflictos sociales causados por la injerencia y manipulación extranjera de la información: análisis y prevención. 4) Mapa de las capacidades de investigación en materia de desinformación en las universidades y centros de investigación españoles. 5) Técnicas, metodologías y prospectiva para combatir la desinformación. 6) Técnicas y metodologías de ciberinteligencia para la investigación de operaciones de información y guerra cognitiva. 7) Las actuaciones de las plataformas de internet en materia de desinformación. Del código de buenas prácticas al reglamento de servicios digitales.

[1537] IBIDEM, página 15.

Ediciones Universidad de Salamanca | CC BY-NC-ND

dictaduras para asegurarse el control de los medios. Este es el punto clave que diferencia a las democracias, como las europeas, de las autarquías, como la rusa o la china, respecto a su respuesta frente a las narrativas desinformadoras.

3. Dos de las principales herramientas con que cuentan las democracias frente a la amenaza desinformativa para alcanzar ese equilibrio entre libertad y seguridad, son la *cooperación internacional* y la *coordinación de todos los actores* implicados en la defensa de dichos valores y la legitimidad del marco institucional que los respalda. Estos no son otros que los verificadores especializados, las administraciones públicas, el sector privado -academia, investigadores y periodistas-, las organizaciones de la sociedad civil y, lógicamente, las grandes plataformas y los prestadores de servicios en línea como principales garantes de la seguridad de sus clientes. En este sentido, destacar la utilidad de la labor desempeñada por los verificadores a través de la refutación de falsedades en Internet y a su labor activa para evitar la difusión de contenidos engañosos o descontextualizados en los medios de comunicación[1538].
4. Otra de esas valiosas herramientas en la lucha contra la manipulación informativa es la referida al impulso de una *estrategia* basada en el fomento de programas de alfabetización mediática y de sensibilización de la población, la apuesta por la transparencia y la comunicación institucional proactiva para ocupar el espacio informativo con narrativas contrastadas y, finalmente, el estímulo del pensamiento crítico ciudadano que lleve a la búsqueda de diferentes perspectivas de opinión y fuentes de información alternativas.
5. La *IA* es sin duda un *potenciador de la amenaza desinformativa*, porque eleva exponencialmente la cantidad, la calidad y la verosimilitud de los contenidos falsos generados, pero *también abre nuevas capacidades de respuesta* mediante el rastreo automático de narrativas, la detección de patrones o la ordenación de contenidos para priorizar el trabajo de verificación, entre otros.

Consolidada ya la iniciativa nacional de colaboración público-privada que representa el *Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional*, en enero de 2025 se publica su segundo texto: *Iniciativas 2024*[1539]. En esta ocasión, el Foro ofrece a través de seis capítulos un recorrido por algunas de las aristas más cortantes que presenta la desinformación, que van desde la delimitación conceptual a la ingeniería de la desinformación, pasando por el escepticismo mediático y ciudadano ante la posible afectación a la seguridad nacional de esta amenaza, entre otros[1540]. Este documento

[1538] Foro contra las campañas de desinformación en el ámbito de la seguridad nacional. Trabajos 2023. Catálogo de publicaciones de la Administración General del Estado. Madrid. Noviembre 2023. Capítulo 1, página 16. Disponible en: https://es.scribd.com/document/694443774/Foro-Campanas-Desinfo-GT-2023-Accesible (20/10/2024).

[1539] Trabajos del Foro contra las campañas de desinformación. *Iniciativas 2024*. Catálogo de publicaciones de la Administración General del Estado (NIPO 143-24-053-2). Noviembre 2024. Disponible en: https://www.dsn.gob.es/sites/default/files/2024-12/MODIFICADO%20ACCESIBLE%20TRABAJOS%20FORO%20CAMPA%C3%91AS%20DE%20DESINFORMACI%C3%93N.%20INICIATIVAS%20%202024.pdf (04/01/2025).

[1540] El libro *Iniciativas 2024* se estructura en seis Capítulos -aunque se completa con dos iniciativas más que no aparecen recopiladas en el libro-: 1) 125 términos sobre desinformación. 2) El papel de los medios de comunicación y las direcciones de comunicación en el combate contra la desinformación. 3) Monetización y economía de la desinformación: análisis del modelo de negocio en las operaciones de desinformación digital. 4) Ingeniería de la desinformación: infraestructura tecnológica de las operaciones

Ediciones Universidad de Salamanca | CC BY-NC-ND

culmina el trabajo de investigación e intercambio de conocimiento del Foro durante el periodo anual 2024 y refleja "el interés común de avanzar hacia una sociedad más resiliente y mejor informada para hacer frente a las campañas de desinformación y la injerencia extranjera"[1541]. A nuestra consideración, merecen destacarse las siguientes reflexiones transversales que propone este documento:

1. La *coordinación público-privada* como base de la respuesta frente a la desinformación, vinculando al sector privado -academia e investigadores, expertos en ciberseguridad, analistas de datos, periodistas, comunicadores de empresas e instituciones- junto con el sector público -fuerzas y cuerpos de seguridad, poder judicial y legislativo-, para adaptar una dimensión multidisciplinar contra la amenaza.
2. La lucha eficaz contra la desinformación requiere una defensa conjunta y decidida de la verdad. Sobre esta base, es preciso *fomentar la resiliencia de la sociedad* a través de su alfabetización mediática, la concienciación sobre su corresponsabilidad y el deber de participar activamente en la respuesta contra la amenaza. El reto de la alfabetización mediática e informacional debe compartirse entre aquellos que, como los medios de comunicación y las plataformas digitales, tienen mayor capacidad para llegar a todos los públicos, junto con las familias y docentes, claves en la educación de los jóvenes, e incluso los verificadores por su alta especialización para la detección de narrativas desinformadoras -muchas de ellas desapercibidas-. Para apoyar esta perspectiva, será esencial disponer de una adecuada política de *comunicación estratégica*, para lo cual se propone la creación de un *cuerpo profesional de técnicos de comunicación del Estado*, integrados en una red amplia de comunicadores del sector privado y de los medios de comunicación[1542].
3. La desinformación tiene un *impacto multidimensional que transciende el ámbito político y social,* afectando incluso a la estabilidad económica y financiera de un país. Asimismo, se advierte del peligro que supone que la desinformación se convierta en un problema estructural, por cuanto conlleva para amplios sectores de la ciudadanía la desviación perceptiva de la realidad y, consecuentemente, la causación de graves daños con consecuencias para el progreso social y económico persistentes en el tiempo[1543].
4. Es cada vez más evidente la *íntima relación entre tecnología y desinformación*. Ésta ha ampliado de manera exponencial su capacidad de influencia gracias a la expansión del uso de Internet, la penetración de las redes sociales y el desarrollo de la IA. Como consecuencia, la producción y difusión de información manipulada es muy barata y extremadamente rentable en comparación a la transmisión de noticias legítimas y veraces. Así, las actuales herramientas, servicios y productos digitales permiten ofuscar la actividad desinformativa o de injerencia, dificultando la atribución del ataque a sus verdaderos autores y, con ello, identificar sus intereses. En este sentido, Rusia, China e Irán son claros

digitales en campañas de manipulación. 5) Campañas de desinformación y promoción del discurso de odio. 6) Escepticismo mediático y de la opinión pública española ante la existencia de campañas de desinformación que afectan a la seguridad nacional.

[1541] IBIDEM, página 4.

[1542] IBIDEM, página 51.

[1543] IBIDEM, página 51.

Ediciones Universidad de Salamanca | CC BY-NC-ND

ejemplos de estrategias de Estado enfocadas al largo plazo, que utilizan todos los recursos a su alcance para generar narrativas manipuladas que favorezcan sus intereses.

En base al objeto de nuestro estudio, merece especial atención el Capítulo 6, titulado *Escepticismo mediático y de la opinión pública española ante la existencia de campañas de desinformación que afectan a la seguridad nacional*, de cuyas conclusiones destacamos las siguientes:

1. El ciudadano medio español está concienciado sobre el riesgo genérico de la desinformación y la injerencia extranjera pero no lo está sobre la amenaza concreta que supone y los efectos que conlleva. Como principales causas se barajan, entre otras: la falta de información sobre la amenaza y la complejidad de su manifestación fáctica; la minimización o ridiculización de este tipo de acciones de injerencia extranjera por una sociedad española focalizada en la amenaza interior desde hace años; la desconexión mediática y el desinterés que conlleva respecto a lo que sucede en el entorno social y político; la falta de conciencia sobre la corresponsabilidad ciudadana en la lucha contra la desinformación; la erosión de la legitimidad de las instituciones responsables de trabajar ese compromiso de la población; y la falta de una visión democrática de la cultura de Seguridad y Defensa en España que, históricamente, se ha vinculado con valores ideológicos y políticos de épocas pasadas.
2. Por otra parte, los medios de comunicación no disponen de un contexto favorable para dar cuenta de las narrativas desinformadoras y la injerencia extranjera por la propia ambigüedad que, para la opinión pública, tiene el concepto de seguridad nacional. A ello hay que sumar la inexistencia de un circuito informativo de calidad al que recurrir para obtener información sobre estos asuntos, y la falta de portavoces oficiales capacitados para comunicar y conectar de manera creíble y cercana con las audiencias hablando de estas materias -seguridad nacional, desinformación, amenaza, corresponsabilidad social, etc.-.

Las recomendaciones que desde el Foro se proponen para contrarrestar estos dos inconvenientes y avanzar hacia una sociedad más resiliente y mejor informada frente a la desinformación y la injerencia extranjera son básicamente dos: fomentar la alfabetización mediática y la concienciación de la ciudadanía y, por otro lado, promover la inclusión de la seguridad nacional en la agenda mediática.

8.1.4. El Plan de Acción por la Democracia

Desde el entendimiento de que las campañas de desinformación entran en el ámbito de la seguridad nacional por su afectación a los principios, valores y procesos democráticos, y desde la convicción de que la protección de éstos constituye el pilar sobre el que construir la estrategia de respuesta contra dicha amenaza, en septiembre de 2024 el Gobierno de la nación presenta el *Plan de Acción por la Democracia*[1544] con el objetivo

[1544] La propuesta del Plan de Acción por la Democracia se lleva a cabo por el Presidente del Gobierno en la sesión plenaria del Congreso de los Diputados, de 17 de julio de 2024, y la presentación oficial tiene lugar el 17 de septiembre de ese mismo año. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

de protegerla e incentivarla ante la erosión que muestra para los ciudadanos, mediante la propuesta de una serie de medidas de mejora de la transparencia y la rendición de cuentas del *Gobierno*, de los *medios de comunicación* y del *poder legislativo*[1545]. Estos tres ejes de actuación vertebran un total de treinta y una medidas de las que solo dos corresponden expresamente al ámbito de la amenaza desinformativa: la aprobación de una *Estrategia Nacional contra las Campañas de Desinformación*, y la creación de una nueva *comisión en el Congreso de los Diputados sobre desinformación*.

Respecto a la primera de ellas, se señalan como instituciones responsables de llevarla a cabo al DSN y al Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. En este sentido, el CSN aprueba el 28 de enero de 2025 el *Acuerdo de elaboración de la Estrategia Nacional contra las Campañas de Desinformación*[1546], para dar cumplimiento a la *línea de acción* número 13 de la ESN 2021, que se refiere específicamente a esta medida[1547]. Por nuestra parte, a falta de la concreción efectiva de esta Estrategia de segundo nivel, consideramos que su redacción:

1. Constituye una iniciativa adecuada para cimentar un marco coherente e integral de defensa del Estado de Derecho y la democracia frente a la desinformación y las injerencias extranjeras, que debe *integrarse junto con las siete estrategias de segundo nivel* ya definidas en el marco de los ámbitos de especial interés del artículo 10 LSN 2015[1548]. A su vez, como no puede ser de otra manera, esta nueva Estrategia Nacional deberá estar en íntima comunión con el *Plan de Acción para la Democracia Europea*[1549], que fija las líneas marcadas por la Comisión para promover elecciones libres y justas, reforzar la libertad y la autorregulación de los medios de comunicación como garantía del derecho de los ciudadanos a la información, y luchar contra la desinformación a través de una respuesta global, estructurada y colectiva frente a la manipulación informativa como piedra angular de una opinión pública plural, formada y libre.
2. Dicha Estrategia Nacional deberá incluir una faceta de *intervención activa*, basada en la colaboración público-privada -con especial atención a los foros especializados, la academia y los verificadores de datos-, la cooperación internacional y europea -a través del intercambio ágil y dinámico de datos-, y la aplicación de la tecnología de la IA al diseño de un sistema de alerta temprana que permita detectar las narrativas desinformadoras en su fase más inicial para, de esta manera, poder comenzar a neutralizarlas antes de que causen daños graves. Por otro lado, una faceta de *intervención pasiva o de resistencia* a la

https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (04/01/2025).

[1545] El Plan de Acción por la Democracia señala específicamente a los partidos políticos cuando se refiere al poder legislativo, con la idea de continuar la senda iniciada en 2020 con el Código de Conducta de las Cortes Generales y, posteriormente, con la reforma del Código Penal en materia de corrupción mediante los delitos de malversación y de enriquecimiento ilícito (LO 14/2022).

[1546] Orden PJC/248/2025, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 28 de enero de 2025, por el que se aprueba el procedimiento para la elaboración de la Estrategia Nacional contra las Campañas de Desinformación. BOE núm. 64, de 15 de marzo de 2025. BOE-A-2025-5151. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151 (17/03/2025).

[1547] Ver Capítulo 4, apartado 4.4.4.

[1548] Ver Capítulo 4, apartado 4.5.8.

[1549] Ver Capítulo 7, apartado 7.2.2.2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

amenaza, a través del fomento de la alfabetización mediática y la sensibilización de la ciudadanía para implicarla en la defensa de sus propios derechos y libertades y, al mismo tiempo, hacerla corresponsable por su rol activo en la transferencia de mensajes y narrativas.

3. Además, será necesario *fortalecer la comunicación* en un doble sentido:
    a. Desde el *punto de vista operativo*, para establecer adecuados canales de comunicación entre los diferentes niveles de las administraciones públicas implicadas, la sociedad civil y los prestadores de servicios en línea.
    b. Desde el *punto de vista estratégico*, apostando por la comunicación como forma de ocupar de manera anticipada y efectiva el espacio informativo que busca conquistar la desinformación y, desde este posicionamiento, trabajar la narrativa del relato para anticiparse a los actores interesados que la propagan en beneficio de sus propios intereses.
4. Finalmente, la Estrategia Nacional contra las Campañas de Desinformación deberá estar particularmente atenta a evitar intromisiones o limitaciones de libertades y ser planteada desde el *profundo respeto a los derechos a la libertad de expresión y de acceso a información veraz*, recogidos en el artículo 20 de la CE, porque "la política de seguridad nacional ha de diseñarse e implementarse también bajo el enfoque de los derechos fundamentales" (SERRA CRISTÓBAL, 2015, pág. 110).

En cuanto a la segunda medida del *Plan de Acción por la Democracia*, relativa a la *creación de una nueva comisión en el Congreso de los Diputados sobre desinformación*, son lógicamente las Cortes Generales las responsables de su ejecución práctica. La constitución de una comisión parlamentaria de carácter permanente para la supervisión de esta amenaza, su análisis, estudio, discusión y valoración de medidas legislativas al respecto, es siempre bien recibida pues las conclusiones de su trabajo contribuirían a desarrollar una de las dimensiones más comprometidas de la lucha contra la desinformación: la perspectiva legal, principalmente en el ámbito constitucional y penal[1550]. En este sentido, la profesora Corredoira y Alfonso, señala la oportunidad de acometer reformas en la legislación española "para garantizar mejor los procesos [*electorales*] y sus instituciones (también las involucradas en el plan de Seguridad Nacional) y por supuesto fortalecer el conjunto de las autoridades electorales ponderando los nuevos desafíos del derecho a la información" (CORREDOIRA Y ALFONSO, 2024, pág. 235). Respecto al debate sobre necesidad de la reforma del Código Penal, sería conveniente el análisis de la posibilidad de incluir nuevos tipos delictivos

[1550] En este sentido, el Informe de la Secretaría Técnica de la Fiscalía General del Estado, de 20 de abril de 2020, titulado *Tratamiento penal de las fake news*, supone una guía para interpretar el posible encaje de las noticias falsas dentro de nuestro ordenamiento penal, el cual no recoge ningún tipo delictivo específico al respecto. Por ello, la propagación de noticias falsas o engañosas, que en modo alguno quedan amparadas por la libertad de expresión por cuanto ésta no tiene un carácter absoluto (STC 235/2007, de 7 de noviembre), han de encuadrarse en otros tipos como los delitos de odio, el descubrimiento y la revelación de secretos, el delito contra la integridad moral, los desórdenes públicos, las injurias y calumnias, los delitos contra la salud pública, estafas e intrusismo, o los delitos contra el mercado y los consumidores. Igualmente, sería de máximo interés avanzar en la definición de un tipo penal que cubriera los supuestos de desinformación con posible afectación a la seguridad nacional, por ejemplo, de narrativas orquestadas en el ámbito de periodos electorales, o con afectación a altas instituciones del Estado.

Ediciones Universidad de Salamanca | CC BY-NC-ND

que contemplaran los comportamientos que difunden públicamente, con manifiesto desprecio por la verdad, contenidos falsos o deliberadamente manipulados que pueden generar odio, hostilidad, violencia o discriminación. También consideramos de carácter urgente la implementación en nuestro ordenamiento de las previsiones de la DSA para la retirada de contenidos ilícitos en las plataformas digitales e Internet, así como la regulación en términos jurídicos de la utilización efectiva de la IA en la lucha contra la desinformación por parte de los poderes públicos, para contrarrestar sus efectos dañinos. Estas aportaciones ayudarían a que el marco legal evolucionase, si no a la par, al menos a no demasiada distancia de la realidad definida por las nuevas formas de criminalidad, el avance de la tecnología y los renovados hábitos sociales de comunicación y consumo de información.

8.2. El marco de respuesta español frente a la desinformación con afectación a la seguridad nacional

Desde el año 2021, en que se publica en España la primera ESN que recoge las campañas de desinformación como un riesgo para la seguridad nacional, dicha amenaza se ha consolidado y ha ganado protagonismo hasta convertirse en una de las más graves para la seguridad del Estado y los sistemas democráticos actuales[1551] aprovechando, precisamente, el compromiso de estos con el riguroso respeto a los derechos fundamentales y los principios constitucionales en la lucha contra la misma, lo cual conlleva que, como ya hemos analizado anteriormente, parte de los fenómenos desinformativos no puedan tener una adecuada respuesta legal en democracia (COTINO HUESO, 2022, pág. 200).

El acceso a la información veraz y de calidad en un contexto de participación abierto, plural y libre de injerencias, donde cualquier ciudadano pueda formarse y expresar libremente sus opiniones y los medios de comunicación no estén atenazados por ningún tipo de censura previa a su trabajo, constituye la base de la democracia. Estos principios son radicalmente opuestos a los que sustentan las autarquías que, por ello, tratan de atacarlos para degradar las instituciones democráticas y su funcionamiento, generando desafección en los ciudadanos a los que ofrecen una visión pesimista de la realidad buscando justificar su modelo de sociedad alejado de la transparencia, la rendición de cuentas y el respeto de los derechos fundamentales.

8.2.1. El ámbito legal de la respuesta

La necesidad de configurar un marco normativo desde el que articular la adecuada cobertura jurídica de la respuesta española a este desafío analizado en los capítulos precedentes, nos obliga a comenzar este apartado recordando[1552] la definición de *seguridad nacional* que ofrece el artículo 3 LSN, en la que queda reflejada su esencia tripartita que, a la sazón, pivota sobre la seguridad individual de las personas, la colectiva del Estado y la global de la comunidad internacional, así como el compromiso de aquel para protegerlas activamente dentro del marco constitucional y legal:

[1551] Iniciativas 2024, Op. Cit., página 4.
[1552] Ver Capítulo 4, apartado 4.3.1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos".

A continuación, el artículo 4 de la LSN establece que la *Política de Seguridad Nacional* es una política pública en la que participan todas las Administraciones Públicas y la sociedad en general, quedando de esta forma patente que la seguridad nacional requiere un compromiso activo público-privado, conjunto y coordinado[1553] bajo la responsabilidad del Gobierno de la nación que, en un escenario de gobernanza y corresponsabilidad compartida, coordina como actor cualificado al resto de *stakeholders* involucrados.

El articulo 9 LSN es crucial para la delimitación tanto del escenario de actuación de la seguridad nacional como de la responsabilidad en las tareas de salvaguarda y protección que requiere. Al primero de los aspectos se refiere al concretar los denominados *componentes fundamentales de la seguridad nacional* que, de acuerdo al artículo 9 LSN, son la Defensa Nacional, la Seguridad Pública y la Acción Exterior. Por lo que respecta a la segunda cuestión, continua este precepto señalando que los Servicios de Inteligencia e Información del Estado, en sus correspondientes ámbitos competenciales, apoyarán permanentemente al SSN para prevenir y detectar los riesgos y amenazas, contribuyendo también a su neutralización. Es aquí donde se define la estructura colaborativa del SSN[1554] en la que tienen cabida el DSN, el Centro Nacional de Inteligencia y los Servicios de Información de la Policía Nacional y de la Guardia Civil, a través de la Secretaría de Estado de Seguridad que los coordina e integra[1555].

Una vez recapitulado el marco conceptual en el que nos desenvolvemos, hay que destacar que la ESN 2021 actualiza el mapa de riesgos a los que atiende la seguridad nacional como política de Estado, incluyendo entre ellos las campañas de desinformación que, al igual que otros de naturaleza híbrida, requiere respuestas colectivas y la integración de capacidades[1556] para hacer frente a sus efectos desestabilizadores y de aliento polarizador. En este sentido advierte que:

> "Las campañas de desinformación tienen clara repercusión en la Seguridad Nacional y deben diferenciarse de otros factores como la información falsa —*fake news*— o información errónea —*misinformation*—. De hecho, las campañas de desinformación no contienen necesariamente noticias falsas, sino que pretenden

[1553] Este compromiso público-privado, conjunto y coordinado se especifica a través de los artículos 6, 7 y 8 referidos respectivamente a la cooperación con las Comunidades Autónomas, a la colaboración privada y a la participación ciudadana en la seguridad nacional.
[1554] Ver Capítulo 4, apartado 4.3.2.
[1555] La Secretaría de Estado de Seguridad, a través del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) integra la información que en estas áreas funcionales aportan los Servicios de Información de la Policía Nacional, la Guardia Civil, la Ertzaintza y los Mossos d'Esquadra que, aunque de naturaleza autonómica, aportan también información e inteligencia para la valoración y respuesta a la amenaza.
[1556] Estrategia de Seguridad Nacional 2021. Op. Cit. Página 19.

Ediciones Universidad de Salamanca | CC BY-NC-ND

> distorsionar la realidad mediante contenido manipulado. […] Por su potencial peligrosidad, cabe señalar las estrategias de desinformación de actores extranjeros, tanto estatales como no estatales, que desarrollan aparatos de propaganda con la intención de polarizar a la sociedad y minar su confianza en las instituciones"[1557].

Dicho lo anterior, para poder determinar el alcance de la amenaza desinformativa y la consideración de su posible afectación a la seguridad nacional debemos atender a un doble parámetro:

1) Primeramente, a la naturaleza de los sujetos y bienes afectados, para concretar la gravedad de los efectos conforme a su incidencia en el normal desarrollo de la actividad de los ciudadanos en un entorno de seguridad, como objetivo de la acción protectora del Estado.
2) En segundo lugar, a la magnitud de las medidas necesariamente adoptadas para la resolución del incidente y la vuelta a la estabilidad que garantice la seguridad de la nación.

Respecto a la primera de las variables, la naturaleza de los sujetos afectados, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas[1558], en su artículo 2 define varios conceptos, como el *servicio esencial*[1559], el *sector estratégico*[1560], las *infraestructuras estratégicas*[1561] y las *infraestructuras críticas*[1562].

A esta consideración sobre la naturaleza del sujeto afectado hay que añadir lo que la Ley de protección de infraestructuras críticas denomina *criterios horizontales de criticidad*[1563], conforme a los cuales se determina la criticidad, la gravedad y las consecuencias del ataque, y que se corresponden con cuatro variables:

1. El *número de personas afectadas* en función del número potencial de víctimas.
2. El *impacto económico* en base a la magnitud de las pérdidas.
3. El *impacto medioambiental* sufrido por la degradación del entorno afectado.
4. El *impacto público y social* conforme a la incidencia en la confianza de la población respecto a la capacidad de las Administraciones Públicas, el

[1557] IBIDEM, página 60.
[1558] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. BOE número 102, de fecha 29/04/2011, referencia BOE-A-2011-7630. Disponible en: https://www.boe.es/eli/es/l/2011/04/28/8/con (21/01/2025).
[1559] El *servicio esencial* se define como "el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas".
[1560] El *sector estratégico* se refiere a "cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país".
[1561] Las *infraestructuras estratégicas* son "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales".
[1562] Las *infraestructuras críticas* son aquellas "infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales".
[1563] Ley 8/2011 de medidas para la protección de las infraestructuras críticas. Op. Cit., artículo 2.h)

Ediciones Universidad de Salamanca | CC BY-NC-ND

> sufrimiento físico y la alteración de la vida cotidiana, incluida también la pérdida y el grave deterioro de servicios de carácter esencial.

En cuanto a la gravedad de los efectos y la magnitud de las medidas requeridas para su resolución, segunda de las variables para determinar el alcance de la amenaza y la evaluación de su quebrantamiento a la seguridad nacional, el artículo 23.2 LSN concreta el contexto de crisis en el que opera la estructura del SSN y sus procedimientos para responder y retornar a la normalidad, definiendo la *situación de interés para la seguridad nacional* como:

> "[…] aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles, en los términos previstos en esta Ley".

Como ya vimos en su momento[1564], este esquema legal es el que permite considerar el verdadero alcance de la *situación de interés para la Seguridad Nacional*, trascendiendo de la mera naturaleza esencial o crítica del *sujeto atacado* para poder valorar otros indicadores como la gravedad de los *efectos de la agresión*, o la dimensión, urgencia y transversalidad de las *medidas adoptadas* para restablecer la situación a los parámetros normales anteriores a la crisis. De esta forma, la evaluación y clasificación de los efectos causados sobre la seguridad nacional se efectúa desde una triple dimensión: el *sujeto pasivo* del ataque, los *efectos causados* por éste y las *medidas adoptadas* para restablecer la situación.

Finalmente, el artículo 23.3 LSN resalta el hecho de que estas *situaciones de interés para la seguridad nacional,* conforme a los principios y valores democráticos de nuestro Estado, deberán afrontarse "con los poderes y medios públicos ordinarios de las distintas Administraciones Públicas y en ningún caso podrá implicar la suspensión[1565] de los derechos fundamentales y libertades públicas de los ciudadanos". Lógicamente, estos órganos y procedimientos de gestión de crisis a los que se refiere la LSN deben ser, también, compatibles con los utilizados por el resto de aliados europeos y miembros de la comunidad internacional, de la que España forma parte.

A partir de estas consideraciones legales podemos comprender la inclusión de la amenaza desinformativa en la esfera de la seguridad nacional al incardinarse en el ámbito de actuación del SSN[1566], en el que se integran los componentes fundamentales

[1564] Ver Capítulo 4, apartado 4.8.

[1565] En este sentido, respecto a la distinción entre suspensión y restricción de derechos fundamentales, en base a la intensidad de la injerencia, véase la Sentencia Tribunal Constitucional 136/2024, de 5 de noviembre. BOE núm. 294, de 06 de diciembre de 2024. Disponible en: https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/31313#complete_resolucion&completa (14/01/2025).

[1566] El artículo 18 LSN define al Sistema de Seguridad Nacional como el "conjunto de órganos, organismos, recursos y procedimientos, integrados en la estructura prevista en el artículo 20 de esta ley, que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones".

Ediciones Universidad de Salamanca | CC BY-NC-ND

de aquella -defensa nacional, seguridad pública y acción exterior- a través de los mecanismos de enlace y coordinación determinados por el CSN.

Teniendo en cuenta que al SSN le corresponde evaluar las amenazas y situaciones de crisis que puedan afectar a la seguridad nacional, recabar la información necesaria para apoyar las decisiones de respuesta y detectar las necesidades para garantizar su disponibilidad y adecuado funcionamiento[1567], es manifiesta su competencia en la gestión de crisis[1568] propiciada por una situación de interés para la seguridad nacional que, conforme al artículo 22.2 LSN, implicará a los distintos organismos integrantes de la estructura del SSN, conforme a sus competencias y de acuerdo a la naturaleza de la amenaza en cuestión[1569], tal y como establece el ya citado artículo 9 LSN.

Es esta la forma en que tiene entrada la actividad operativa del CNI[1570] y de los Servicios de Inteligencia e Información del Estado[1571] como parte del sistema colaborativo del

[1567] El artículo 19 LSN delimita las funciones del Sistema de Seguridad Nacional, señalando que "le corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en esta ley, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema".

[1568] De acuerdo al artículo 22.1 LSN, la gestión de crisis "es el conjunto ordinario de actuaciones dirigidas a detectar y valorar los riesgos y amenazas concretos para la Seguridad Nacional, facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios".

[1569] El artículo 22.2 LSN señala que "la gestión de crisis se desarrollará a través de instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación. Su desarrollo será gradual e implicará a los diferentes órganos que componen la estructura del Sistema de Seguridad Nacional, según sus competencias y de acuerdo con la situación de crisis que se produzca. Asimismo, en la gestión de crisis participarán las autoridades de la Comunidad Autónoma que, en su caso, resulte afectada".

[1570] El artículo 1 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, lo define como "el organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones".
BOE núm. 109, de 07/05/2002, referencia BOE-A-2002-8628. Disponible en: https://www.boe.es/eli/es/l/2002/05/06/11/con (14/01/2025).

[1571] Como ya vimos en el Capítulo 4, apartado 4.3.2., en España, según manifiesta el Ministerio del Interior en su declaración de perfil de país ante el Comité de Expertos sobre Terrorismo "CODEXTER" del Consejo de Europa, en la "Reseña relativa a la capacidad antiterrorista de España" efectuada en la 24ª reunión, celebrada entre el 16 y 17 mayo de 2013 en Estrasburgo, páginas 8 y 9, "en virtud del RD 400/2012, las tareas relacionadas con la información y/o inteligencia y con la lucha antiterrorista, tanto de la Policía Nacional como de la Guardia Civil, las desempeñan sus respectivos Servicios de Información: 1) La Comisaría General de Información (Policía Nacional) se encarga de recabar, recibir, procesar y desarrollar la información de interés para mantener el orden y la seguridad pública dentro del ámbito de actuación de su Dirección General, así como de su aplicación o uso, especialmente en lo referente a la lucha contra el terrorismo. 2) El Servicio de Información (Guardia Civil) se encarga de organizar, dirigir y gestionar la recopilación, la recepción, el tratamiento, el análisis y la distribución de la información de interés para mantener el orden y la seguridad pública dentro del ámbito de actuación de su Dirección General, así como de su aplicación o uso, especialmente en lo referente a la lucha contra el terrorismo. 3) Estos servicios de inteligencia y/o información son, por lo tanto, órganos de gestión que dependen de las Fuerzas y Cuerpos de Seguridad del Estado, legalmente designados para luchar contra el terrorismo, tanto mediante la prevención como la represión. Todo ello sin perjuicio de las funciones asumidas, en esta materia, por el Centro Nacional de Inteligencia, dependiente del Ministerio de la Presidencia".

Ediciones Universidad de Salamanca | CC BY-NC-ND

SSN, en funciones de apoyo permanente a éste proporcionando elementos de juicio, información y cualquier tipo de propuesta necesaria para prevenir y detectar los riesgos y amenazas, así como contribuir a su neutralización[1572].

Respecto a esta actividad operativa en el marco de respuesta a una amenaza desinformativa con afectación a la seguridad nacional, la profesora Carlón Ruiz puntualiza, a colación del *Procedimiento de actuación contra la desinformación* de octubre de 2020, que:

> "En estos términos, la actuación de detección y seguimiento de las «campañas de desinformación» pudiera resultar legítima, en cuanto afecte, en último término, a la seguridad nacional -de forma menos incisiva cuando lo haga a otros bienes públicos especialmente cualificados-, legitimando en tales casos acciones de alcance necesariamente muy limitado en lo que suponga supervisión y, en su caso, intervención activa, en el proceso de comunicación […]. Junto a ello, ahora y siempre, cuando estamos ante el núcleo duro de campañas de desestabilización que puedan atentar contra la seguridad nacional, debe actuarse con los mecanismos adecuados, en los que el sigilo es premisa. Sigilo que no es por sí mismo equivalente a afectación de derechos fundamentales" (CARLÓN RUIZ, 2020).

Resulta relevante la apreciación de la profesora Carlón Ruiz por cuanto abunda en la legitimidad y legalidad de la respuesta del Estado frente a la desinformación lesiva para la seguridad nacional que, a través de las estructuras y procedimientos establecidos para mitigarla donde *el sigilo es premisa* por la propia naturaleza de los organismos involucrados, puede conllevar la intervención mínima e imprescindible de los procesos de comunicación pero no así la afectación de derechos fundamentales. En este sentido, podemos hacer dos reflexiones:

1. La primera de ella es que la clasificación de *secreto* de las estructuras, actividades, fuentes, procedimientos y herramientas que, en el desempeño de su labor, utilizan los Servicios de Inteligencia e Información del Estado, que a la postre es una medida orientada a evitar que todo ello sea conocido por quienes pudieran utilizar esta información contra los intereses nacionales, no está reñida con su calidad democrática y las exigencias de transparencia legalmente establecidas, que garantizan su credibilidad y reconocimiento institucional (SANSÓ-RUBERT PASCUAL, 2024, pág. 97). No obstante, debemos recordar que el secreto es una excepción constitucional a la que solo ha de recurrirse en caso necesario e inevitable (SERRA CRISTÓBAL, 2015, pág. 88).
2. La segunda es que, en base al principio de confianza en las instituciones democráticas y dado que la seguridad y la libertad son dos conceptos íntimamente unidos, necesarios para que los ciudadanos puedan desarrollar sus proyectos vitales al amparo de un sistema de derechos en cuya cúspide se encuentra la Constitución (GRANDE-MARLASKA, y otros, 2019, pág. 20), la actuación del CNI está sometida a control parlamentario y judicial específico

[1572] Como hemos visto anteriormente, el artículo 9.2 LSN determina que "los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, apoyarán permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización".

Ediciones Universidad de Salamanca | CC BY-NC-ND

previo[1573] y la de las Fuerzas y Cuerpos de Seguridad al control judicial ordinario, de acuerdo a lo exigido por la Constitución Española en su artículo 18[1574].

Podemos de esta forma concluir que la acción del Estado dirigida a su protección y la de la sociedad a la que sirve a través de sus Servicios de Inteligencia e Información debe ir, necesariamente, en pos de una *seguridad democrática*, caracterizada por la garantía de la legalidad de sus procedimientos y objetivos (SANSÓ-RUBERT PASCUAL, 2024, pág. 90). Es decir, la actuación de estas estructuras de seguridad del Estado en el marco del SSN español operan al amparo de las garantías constitucionales de reserva de ley, garantía judicial y los principios de necesidad, temporalidad y proporcionalidad.

8.2.2. La articulación operativa de la respuesta

Gracias al esquema normativo que acabamos de analizar, en los últimos años se han podido llevar a cabo en España operaciones policiales coordinadas desde la Audiencia Nacional, tanto contra ciberataques que han supuesto la exposición de millones de datos de ciudadanos españoles de bases gubernamentales tan críticas como el Punto Neutro Judicial, la Agencia Estatal de Administración Tributaria o la Dirección General de Tráfico[1575], como contra campañas de desinformación con ánimo desestabilizador como la atribuida al actor prorruso NoName 057 en el marco del proceso de elecciones generales españolas de julio de 2023[1576]. En este sentido, la profesora Corredoira y Alfonso señala que:

[1573] De acuerdo a la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, la actividad del CNI está sometida a control parlamentario (artículo 11) y a control judicial previo (artículo 12) conforme a la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. BOE núm. 109, de 7 de mayo de 2002. BOE-A-2002-8627. Disponible en: https://www.boe.es/eli/es/lo/2002/05/06/2 (14/01/2025).

[1574] El artículo 18.2 CE establece que "El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito". Por su parte, el apartado 3 determina que "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

[1575] La Comisaría General de Información de la Policía Nacional detuvo en marzo de 2023 en Madrid a un conocido ciberdelincuente conocido como Alcasec que, a través de la vulneración de credenciales de acceso, fue escalando privilegios en los sistemas informáticos de diferentes instituciones públicas hasta acceder a datos confidenciales y restringidos, entre otros del Punto Neutro Judicial del Consejo General del Poder Judicial. Con los datos exfiltrados desarrolló una plataforma de consulta –Udyat- a través de la que monetizaba el fruto de sus delitos, que ocultaba a través de una compleja estructura de mixers de criptomonedas. Lo relevantes del caso es la clasificación de estos ciberataques, por primera vez en España, como amenaza grave a la Seguridad Nacional por su magnitud, alcance y afectación a millones de datos personales de ciudadanos españoles. Puede verse la repercusión nacional del caso en prensa. Disponible en: https://elpais.com/espana/2023-04-03/detenido-el-joven-hacker-alcasec-en-la-causa-sobre-el-ciberataque-al-poder-judicial.html
https://www.abc.es/espana/alcasec-detenido-hackeo-punto-neutro-judicial-20230403113056-nt.html
https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=15523#
https://www.larazon.es/espana/audiencia-nacional-luz-verde-procesamiento-dos-hackers-que-atacaron-punto-neutro-judicial_202401046596af29cf86730001c74a71.html (12/01/2025).

[1576] Durante el desarrollo de la jornada electoral del 23 de julio de 2023, la Comisaría General de Información de la Policía Nacional y la Unidad Central Operativa de la Guardia Civil dieron respuesta en el marco del dispositivo extraordinario de ciberseguridad establecido al efecto por la Instrucción de la Secretaría de Estado de Seguridad 7/2023 para la vigilancia y protección del adecuado desarrollo del proceso electoral, a un ataque del actor prorruso NoName 057. Éste, operando con su típica estrategia

Ediciones Universidad de Salamanca | CC BY-NC-ND

> "La desinformación no ha sido el único problema desestabilizador en distintos períodos electorales; también lo son las interferencias extranjeras, la financiación de terceros en campañas electorales españolas, o los *hackeos* a redes estratégicas, etc., fenómenos ante los que la JEC y las juntas provinciales responden con los medios que tienen, destacando sin duda el apoyo de las Fuerzas y Cuerpos de seguridad" (CORREDOIRA Y ALFONSO, 2024, pág. 218)

Del mismo modo, esta misma base normativa es la que sustenta la investigación policial, coordinada desde un Juzgado de Instrucción de Madrid, que ha permitido la vinculación entre la difusión de publicaciones en una plataforma digital con los delitos de incitación a cometer desórdenes públicos, o llevar a cabo acciones coordinadas que pudieran ser calificadas como atentado, resistencia o desobediencia a la autoridad en el ejercicio de sus funciones[1577].

Una vez explicado a lo largo de los capítulos anteriores que el ciberespacio ocupa hoy día un lugar preferente como entorno proclive para la amenaza híbrida y desinformadora, por su naturaleza digital y dimensión global, donde la anonimización de las acciones y la consiguiente dificultad de atribución de delitos es un axioma constante, debemos convenir ahora que la cibercriminalidad no se guía únicamente por intereses económicos sino que busca objetivos distintos a través de una multiplicidad de formas de actuación que la Estrategia Nacional de Ciberseguridad de 2019 define

---

mixta de ciberataques amplificados por narrativas desinformadoras, consiguió enviar a la comunidad rusa española, a través de chats privados de Telegram, un mensaje de advertencia sobre un posible ataque terrorista de ETA a varios colegios electorales, buscando su no participación en los comicios. Al mismo tiempo, NoName 057 consiguió levantar una página espejo de la página web oficial del Ministerio del Interior y echar abajo la real, en la que se publican los datos oficiales del escrutinio electoral, con el doble objetivo de desprestigiar a la institución y generar dudas sobre la transparencia del proceso ante la opinión pública. La mitigación del ataque y la atribución de la autoría se llevaron a cabo en el ámbito de una investigación coordinada judicialmente por la Audiencia Nacional y la Fiscalía. En cuanto a la Instrucción de la Secretaría de Estado de Seguridad 7/2023, puede consultarse la página web. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/paginas/2023/170723-dispositivo-seguridad-elecciones-23j.aspx
Respecto al incidente desinformador de NoName 057 en las elecciones generales españolas de julio de 2023, puede consultarse la referencia en el compendio de ciberseguridad aplicado a las elecciones, de la Comisión Europea, titulado Compendium on Elections Cybersecurity and Resilience 2024. Disponible en: https://digital-strategy.ec.europa.eu/en/news/new-cybersecurity-compendium-how-protect-integrity-elections-published (11/01/2025).

[1577] El delito de incitación a desórdenes públicos se introdujo en el artículo 559 CP por la LO 1/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal. En la misma reforma se introdujeron los delitos de atentado contra la autoridad, sus agentes y los funcionarios públicos, y de la resistencia y desobediencia, en los artículos del 550 al 556 CP. Nuevamente, la Comisaría General de Información de la Policía Nacional llevó a cabo una investigación, coordinada desde el Juzgado de Instrucción número 13 de Madrid, en la que se demostraba que las publicaciones en el canal de Telegram de Luis "Alvise" Pérez, en el marco de las protestas de noviembre de 2023 contra la amnistía para los responsables del proceso independentista catalán, incitaban a cometer desórdenes públicos, atentar contra los agentes de las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones e, incluso, emplear sustancias nocivas contra la salud de las personas, a partir de las narrativas desinformadoras que se divulgaban desde dicha plataforma, abierta al público y con una gran capacidad de difusión en atención al elevado número de seguidores y visualizaciones que tenía. Puede consultarse el seguimiento en prensa de esta investigación. Disponible en: https://www.elmundo.es/espana/2025/01/11/6782572d21efa0673a8b457c.html (11/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

como fines maliciosos del ciberespacio, en torno a cuatro grandes tipos de tipologías delictivas:

1. El *ciberespionaje*, donde prima una motivación geopolítica del actor estatal o paraestatal, el cual emplea todas las capacidades y recursos a su alcance para conseguir penetrar en las estructuras del agredido y adquirir un elevado nivel de persistencia, con la finalidad de prolongar en el tiempo su actividad de manera inadvertida.
2. Las *amenazas híbridas*, cuyo objetivo es aprovechar las debilidades sistémicas del objetivo a través de una amplia gama de métodos y herramientas que forman parte de un ataque coordinado con un objetivo estratégico superior. Detrás de estas acciones también se encuentran actores estatales, paraestatales o de naturaleza terrorista o radical.
3. El *cibercrimen*, problema de seguridad ciudadana que cada año adquiere más protagonismo en las estadísticas de criminalidad publicadas por el Ministerio del Interior, y que engloba a un amplio espectro delincuencial que abarca desde el terrorismo y los radicalismos ideológicos hasta el ciberdelito estrictamente vinculado a la motivación económica del actor.
4. El *hacktivismo* que, desde una motivación ideológica, busca el impacto mediático o social de sus ciberataques para reivindicar una determinada postura frente a una temática o realidad concreta.

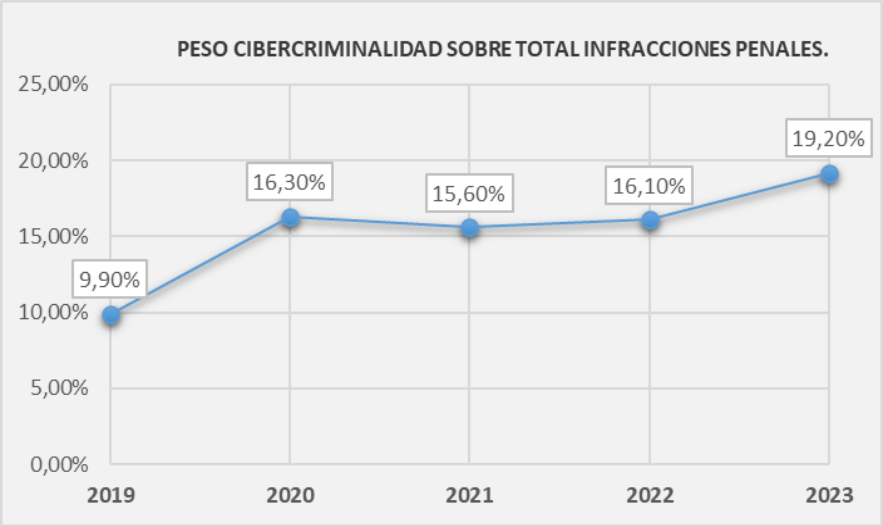


Gráfico 8.2.
Porcentaje que representa la cibercriminalidad sobre el total de infracciones penales
Fuente: Sistema Estadístico de Criminalidad (SEC) en España

Es decir, de las ciberamenazas recogidas en la Estrategia Nacional de Ciberseguridad, tres de ellas comparten una motivación distinta a la económica, salvo el cibercrimen que, paradójicamente, es el índice delincuencial que más crece en las estadísticas de criminalidad anuales[1578], tal y como recoge la tabla comparativa del gráfico 8.2.

[1578] En cuanto a los datos disponibles de 2024, continua la tendencia al alza pero a un ritmo decreciente. Este ritmo decreciente es particularmente claro en el caso de las estafas que, hasta el mes de marzo,

Ediciones Universidad de Salamanca | CC BY-NC-ND

Así, el hecho de que la motivación económica sea la principal no excluye que existan otras posibles motivaciones de la ciberamenaza, tales como:

1. La difusión en redes y chats públicos de fines activistas -negacionismo, ideologías de extrema izquierda o derecha, ecologismo radical, etc.- para movilizar a la ciudadanía en defensa de una particular interpretación política, social, económica o filosófica frente a una cuestión concreta, como por ejemplo la efectividad y pertinencia de la vacunación poblacional frente al COVID-19, o la postulación de teorías conspirativas que abogan por la existencia de una élite en la clandestinidad que dirige los gobiernos del mundo y controla su población mediante, entre otras, la Agenda 2030[1579].
2. La influencia a través de narrativas de manipulación difundidas en la red para conseguir resultados propicios para los intereses de determinados grupos de presión -políticos, económicos, de poder- y tratar de cambiar políticas de Estado vinculadas a decisiones estratégicas en el ámbito de la energía, los transportes, las infraestructuras críticas o las alianzas comerciales, entre otras.
3. Entre Estados y sus actores, la búsqueda de información sobre un adversario a través de *canales no oficiales* para obtener una ventaja competitiva o de posicionamiento geopolítico, como es el caso del enfrentamiento entre China y EE.UU. por los casos de operaciones de espionaje industrial para adquirir *know how* tecnológico con el que, por ejemplo, Pekín ha sido capaz de diseñar aviones cazabombarderos de 5ª generación, como el J20, sin haber llegado a desarrollar ningún modelo de la 4ª generación[1580].
4. El uso del ciberespacio como un entorno de confrontación más entre Estados, en el que se llevan a cabo acciones de injerencia para vulnerar la seguridad del

---

crecen un 14,3% con respecto a 2023, y terminan en un crecimiento de solo el 0,9% en el acumulado hasta octubre con respecto al mismo periodo del año anterior. Todo parece indicar que, si se mantiene esta tendencia de los tres primeros trimestres, como parece ocurrir, es previsible que en el total del 2024 observemos una ligera disminución porcentual en el número de estafas en el ciberespacio por primera vez desde 2015, y posiblemente también en el total de ciberdelitos. Datos disponibles en la página del Ministerio del Interior de estadísticas de cibercriminalidad. Disponible en: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/balances.html (11/01/2025).

[1579] En España dos de los más activos partidarios de las teorías conspirativas son Rafael Palacios López, "Rafapal", y Miguel Celades. Ambos utilizan mayormente Telegram para la difusión de sus narrativas desinformativas de carácter conspirativo que, mediante explicaciones sencillas, tratan de explicar procesos complejos, como por ejemplo las estelas de condensación producidas por la interacción de los gases de combustión que expulsan los aviones en la atmósfera y que sustentan la teoría de los *chemtrails*, según la cual los Gobiernos y otras organizaciones secretas están rociando sustancias peligrosas a través de las estelas que dejan los aviones para modificar el clima a nivel global, controlar a la población mundial y causar enfermedades. Amplia repercusión en prensa. Disponible en: https://elpais.com/ciencia/2023-02-22/terraplanismo-chemtrails-y-negacionistas-de-la-pandemia-unas-jornadas-de-la-universidad-de-cordoba-dan-voz-a-los-censurados.html
https://www.newtral.es/teoria-conspiracion-chemtrails/20230509/
https://www.elconfidencial.com/espana/2023-02-03/rafapa-jefe-conspiracion-espana-clones_3569156/ (11/01/2025).

[1580] Sobre la polémica de los componentes y diseños similares compartidos por los cazabombarderos chino J20 y estadounidense F35. Amplia repercusión en prensa. Disponible en:
https://galaxiamilitar.es/el-caza-furtivo-j-20-construido-gracias-a-la-tecnologia-estadounidense-robada/
https://www.diariolasamericas.com/economia/china-crea-aviones-combate-tecnologia-robada-eeuu-n5332195 (11/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

adversario o conseguir su desgaste institucional, se instrumentalizan narrativas con fines desestabilizadores[1581], o se llevan a cabo operaciones encubiertas de exfiltración de datos para obtener información sensible con la que atacar al contrario llegado el caso y aumentar su alcance e impacto[1582].

En definitiva, podemos decir que la gravedad de la ciberamenaza se evalúa considerando indicadores que van más allá de la cifra de delitos y que atienden a la naturaleza y el carácter de la amenaza que, como la desinformativa, tiene capacidad para afectar a la seguridad en sus diferentes dimensiones. Por esta razón, como señala Fernández Rodríguez:

> "[…] la manipulación informativa dificulta la construcción de esta situación ideal de seguridad, pero también es un grave problema en otros entendimientos tradicionales de seguridad, como la seguridad nacional o la seguridad ciudadana […]. La desinformación hará difícil esa acción del Estado y las necesarias políticas de seguridad que debe desarrollar y aplicar. Pero, además, la desinformación ligada a las cuestiones de seguridad puede generar por sí misma conflictos y potenciar los enfrentamientos" (FERNÁNDEZ RODRÍGUEZ, 2024, pág. 72).

Continuando con nuestro estudio, tal y como hemos analizado anteriormente, el *Procedimiento de actuación contra la desinformación* reparte la responsabilidad de la respuesta frente a los riesgos de la manipulación informativa entre un amplio elenco de órganos y autoridades, en concreto las siguientes:

1. El Consejo de Seguridad Nacional
2. El Comité de Situación.
3. La Secretaría de Estado de Comunicación.
4. La Comisión Permanente contra la Desinformación.
5. Las Autoridades públicas competentes.
6. El sector privado y la sociedad civil.

A su vez el *Procedimiento* establece cuatro niveles de activación para la detección y respuesta ante las campañas de desinformación con posible impacto en la seguridad nacional:

1. El Nivel 1 se corresponde con la actuación técnica, que implica la detección de la amenaza, la gestión de la alerta temprana, su análisis y la notificación que proceda, así como la investigación del origen y posible motivación de la acción.
2. El Nivel 2 supone el seguimiento y evaluación de la alerta por la Comisión Permanente contra la Desinformación, responsable de la coordinación de las propuestas de actuación y de la decisión de elevarla a la Secretaría de Estado de Comunicación para que valore la realización de una campaña de comunicación pública *ad hoc* para contrarrestar la amenaza desinformativa en cuestión.

[1581] Un ejemplo es la instrumentalización de la inmigración irregular para desestabilizar al Estado contra el que se emplea, a la que se refiere específicamente la Estrategia Nacional de Seguridad Marítima, de marzo de 2024. Amplia repercusión en prensa. Disponible en: https://elpais.com/espana/2024-04-16/tres-informes-de-seguridad-nacional-alertan-sobre-el-posible-uso-de-la-migracion-irregular-contra-espana.html?event_log=oklogin (11/01/2025).

[1582] Ver Capítulo 6, apartado 6.1.2.

Ediciones Universidad de Salamanca | CC BY-NC-ND

3. El Nivel 3 conlleva la adopción de decisiones a nivel político-estratégico por parte de la Secretaría de Estado de Comunicación y el seguimiento de la alerta por el Comité de Situación como mecanismo de gestión de crisis por excelencia del SSN, responsable de centralizar la información que suministren las autoridades y organismos competentes en caso de que la campaña de desinformación tenga una afectación para la seguridad nacional.
4. El Nivel 4 corresponde a la gestión política de la situación de crisis y, como tal, es responsabilidad del Consejo de Seguridad Nacional como órgano asesor del Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del SSN.

Puesto que los niveles 3 y 4 corresponden al ámbito político y estratégico, por lo tanto, condicionados por las líneas definidas por el Gobierno en el marco de las políticas de Estado de seguridad que rijan en cada momento, nos centraremos en el análisis de los niveles 1 y 2 que, con un carácter técnico, se refieren a la respuesta operativa y táctica, respectivamente, ante las campañas desinformativas que se enmarcan dentro de los programas de prevención, concienciación y control que los cuerpos de seguridad y los servicios de inteligencia desempeñan "en la gran mayoría de los Estados, al considerar la desinformación como una amenaza para la seguridad nacional" (SERRA CRISTÓBAL, 2023, pág. 37).

En este sentido, el Nivel 1 de respuesta frente a la amenaza desinformativa se fundamenta en la prevención, detección e investigación de sus manifestaciones, así como en el seguimiento y el análisis de sus posibles consecuencias para los intereses esenciales de la seguridad del Estado, a veces vinculadas con las actividades específicas de inteligencia en el sector de la seguridad nacional. En este procedimiento nacional de actuación contra la manipulación informativa grave, los principales actores involucrados en el marco del SSN son, como ya hemos señalado:

1. El DSN a través de su Unidad de Ciberseguridad y Desinformación[1583], la cual asume como competencias específicas aquellas relacionadas directamente con la vulnerabilidad del ciberespacio y la lucha contra las campañas de desinformación, en concreto:
    a. Ejercer de enlace para garantizar la cooperación transfronteriza con las autoridades competentes de otros Estados miembros de la UE, como por ejemplo con el grupo de cooperación NIS de la Comisión Europea, o con la Red Europea de Organizaciones de Enlace para la Cibercrisis (*EU-CyCLONe*)[1584].
    b. La participación en el *Rapid Alert System* (RAS)[1585] de la UE y en los grupos de trabajo técnicos del Servicio de Acción Exterior para el estudio de

[1583] Ver Capítulo 4, apartado 4.3.3.
[1584] Ver Capítulo 7, apartado 7.2.4. EU-CyCLONe es una red de cooperación entre las autoridades nacionales de los Estados miembros encargadas de la gestión de crisis cibernéticas, en el marco de la NIS2.
[1585] Ver Capítulo 7, apartado 7.2.1.3. Como indicamos, el Sistema de Alerta Rápida de la UE es uno de los pilares del Plan de Acción contra la Desinformación del Consejo Europeo, cuyo objetivo es facilitar el intercambio de información sobre las campañas desinformativas y coordinar la respuesta de los Estados miembros ante ellas.

Ediciones Universidad de Salamanca | CC BY-NC-ND

herramientas destinadas al análisis y la detección de campañas de desinformación.

c. El apoyo y la coordinación de la participación española en foros y grupos de trabajo de nivel político-estratégico conforme a lo establecido por el Consejo Nacional de Ciberseguridad.
d. Coordinación de los Foros de Ciberseguridad y de Desinformación en el ámbito de la seguridad nacional, a través de los cuáles impulsa la colaboración público privada en ambas materias.
e. Coordinación de la participación nacional en los ejercicios de gestión de crisis de ciberseguridad, como el ejercicio *Cyber Europe*[1586] organizado por la ENISA y el ejercicio cibernético *Blue Olex*[1587] de gestión de crisis de seguridad en la UE.
f. En el marco competencial del DSN, el asesoramiento especializado al Presidente del Gobierno respecto a la vertiente técnica, desinformativa o ciberespacial de la amenaza, el impulso del SSN en estas materias, y el apoyo al resto de Unidades del Departamento para la elaboración de productos específicos, como la redacción de las diferentes *Estrategias de segundo nivel* o del *Informe Anual de Seguridad Nacional*,[1588].

2. El CNI, que como servicio de inteligencia nacional es el responsable de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier amenaza que afecte a la independencia e integridad de España, los intereses nacionales o la estabilidad institucional[1589], para lo cual debe llevar a cabo las tareas de prevención, detección y neutralización de las actividades de actores o servicios extranjeros que pongan en riesgo el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la seguridad del Estado o la estabilidad de sus instituciones, entre otras[1590]. Dentro de su estructura merece ser destacada la labor técnica que desempeña el Centro Criptológico Nacional (CCN) como gestor de incidentes de ciberseguridad y gestor del Sistema de Alerta Temprana para su detección y mitigación de impacto. Asimismo, el CCN elabora informes de análisis de ciberamenaza[1591] y

[1586] Los ejercicios de ciberseguridad Cyber Europe comprueban el factor de resiliencia ante posibles ataques a las infraestructuras y servicios esenciales, como por ejemplo el sector sanitario. En este sentido, puede consultarse la página web de ENISA. Disponible en: https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2022-testing-the-resilience-of-the-european-healthcare-sector (12/01/2025).

[1587] Blue Olex consiste en un ejercicio con el que se valora la capacidad y se entrena la respuesta de la comunidad de ciberseguridad de la UE, en el marco de la Red CyCLONe, en caso de una crisis cibernética que afecte a sus Estados miembros, con el objetivo de reforzar la cooperación entre las autoridades nacionales de ciberseguridad, la Comisión Europea y ENISA. Disponible en: https://www.dsn.gob.es/index.php/es/es/actualidad/sala-prensa/ejercicio-blue-olex-2023-gesti%C3%B3n-crisis-ciberseguridad (12/01/2025).

[1588] El Informe Anual de Seguridad Nacional compendia un minucioso estudio de las amenazas para ésta, presenta los resultados de la percepción del riesgo que tiene la sociedad española, ofrece un análisis prospectivo de tendencias a cinco años y da cuenta de los resultados de desarrollo del Plan de Cultura de Seguridad Nacional. Se vienen haciendo desde el año 2014, y están disponibles en la página web oficial del DSN. Disponible en: https://www.dsn.gob.es/publicaciones/informes-anuales (11/01/2025).

[1589] Ley reguladora del Centro Nacional de Inteligencia, Op. Cit., Artículo 1.

[1590] IBIDEM, artículo 4.

[1591] El último informe de este tipo publicado es el de *Ciberamenazas y tendencias* de diciembre de 2024. Disponible en: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html (11/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

guías de buenas prácticas y procedimientos de ciberseguridad aplicados a software específico[1592], además de ofrecer un amplio catálogo de cursos de formación y especialización en estas materias[1593].

3. Las Unidades especializadas en ciberamenaza de las Fuerzas y Cuerpos de Seguridad, entre cuyas funciones se encuentran las de:
    a. Monitorización y vigilancia para la detección y recopilación de todo tipo de datos e información de interés sobre los agentes de la amenaza cuyas actuaciones en el ciberespacio pudieran suponer un riesgo para la seguridad nacional. Dentro de esta labor, se encuentra la monitorización para detectar las narrativas tendenciosas, sus actores, sus motivaciones y sus posibles objetivos.
    b. El análisis de las TTP (técnicas, tácticas y procedimientos) que utilizan estos actores para poder identificarlos y hacer la correspondiente atribución de acciones en el ciberespacio.
    c. El enriquecimiento de la información disponible para generar inteligencia que, por un lado, sea comunicada a instancias superiores para la adopción de las decisiones que correspondan y, por otro, permita ser explotada operativamente a través de su judicialización, tanto a nivel nacional como internacional, para la persecución de este tipo de delitos, la identificación de sus autores y su puesta a disposición judicial con las pruebas de cargo y evidencias digitales obtenidas.
    d. La participación en foros y grupos de trabajo multidisciplinares para fomentar la colaboración público-privada, tanto de carácter nacional como internacional.
    e. La colaboración institucional para fomentar el intercambio de conocimiento, abrir canales de comunicación y potenciar líneas de investigación conjunta con el ámbito académico -Universidades y *think tanks*- y el entorno profesional -sector periodístico y de verificadores independientes-.
    f. La cooperación con estructuras policiales supranacionales -EUROPOL, INTERPOL- y servicios homólogos internacionales y europeos para la lucha contra la desinformación.

Además de estos órganos e instituciones con competencias específicas, el *Procedimiento de actuación contra la desinformación* determina que podrán ser convocados para mejorar estas capacidades aquellos expertos que se consideren en función de la naturaleza de la amenaza detectada. Asimismo, se contempla la colaboración del sector privado -medios de comunicación, plataformas digitales, asociaciones civiles, etc.-.

En el Nivel 2 de activación de la respuesta frente a la amenaza desinformativa se encuentra la *Comisión Permanente contra la Desinformación*, presidida por la persona que dirija el DSN y coordinada por la Secretaría de Estado de Comunicación como responsable de la comunicación estratégica del Gobierno. Está compuesta por un

[1592] Puede consultarse en la página del CCN. Disponible en: https://www.ccn-cert.cni.es/es/guias?format=html (11/01/2025).

[1593] Puede consultarse la oferta formativa del CCN en su página web. Disponible en: https://angeles.ccn-cert.cni.es/es/oferta-formativa (11/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

representante del Ministerio de Defensa -del CNI-, del Ministerio del Interior -de la Dirección General de Coordinación y Estudios de la SES-, del Ministerio de Asuntos Exteriores, UE y Cooperación -de la Dirección General de Comunicación, Diplomacia Pública y Redes-, y del Ministerio de Asuntos Económicos y Transformación Digital -de la Secretaría de Estado de Transformación Digital e Inteligencia Artificial-, pudiendo además ser convocados en calidad de expertos, en función de los asuntos tratados, otros representantes de la Administración nacional, autonómica o local, y del sector privado.

Su visión es táctica y, conforme a ella, el principal objetivo es asegurar la integración efectiva de las correspondientes acciones de respuesta de los diferentes Ministerios para proponer posibles medidas de mitigación y apoyar el proceso de toma de decisiones a nivel estratégico, donde entra la Secretaría de Estado de Comunicación y el Comité de Situación. Entre sus funciones debemos referirnos a las siguientes:

1. Apoyo a la Secretaría de Estado de Comunicación mediante el análisis y propuesta de iniciativas en el ámbito nacional, europeo e internacional en materia de lucha contra la desinformación, así como mediante el refuerzo de las relaciones de coordinación y cooperación entre los diferentes niveles de la Administración, y el fomento de la colaboración entre el sector público y privado.
2. Emisión de informes de apoyo para la valoración técnica y operativa de la amenaza.
3. Estudio de recursos y necesidades en el ámbito de la lucha contra la desinformación y propuesta de priorización de actuaciones necesarias identificadas.
4. Verificación de la ejecución de actuaciones previstas y estudio de la necesidad de grupos de trabajo de apoyo.
5. Elevación de propuestas y recomendaciones sobre estas materias y sobre la Estrategia Nacional de Lucha contra la Desinformación al CSN.
6. Apoyo de la investigación de la amenaza desinformativa en colaboración con el sector privado y la sociedad civil.

Queda finalmente destacar que este *Procedimiento de actuación contra la desinformación* pone en valor la corresponsabilidad del sector privado y de la sociedad civil en la estrategia de respuesta, dándoles entrada en los diferentes niveles de activación que define. Sin duda, la primera línea de defensa contra la amenaza desinformativa comienza en los últimos destinarios de la misma: los ciudadanos (BADILLO MATOS, et al., 2023, p. 37).

8.3. El desafío pendiente: la proyección de la resiliencia en el contexto de la seguridad nacional

La construcción de una estrategia de respuesta democrática para enfrentar con éxito la amenaza desinformativa que, en definitiva, busca condicionar a la opinión pública mediante la manipulación de la percepción de la realidad, exige no solo disponer del marco normativo y de los adecuados órganos e instituciones con competencias específicas sino, también, atender a la capacidad de resiliencia del Estado a través de sus múltiples dimensiones afectadas, entre las que una principal es la propia sociedad (ÁLVAREZ ROBLES, 2025, pág. 347). Y todo ello habrá de orquestarse en el marco de un

Ediciones Universidad de Salamanca | CC BY-NC-ND

unánime, firme y decidido compromiso con la política de Estado que guía la seguridad nacional.

8.3.1. La incorporación de la resiliencia en las Estrategias de Seguridad españolas

La resiliencia como capacidad de adaptarse frente al ataque de un agente agresor y recuperarse para salir fortalecido[1594] es un concepto al que nos hemos referido en Capítulos anteriores. Así lo hicimos cuando estudiamos la propuesta de *seguridad humana* de las NNUU[1595] que fomenta la resiliencia de las personas para actuar por sí mismas en su propio beneficio. De igual forma, al analizar el *Concepto Estratégico de Madrid* presentado por la OTAN como enfoque robusto, integrado y coherente para aumentar su resiliencia y la de sus aliados frente a las nuevas amenazas en el contexto geopolítico actual, determinado por conflictos como el de Rusia y Ucrania[1596]. Y, lógicamente, al profundizar en la estructura de respuesta que la UE propone, entre otras, frente a la amenaza desinformativa a través del documento titulado *Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas*[1597].

En este sentido, tanto la OTAN como la UE entienden necesaria la estrategia de comunicación que potencie el enfoque de *aproximación integral* tanto de la Administración Pública como de la sociedad, para reforzar su compromiso con la capacidad de resiliencia que, sin duda, es una responsabilidad nacional pero que, también, tiene una dimensión transversal que afecta a los compromisos con los aliados y resto de miembros de la comunidad internacional[1598].

De igual manera, en clave interna, hemos aludido a la resiliencia al estudiar la Ley de Seguridad Nacional de 2015, que se refiere a ella en su artículo 4 al señalar los principios que definen la Política de Seguridad Nacional, como la capacidad de resistencia y recuperación de las infraestructuras y las personas[1599].

No obstante, es la Estrategia Española de Seguridad de 2011 la que primeramente introduce la *capacidad de resistencia y recuperación* en nuestro catálogo de documentos estratégico-políticos, catalogándola como uno de los seis conceptos básicos que pretende impulsar, *para hacer frente a retos, amenazas y desafíos que*, no conocidos hasta el momento, *puedan ir surgiendo*[1600].

[1594] La resiliencia en el marco de la seguridad nacional. Presidencia del Gobierno, marzo 2024. NIPO 143-24-031-8. Página 9. Disponible en: https://www.dsn.gob.es/index.php/node/23443 (17/01/2025).
[1595] Ver Capítulo 1, apartado 1.3.1.
[1596] Ver Capítulo 2, apartado 2.2.5.
[1597] Comunicación Conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo. *Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas*. Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 13.6.2018. JOIN(2018) 16 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0016 (17/01/2025).
[1598] Orden PCM/714/2022, de 23 de julio, por la que se modifica el Comité de Situación. Op. Cit. Página 1.
[1599] Ver Capítulo 4, apartado 4.3.1.
[1600] Ver Capítulo 4, apartado 4.4.1.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En esta misma línea, la Estrategia de Seguridad Nacional de 2013 señala como uno de sus principios informadores la resiliencia, concebida entonces como la *aptitud de los recursos humanos y materiales* para afrontar con flexibilidad y fortaleza las situaciones de crisis y sobreponerse a ellas minimizando y absorbiendo sus consecuencias negativas[1601].

Por su parte, la Estrategia de Seguridad Nacional de 2017 recurre a la resiliencia como uno de sus principios rectores -junto con la unidad de acción, la anticipación y la eficiencia- y, también, como línea de acción de la Seguridad Nacional en cuanto *mecanismo de superación y vuelta a la normalidad*, referida tanto a la sociedad civil como a las infraestructuras críticas[1602].

Finalmente, la Estrategia de Seguridad Nacional de 2021 presenta la resiliencia como una de las claves de garantía de resistencia, transformación y recuperación ante una crisis con afectación a la seguridad nacional, desde un *enfoque integral, con múltiples facetas* que van desde la resiliencia ambiental y ecológica a la ciber resiliencia, pasando por la economía, las cadenas de suministro, las infraestructuras críticas y esenciales, el sistema de gobierno y la sociedad en su conjunto[1603].

8.3.2. El tratamiento de la resiliencia en las estrategias de segundo nivel

También las estrategias de segundo nivel, que atienden a los distintos ámbitos de especial interés que marca la LSN 2015 y dan consistencia a la estructura de respuesta del SSN frente a los desafíos que conllevan, se refieren a la resiliencia y la adaptan e integran en las líneas de actuación específicas que requieren cada una de las amenazas concretas que contemplan.

Así, la Estrategia de Seguridad Energética Nacional de 2015[1604] interpreta la resiliencia como *pieza clave de las infraestructuras TIC* que dan soporte al sector energético, para garantizar la continuidad del suministro de energía, esencial para el normal desarrollo de la vida de los ciudadanos y el adecuado funcionamiento del armazón industrial y económico del país.

La Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023[1605] va un paso más allá y no se queda en la mera consideración de la resiliencia como *principio rector de la política de Seguridad Nacional*, sino que la vincula directamente con las *labores de inteligencia* que, en este sentido, debe complementar su faceta *preventiva* de la amenaza con otra de carácter *reactivo* que permita impulsar la respuesta y, de esta manera, provocar cambios hacia escenarios de recuperación más beneficiosos para la sociedad.

[1601] Ver Capítulo 4, apartado 4.4.2.
[1602] Ver Capítulo 4, apartado 4.4.3.
[1603] Ver Capítulo 4, apartado 4.4.4.
[1604] Ver Capítulo 4, apartado 4.7.2.
[1605] Ver Capítulo 4, apartado 4.7.4.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En la Estrategia de Seguridad Aeroespacial Nacional, de abril de 2019[1606], la resiliencia es considerada una *característica fundamental de los sistemas e infraestructuras críticas aeroespaciales* en cuanto elemento capacitador del resto de ámbitos de actividad interna que, a su vez, condiciona la coordinación del sector en su dimensión internacional.

En igual sentido, la Estrategia Nacional de Ciberseguridad del mismo año 2019[1607], también entiende la resiliencia como una *característica fundamental de los sistemas de información, redes de comunicaciones e infraestructuras críticas* que conforman la base de la actividad de los servicios esenciales del país y, por ello, deben ser especialmente resistentes y capaces para recuperarse de un ciberataque asegurando la continuidad de sus protocolos y su operativa de funcionamiento.

Por su parte, la Estrategia Nacional Contra el Terrorismo 2023[1608] señala a la resiliencia como *una de las fortalezas de la sociedad española* que, a lo largo de su historia reciente, ha sabido sobreponerse al terrorismo y sus devastadores efectos desde el respeto a los valores democráticos y el orden constitucional, la defensa de la vida de las personas y sus derechos y libertades.

En la Estrategia Nacional de Seguridad Marítima, de mayo de 2024[1609], la resiliencia se considera como elemento clave referido a la *seguridad de puertos, infraestructuras e instalaciones marítimas* por su fuerte vinculación con el complejo entorno socioeconómico mundial, altamente dependiente de este medio transversal que sostiene la cadena global de suministros.

Finalmente, para favorecer la respuesta ante las catástrofes y desastres naturales, la Estrategia Nacional de Protección Civil, de diciembre de 2024[1610], se marca como objetivo principal potenciar la resiliencia de la sociedad desde tres planos complementarios:

1. El impulso de la *formación* específica en la materia para los equipos involucrados en el Sistema Nacional de Protección Civil.
2. El fomento de la *cultura de prevención* en la sociedad.
3. Y la *incorporación operativa* al sistema de respuesta ante catástrofes de todos aquellos actores involucrados en la ejecución de las medidas de protección civil y la garantía de la seguridad pública.

De esta manera, a través del análisis de las estrategias de segundo nivel que complementan y desarrollan la Estrategia de Seguridad Nacional, podemos decir que la resiliencia es un concepto flexible que se adapta a la consideración concreta de la amenaza a la que atiende, desde un enfoque multidimensional pero integral en su objetivo final: la pronta y decidida recuperación de la sociedad y del Estado en su

[1606] Ver Capítulo 4, apartado 4.7.3.
[1607] Ver Capítulo 4, apartado 4.7.7.
[1608] Ver Capítulo 4, apartado 4.7.6.
[1609] Ver Capítulo 4, apartado 4.7.1.
[1610] Ver Capítulo 4, apartado 4.7.5.

Ediciones Universidad de Salamanca | CC BY-NC-ND

conjunto frente a un ataque con afectación a la seguridad nacional, en cualquiera de sus aspectos.

8.3.3. La resiliencia en el marco de la seguridad nacional

La Orden PCM/714/2022, de 23 de julio, por la que se modifica el Comité de Situación[1611], se justifica a través de la necesidad de reforzar la *resiliencia nacional* que requiere un enfoque de aproximación integral -de la administración y de la sociedad- para garantizar la continuidad de la acción de gobierno y de prestación de los servicios esenciales en caso de gestión de crisis. Con este objetivo, asigna al Comité de Situación las funciones de proponer al Consejo de Seguridad Nacional tanto los instrumentos que favorezcan la mejora de la resiliencia nacional como los objetivos y planes para alcanzarlos. Al mismo tiempo, constituye el Grupo Permanente de Coordinación de la Resiliencia Nacional, dependiente directamente de aquel.

Fruto del ejercicio de estas funciones, el Grupo Permanente de Coordinación de la Resiliencia Nacional publica en marzo de 2024 el documento titulado *La resiliencia en el marco de la seguridad nacional*[1612] que "pretende recopilar y poner en valor todas las actuaciones de la Administración central dirigidas a fortalecer la resiliencia en el ámbito del Sistema de Seguridad Nacional, intentando mantener una perspectiva político-estratégica"[1613]. Este documento deja plena constancia de que España es uno de los primeros Estados del ámbito internacional en integrar en su cuerpo normativo el concepto de resiliencia, tal y como hemos podido comprobar anteriormente, con una configuración multidimensional y flexible que le permite afrontar las distintas caras de la amenaza a la seguridad nacional, siempre cambiante y siempre presta a aprovechar las oportunidades que le brinde el entorno -políticas, estratégicas, tecnológicas, etc.-.

Conforme a estos parámetros, se analizan las medidas de fortalecimiento de la resiliencia frente a los dieciséis riesgos y amenazas que marca la ESN 2021[1614], y otras siete medidas de fortalecimiento de la resiliencia en el marco de la Seguridad Nacional[1615]. De entre todas ellas nos centraremos, de acuerdo al objetivo de nuestra tesis, en las *medidas resilientes vinculadas con las campañas de desinformación*.

[1611] Ver Capítulo 4, apartado 4.3.4.

[1612] La resiliencia en el marco de la seguridad nacional. Catálogo de publicaciones de la Administración General del Estado. NIPO (edición on-line): 143.24.031-8. Marzo 2024. Disponible en: https://www.dsn.gob.es/sites/default/files/documents/Resiliencia%20marco%20SN.pdf (18/01/2025).

[1613] IBIDEM, página 5.

[1614] El mapa de riesgos y amenazas que establece la ESN 2021 en su Capítulo 3º se refiere a: 1) tensión estratégica y regional; 2) terrorismo y radicalización violenta; 3) epidemias y pandemias; 4) amenazas a las Infraestructuras Críticas; 5) emergencias y catástrofes; 6) espionaje e injerencias desde el exterior; 7) campañas de desinformación; 8) vulnerabilidad del ciberespacio; 9) vulnerabilidad del espacio marítimo; 10) vulnerabilidad aeroespacial; 11) inestabilidad económica y financiera: 12) crimen organizado y delincuencia grave; 13) flujos migratorios irregulares; 14) vulnerabilidad energética; 15) proliferación de armas de destrucción masiva; 16) efectos del cambio climático y de la degradación del medio natural.

[1615] Estas siete medidas de fortalecimiento de la resiliencia en el marco de la Seguridad Nacional hacen referencia a: 1) medidas para garantizar el agua y la alimentación; 2) medidas para garantizar el transporte; 3) medidas para garantizar las comunicaciones; 4) medidas para garantizar la continuidad del funcionamiento del Gobierno y de la Administración; 5) medidas para garantizar la protección de la

Ediciones Universidad de Salamanca | CC BY-NC-ND

A este respecto, la ESN 2021[1616] trata por primera vez las *campañas de desinformación* como amenaza que intenta distorsionar la realidad mediante contenido manipulado para polarizar a la sociedad y desgastar a las instituciones. Por ello, tiene clara repercusión en la seguridad nacional buscando generar confusión y socavar la cohesión social o influir en los procesos electorales de las democracias, auténtico objetivo final de su ataque. En íntima conexión con ellas se refiere la ESN 2021 a las injerencias desde el exterior, catalogándolas como *riesgo de elevado componente tecnológico e híbrido* que tratan de alcanzar objetivos de distinta naturaleza que, en conjunto, comparten el interés por la obtención de información sensible, activo estratégico para la seguridad nacional que como tal debe ser protegido.

Frente a estas amenazas se construye un arco resiliente que se apoya en los siguientes elementos:

1. El *Procedimiento de actuación contra la desinformación*[1617] que, como hemos explicado, reserva a la sociedad civil un papel primordial en la lucha contra la desinformación a través del compromiso para su identificación, el freno a su difusión y la promoción de actividades de concienciación sobre la amenaza que representa y la formación que permita evitarla.
2. El *Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional*[1618], máximo exponente de la colaboración público-privada destinada al análisis y estudio de esta amenaza, la propuesta de soluciones integrales frente a ella y la sensibilización de la sociedad, con el objetivo de fortalecer su resiliencia familiarizándose con las distintas herramientas y recursos narrativos utilizados por las campañas de desinformación susceptibles de comprometer la Seguridad Nacional.
3. Los proyectos que, en el marco del *Plan Integral de Cultura de Seguridad Nacional*[1619], fomentan la alfabetización mediática y digital sensibilizando a la sociedad respecto a los requerimientos de la seguridad nacional, los riesgos y amenazas que pueden comprometerla, el esfuerzo que para salvaguardarla hacen los organismos públicos y privados concernidos y, como tarea compartida por todos, la implicación activa y responsable de la ciudadanía en su mantenimiento y defensa, fomentando el pensamiento crítico y el ejercicio responsable de la actividad privada en el ciberespacio, claves sobre las que se construye la resiliencia social frente a la desinformación.
4. La constante labor de análisis, estudio y propuesta de instrumentos normativos y labores técnicas que, a través del *Grupo Permanente de Coordinación de la Resiliencia Nacional,* se lleva a cabo para neutralizar la desinformación y sus efectos sobre la seguridad nacional.

información sensible; 6) medidas para garantizar el empleo de las tecnologías críticas; 7) medidas para garantizar las cadenas de suministro y minimizar las dependencias estratégicas.

[1616] Ver Capítulo 4, apartado 4.4.4.

[1617] Ver apartado 8.1.2.

[1618] Ver apartado 8.1.3.

[1619] Plan Integral de Cultura de Seguridad Nacional. Op. Cit. Artículo 8.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Conforme a lo anterior, la seguridad nacional española tiene un apoyo esencial en el elemento resiliente que aportan no solo las estructuras de Estado sino, también, el ámbito privado y la sociedad civil que, en su conjunto, constituyen la clave de bóveda sobre la que se construye la respuesta frente a la desinformación como una de las principales amenazas para la democracia y sus valores.

8.4. Conclusiones: la estrecha relación entre desinformación y seguridad nacional

Desinformación y seguridad nacional caminan de la mano unidas por las graves consecuencias que aquella puede llegar a producir en la base del sistema institucional que soporta una democracia avanzada como la española. Ataques contra las altas instituciones del Estado o contra los derechos de un gran número de ciudadanos solo pueden entenderse y manejarse desde la seguridad nacional entendida como la triple dimensión de la acción del Estado -individual, colectiva y global- que dispone el artículo 3 de la LSN 2015. Únicamente desde esta perspectiva amplia e integral se puede dar respuesta a una amenaza como la desinformativa que forma parte, en el actual contexto geoestratégico internacional, de una Zona Gris que cada vez ocupa más espacio en las relaciones entre Estados que, por ello, recurren a los conflictos híbridos para articular sus estrategias defensivas y ofensivas.

España viene identificando la desinformación como riesgo asociado a la seguridad desde 2017, ofreciendo una respuesta legal y operativa enmarcada en la estrategia definida por la UE a través del *Plan de Acción contra la Desinformación,* donde deben entenderse iniciativas españolas como la creación de la *Comisión Permanente contra la Desinformación,* el *Procedimiento de actuación contra la desinformación* y el *Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional*.

No obstante, es la ESN 2021 la que, sin ambages, señala a las campañas de desinformación como una grave amenaza en un contexto de crisis multidimensional y global en el que, a través de diferentes mecanismos de conexión, pueden verse afectados distintos ámbitos de la seguridad nacional y, por ende, de la seguridad humana en un Estado social y democrático de Derecho. Por ello, el *Plan de Acción por la Democracia* de septiembre de 2024 y, meses después, en enero de 2025, el *Acuerdo del CSN para la elaboración de la Estrategia Nacional de lucha contra las campañas de desinformación*, suponen el inicio de la materialización práctica de la propuesta presentada en la *línea de acción* número 13 de la ESN 2021, referida específicamente a esta medida.

Sin embargo, el esfuerzo por construir un marco legal de respuesta a la desinformación con afectación a la seguridad nacional no parece ser plenamente correspondido por la población española que, paradójicamente, relaciona estas cuestiones con valores anquilosados que no llegan a *calar* en las generaciones más jóvenes y que alimentan debates políticos y sociales que apuntan hacia supuestos *trabajos en la sombra* limitadores de derechos fundamentales por parte de estructuras del Estado que, precisamente, tienen como objetivo principal la defensa del marco constitucional y los principios y valores democráticos afectados por las narrativas desinformadoras. Como

Ediciones Universidad de Salamanca | CC BY-NC-ND

consecuencia, los ciudadanos entienden que su seguridad es asunto del Estado, considerando que él solo encarna el rol de sujeto pasivo, incluso de víctima, a quien no le compete su defensa. Esta falta de *conciencia de corresponsabilidad* va necesariamente unida a la falta de sensibilización ante amenazas como la desinformativa que, o bien, no se valoran como creíbles o, directamente, se desconocen.

La lucha contra la desinformación no puede afrontarse en democracia desde la censura previa y la suspensión de derechos fundamentales. Esos valores y principios que vertebran nuestra moderna vida en sociedad han sido forjados lentamente, desde finales del siglo XVIII cuando, en documentos como la *Declaración de Derechos de Virginia,* los ciudadanos consensuaron la igualdad natural de todos los hombres y el derecho irrenunciable a la vida, a la libertad, a la propiedad y a la búsqueda de la felicidad y la seguridad, encargando al órgano de gobierno la tarea de procurar el beneficio común, la protección y la seguridad del pueblo. Este modelo de organización social ha costado mucho ganarlo y no podemos perderlo. Por ello, no debemos dar por supuesta la buena salud de la democracia, que no se mantiene sola. Nos corresponde a todos los ciudadanos velar por ella día a día asumiendo el compromiso de su defensa, representado la resiliencia una de las claves de esta defensa.

Y por esta razón se muestra esencial la labor de comunicación estratégica por parte del Estado, para seguir apostando por la alfabetización y la cultura de seguridad, pero no solo dirigida a los más jóvenes, sino también hacia los adultos -con más sesgos-, para darles instrumentos y capacidades que les permitan distinguir la verdad de la mentira, identificar las narrativas falsas o manipuladas y, sobre todo, valorar la información de calidad. La sociedad en su conjunto debe apostar por el pensamiento crítico que recurre a múltiples fuentes de información para, finalmente, adoptar una postura fundamentada que le permita tomar decisiones coherentes a través de las que ejercer sus derechos en democracia. Como dice el lema de la ESN 2021, *la seguridad nacional es un proyecto compartido.*

Ediciones Universidad de Salamanca | CC BY-NC-ND

CONCLUSIONES FINALES

1. La evolución de los conceptos de soberanía y seguridad

El concepto de *soberanía* de la época moderna vinculado al territorio y el monopolio del uso de la fuerza se ha transformado, obligado por la aparición en el siglo XXI de nuevos escenarios de actividad humana, como el espacio ultraterrestre, el ciberespacio o el ámbito cognitivo, que conllevan formas de relacionarse que trascienden ampliamente la dimensión física para dar relevancia a la intangible, en la que predominan las ideologías, los valores y las narrativas de opinión que condicionan el comportamiento humano. Conforme a ello, las fronteras territoriales y la distinción de su vertiente interna y externa quedan no ya superadas sino, directamente, anuladas en este nuevo entorno multidominio en el que se desempeñan tanto las relaciones internacionales como las personales.

El ciberespacio, ámbito de interacción común, global y digital caracterizado por la facilidad de acceso y la anonimidad de las acciones que en él se desarrollan, cuestiona el alcance del principio de soberanía en su entorno, lo que ha llevado a considerar erróneamente que el Estado no puede ejercer en él su autoridad y que el *quinto dominio* es independiente. Ciertamente no es así. A partir de esta premisa podemos referirnos a la *soberanía digital* como la capacidad de un Estado para ejercer el control sobre su propio espacio digital, lo cual supone una multiplicidad de aspectos políticos y sociales, entre otros, que se interconectan a través de un orden de relaciones sustentadas por dos de los principales atributos de la soberanía: el reconocimiento de autoridad –local, estatal, supranacional, internacional- y el funcionamiento de mecanismos de control –normativa, políticas públicas, sistema regulado de sanciones-.

Conforme a ello, los Estados despliegan su potestad soberana sobre las infraestructuras de soporte localizadas en su territorio, así como sobre las personas y las actividades a ellas asociadas. De esta manera, la suprema autoridad de cada Estado en su territorio incluye las capas física, lógica y social del ciberespacio, por lo cual el quinto dominio queda englobado en el principio de soberanía, tanto en su dimensión interna como externa, e igualmente sujeta al Derecho Internacional respecto a las violaciones de dicha soberanía por ciberoperaciones, la práctica de acciones de ciberespionaje u operaciones de influencia a través de la difusión de propaganda, entre otras.

Respecto al concepto de *seguridad*, la visión integral de la *seguridad humana* que lidera Naciones Unidas desde el año 1994 y que, por su propia concepción, afecta a la dimensión estatocéntrica de la seguridad westfaliana, lejos de suponer una amenaza a la soberanía del Estado lo que consigue es, precisamente, complementarla para que se adapte a la lógica evolución de los tiempos. En este sentido, la Asamblea General de NNUU señala en su Resolución 66/290 de 2012 que la seguridad humana *se basa en la implicación nacional* y que *no sustituye a la seguridad del Estado*, reconociendo al mismo tiempo el pleno respeto a la soberanía, la integridad territorial y la no injerencia en asuntos que son esencialmente de la jurisdicción interna de los Estados, principios que

Ediciones Universidad de Salamanca | CC BY-NC-ND

son replicados exactamente en el Manual de Seguridad Humana de NNUU de enero de 2016.

No obstante, a la sombra de fenómenos propios del siglo XXI como la globalización, la transformación digital o la entrada en los ámbitos de influencia internacionales de grandes empresas privadas con capacidades económicas que superan las de algunos Estados, *el concepto de seguridad adquiere una naturaleza polifacética* que abarca *realidades diversas* como la economía, la salud, la tecnología o el ejercicio de los derechos humanos y las libertades fundamentales *en un nuevo entorno, el ciberespacio*, interconectadas a través de la relación entre poderes de distinto nivel, públicos y privados, que como fuerzas contrapuestas se equilibran. Surge de esta manera la ciberseguridad, con un marcado componente tecnológico-digital, como nueva dimensión de la seguridad no solo de los Estados sino, también, de las personas.

Así, la *ciberseguridad* es hoy día un necesario requisito en todas las esferas de actividad, públicas y privadas que, en el marco de las democracias actuales, se presenta como una de las *principales claves de legitimación de la soberanía del Estado*, responsable de dar respuesta adaptada a la naturaleza cambiante de los desafíos y de proteger los derechos y libertades de los ciudadanos en cualquier ámbito de su realidad, tanto física como digital. Por ello, tanto la *soberanía* como la *seguridad*, obligadas por el nuevo entorno global y tecnológico que determina la evolución de los riesgos y amenazas, *deben flexibilizarse para mantenerse activas como garantes del bienestar ciudadano, de su protección y de sus garantías de desarrollo.*

2. La perspectiva multidimensional de la seguridad a través de las Naciones Unidas y la Organización del Tratado del Atlántico Norte

En el actual y complejo contexto internacional las políticas de seguridad de los Estados se construyen desde un *enfoque amplio y colaborativo* que tiene su referencia en cuatro puntos cardinales: 1) la relación entre *seguridad y desarrollo*; 2) la toma en consideración de los planteamientos de los *actores no estatales*; 3) los *nuevos espacios de relación* multinivel y multidimensionales; 4) y los *riesgos y amenazas emergentes* que surgen en este contexto tan abierto.

Como consecuencia, *la seguridad trasciende al Estado-nación* y ya no se entiende de manera individual y aislada, adquiriendo una *perspectiva internacional* que exige respuestas coordinadas, cooperativas y contextualizadas para aportar soluciones holísticas a los nuevos desafíos que debe atender. Ello obliga a apostar por el Derecho Internacional como clave de entendimiento y, a la larga, de subsistencia en una cada vez más subvertida escena mundial, donde estructuras como Naciones Unidas (NNUU) o la Organización del Tratado del Atlántico Norte (OTAN) están obligadas, por un lado, a dirigir los esfuerzos comunes de sus miembros y aliados y, por otro, a constituir opciones reales de acercamiento entre los opuestos. Además, para asegurar su misión, deben hacerlo en permanente estado de adaptación al cambio, cuestión que con mayor o menor nivel de éxito vienen realizando desde el final de la Segunda Guerra Mundial, momento en el que ambas nacieron para complementar el equilibrio bipolar sustentado en el terror nuclear que, con la desaparición de la URSS, devino en un pretendido Nuevo

Ediciones Universidad de Salamanca | CC BY-NC-ND

Orden Mundial en el que los EE.UU. ejercían de árbitro único en el tablero de juego. Sin embargo, el siglo SXXI trae consigo un *contexto internacional multipolar y evolucionado* en el que distintos competidores sistémicos luchan por obtener ventaja y que, por ello, hace más evidente si cabe la *necesidad de encontrar puntos de encuentro* entre ellos.

Respecto a NNUU, siendo cierto que constituye el acuerdo internacional más relevante de la historia por su compromiso con la paz, su dimensión universal y el alcance de sus pronunciamientos en aquellas materias sobre las que se manifiesta, debemos sin embargo concluir que presenta una doble cara, con luces y sombras.

Comenzando por estas últimas, una de sus principales debilidades radica en el anacrónico *derecho al veto* de sus miembros permanentes que, cada vez que lo emplean, centrados en la lucha por la hegemonía y la prevalencia de sus intereses, contribuyen a resaltar su *incapacidad* para llevar a cabo el verdadero propósito para el que se constituyeron como Consejo de Seguridad: *mantener la paz y la seguridad mundiales mediante la aplicación de medidas colectivas consensuadas por sus integrantes, de acuerdo con los principios de la justicia y del Derecho Internacional.* Otras sombras que se proyectan sobre NNUU son los propios *actos de agresión entre Estados* y la permanente *conculcación del Derecho Internacional Humanitario* que, mayormente, acompaña a aquellos. Igualmente, a tenor de la forma de proceder de algunos países, la *falta de cumplimiento de los dictámenes de la Corte Penal Internacional* y la consiguiente quiebra del principio de legalidad en las relaciones entre Estados. Y, por último, la *servidumbre estructural y la carencia de presupuesto independiente* que marca la dependencia de NNUU de las aportaciones de sus miembros.

Por lo que respecta a sus luces, podemos destacar la profunda repercusión de la perspectiva integral del concepto de la *seguridad humana*, íntimamente ligada a la triple esfera de la *libertad para vivir sin temor, sin miseria y con dignidad*, que propugna NNUU desde el año 1994. Vinculada a ella, la consideración de la *gestión anticipativa* como clave para prevenir la amenaza antes de que llegue a producirse el daño en cualquier ámbito de la *seguridad multidimensional y multinivel* que, desde 2015, se proyecta en la Agenda 2030 y en los Objetivos de Desarrollo Sostenible (ODS). Con ello NNUU otorga carta de naturaleza a una nueva manera de entender la seguridad, integral y holística, que no puede perfeccionarse sino desde la acción conjunta de los Estados y desde el enfoque de la persona como sujeto principal de la misma.

Finalmente, como prueba de la capacidad de adaptación de NNUU a la transformación digital y su *compromiso con la aplicabilidad del Derecho Internacional en el ciberepacio*, debemos referirnos a los esfuerzos que actualmente se llevan a cabo por la organización para construir el consenso necesario entre todos los actores intervinientes -Estados, organizaciones supranacionales e internacionales, ciudadanía, sector empresarial, academia, comunidad técnica-, con el objetivo de promover la paz, la seguridad, la cooperación y la confianza internacionales en el quinto dominio, buscando soluciones que puedan llevar al entendimiento entre las diferentes maneras de entender el ciberespacio y el amplio espectro de actividades que en él se dan cita.

Ediciones Universidad de Salamanca | CC BY-NC-ND

En cuanto a la OTAN, actualmente la estructura de cooperación militar intergubernamental más exitosa de la historia, su naturaleza original definida tras la Segunda Guerra Mundial *para mantener a los rusos fuera, a los americanos dentro y a los alemanes debajo*, debe también adaptarse al escenario geopolítico actual y los nuevos roles en él desempeñados por sus actores, puesto que ninguna organización o estructura internacional puede mantenerse ajena al permanentemente cambiante contexto en el que participa, so pena de ir quedando relegada hasta, definitivamente, acabar desapareciendo por su misma anacronía e ineficiencia. Es por ello que la Alianza Atlántica, empujada por el final de la Guerra Fría, se viera obligada a reinventarse dejando de focalizar su acción en la *defensa colectiva* frente a la extinta URSS para convertirse en una comunidad de *seguridad compartida,* a través de la cual afrontar una nueva amenaza asimétrica y multidimensional que exige respuestas complejas, donde la diplomacia y las estrategias híbridas juegan un papel prominente junto al clásico efecto disuasorio de la fuerza cinética.

Paradójicamente, la política expansiva de la Alianza de principios del siglo XXI para extender su cobertura de seguridad a todo el continente europeo, integrando bajo su escudo protector a gran parte de los antiguos componentes del Telón de Acero, será pieza clave en el resurgir de Rusia como principal amenaza al orden internacional a partir de la llegada al poder de su líder, Vladimir Putin, haciendo para ello alarde de sus amplias capacidades en el ciberespacio y en el desempeño de las modernas *operaciones híbridas*.

Ante esta situación, la Cumbre de Madrid de 2022 se ve obligada a definir una nueva estrategia de disuasión y defensa de la OTAN basada en una última interpretación de la seguridad, la denominada *seguridad cooperativa*, que desde un enfoque 360º pretende dotar a los aliados de la capacidad de respuesta ante cualquier amenaza y ante cualquier actor *como quieran, cuando quieran y en el dominio que elijan*. En la actualidad el riesgo se identifica con la asertividad de las políticas globales expansionistas de Rusia y China, el terrorismo internacional que continúa golpeando a las democracias occidentales, el uso del ciberespacio como dominio de confrontación y el cambio climático derivado del uso intensivo de los recursos naturales y el consumo de combustibles fósiles para mantener el desarrollo económico.

Este ideario de alta capacitación operativa en cualquier dominio de enfrentamiento conlleva, *per se*, un compromiso con la estructura de gestión, de soporte técnico y de combate en el ciberespacio, en el que la Alianza considera directamente aplicable el Derecho Internacional vigente para la resolución de las controversias que las relaciones *inter pares* siempre generan. El esfuerzo realizado en este sentido se ampara con la consideración de la amenaza híbrida como un arma más en el elenco de las disponibles para respaldar su capacidad de disuasión y defensa.

De esta manera la OTAN reafirma su posición histórica como elemento de seguridad colaborativa esencial para la Unión, incluso en su ya iniciado camino hacia la *autonomía estratégica*, tal y como se percibe en el Libro Blanco de la Defensa Europea, que específicamente cuenta con aquella para dar solución a sus brechas críticas de capacidad

Ediciones Universidad de Salamanca | CC BY-NC-ND

para la guerra de alta intensidad, donde la escala, el coste y la complejidad de las medidas a adoptar supera las posibilidades de los propios socios europeos.

Finalmente, destacar que este periplo evolutivo ha transitado por distintas fases en la salud de la relación entre los aliados de ambos lados del Atlántico, por cuanto los considerandos de la defensa de EE.UU. y de la UE no siempre han ido en la misma dirección. Avanzado ya el primer cuarto del siglo XXI podemos decir que la relación entre ellos vive un momento de tensa expectación ante la llegada, otra vez, a la Casa Blanca del Presidente republicano Donald Trump, que lanza como carta de presentación su triple postulado: la no entrada de Ucrania en la OTAN, el acuerdo de paz con Rusia al margen de los europeos, y el compromiso de la UE de destinar, al menos, el 5% de su producto interior bruto a gastos de defensa.

3. El replanteamiento de la estrategia de seguridad y los principios europeos en el ciberespacio

Al referimos a la Unión Europea debemos comenzar destacando su exitosa condición, por cuanto se trata de la única estructura organizativa de carácter supranacional que funciona actualmente, en la que sus Estados miembros han cedido parte de su soberanía como medio para alcanzar una serie de objetivos comunes a la vez que comparten unos valores superiores que resultan esenciales para comprenderla: el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad, la igualdad, la democracia y el respeto a los derechos humanos.

Este proyecto de integración europeo ha afrontado retos sin precedentes como crisis económicas a nivel mundial, el abandono de uno de sus miembros, guerras en su territorio, el azote del terrorismo y el constante drama humano de la inmigración que trata de cruzar sus fronteras para alcanzar una vida digna.

Con la firma del Tratado de Maastricht en 1992, la Unión ordena sus competencias en torno a tres pilares: un primer pilar de integración política y económica a través de los Tratados, un segundo pilar relativo a la cooperación en Política Exterior y de Seguridad Común, y un tercer pilar sobre cooperación en el ámbito de la Justicia y los Asuntos de Interior. Será después, con la entrada en vigor del Tratado de Lisboa de 2009, cuando se consiga la personalidad jurídica única de la UE a partir de la cual iniciar una nueva dimensión expansiva hacia el Este que, a fecha de hoy, ha ralentizado su curso para hacer una profunda revisión de los principios y acuerdos constitutivos, adaptar la gestión de las competencias que tiene atribuidas la Unión y reforzar su capacidad de actuación mediante la reforma de los procedimientos de votación.

En cuanto a su política de defensa, es relevante destacar que las iniciativas estrictamente europeas para alcanzar una estructura propia e independiente de la OTAN y de su máximo tutor, los EE.UU., históricamente quedaron anuladas por el conflicto de intereses que generaba ese anhelo de autonomía continental entre los aliados noratlánticos y las propias contradicciones internas de la UE, que no conseguía definir una visión única y compartida sobre los riesgos y amenazas a los que atender, ni

Ediciones Universidad de Salamanca | CC BY-NC-ND

sobre los posibles elementos de disuasión que utilizar ni, tampoco, en cuanto al arbitrio de una respuesta defensiva conjunta.

Es así que la definición y el alcance de una *autonomía estratégica europea* ha sido factor de enfrentamiento interno entre los Estados miembros más que objetivo conjunto e innegociable sobre el que trabajar decididamente, en ocasiones por la dicotomía entre la opción de recuperar espacio frente a EE.UU. y la de medir esos pasos por miedo a desvincularse demasiado pronto de él, en otras por la propia heterogeneidad de los socios europeos que interpretan la defensa, la seguridad y la amenaza de diferentes maneras, y en otras por los movimientos unilaterales de política exterior de los EEMM que, aun siendo legítimos, confrontan abiertamente con la postura oficial de la Unión, resquebrajando su pretendida acción común ante el resto de actores internacionales. Por eso, *la implementación de una estrategia de política exterior y de seguridad común europea continúa siendo, al menos por ahora, una de las más complicadas tareas que debe atender.*

Un paso adelante en este sentido supone la aprobación en marzo de 2022, casi al mismo tiempo en que Rusia invade Ucrania, de la Brújula Estratégica para la Seguridad y la Defensa, apostillada con el lema *Por una Unión Europea que proteja a sus ciudadanos, valores e intereses y contribuya a la paz y la seguridad internacionales*. La principal novedad de este documento, que pretende ser la firme constatación de la legítima ambición europea por convertirse en un proveedor de seguridad capaz y confiable, es el cambio de mentalidad que subyace, determinada por tres elementos característicos: el compromiso de llevarla a la práctica que cada uno de los EEMM asume con su aprobación; el sistema de seguimiento que se formaliza a través de los Informes Anuales de progreso en su aplicación; y el enfoque práctico que la guía a tenor de las tareas asignadas, los medios propuestos y los recursos dedicados para alcanzar los objetivos propuestos.

La Unión ha madurado y en el siglo XXI busca su lugar como jugador geoestratégico relevante. La ambición territorial rusa que le lleva a invadir Ucrania y la segunda presidencia de Donald Trump poniendo en tela de juicio las bases de la principal alianza defensiva de la UE, han funcionado como elementos disruptivos que contribuyen a que adopte *un papel más asertivo en la determinación de sus propias capacidades de defensa*, las cuales pasan por disponer de más armas y estar dispuesta a utilizarlas, por tener la autonomía tecnológica para producirlas y mantenerlas, y por invertir en investigación y desarrollo industrial que pueda aplicarse al campo militar. Esta proactividad es el camino a seguir que marca el Libro Blanco de la Defensa Europea, junto con el Plan ReArm Europe. La unidad y la fuerza junto con la disuasión como garantía de la paz son las guías para recorrer ese camino hacia la capacidad de influencia en el tablero mundial, multipolar y asimétrico en el que, lógicamente, el hecho de jugar exige competir. Factor determinante para la consolidación de esta estrategia será ver el papel que la Unión logre tener en la resolución del conflicto bélico entre Rusia y Ucrania, donde los EE.UU. pretenden obtener rédito como líder mundial ejerciendo su mediación al margen de los europeos que, en el Libro Blanco, ya dejan claro su postura al respecto: el futuro de seguridad y defensa de Ucrania está íntimamente vinculado al de Europa.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Por ello la Unión ha adoptado un nuevo rol, más beligerante y activo, consciente de que la defensa de sus principios democráticos son su principal fortaleza pero que, para ponerlos en valor, el *soft power* no es suficiente. Y esta estrategia aplica tanto en el ámbito físico como en el ciberespacio.

En este sentido, *la UE está decidida a recuperar el control sobre su soberanía digital como pilar fundamental de su pretendida y ansiada autonomía estratégica*. Los graves problemas de abastecimiento de bienes de primera necesidad y recursos sanitarios esenciales durante la pandemia del COVID 19; los fallos en el control y el inadecuado tratamiento de datos de los ciudadanos europeos alojados en servidores fuera del ámbito de la Unión; la constante propagación de narrativas desinformadoras que atacan y desgastan las democracias; las injerencias externas en los procesos electorales o el salto cualitativo que supone la invasión rusa de Ucrania y el inicio de una nueva guerra de aspecto convencional en suelo europeo que, no por casualidad, comienza con acciones ofensivas en el ciberespacio, obligan a la UE a repensar su estrategia de seguridad en el ciberespacio en torno a dos ejes principales: el *alineamiento con el Derecho Internacional*, y la definición de una línea de acción común europea basada en el *diseño de un orden normativo acorde con ella*.

En cuanto al primero de ellos, la Unión considera que su estrategia en el ciberespacio debe avanzar alineada con los principios de la Carta de las NNUU para alcanzar un mundo pacífico, justo y sostenible *dentro del marco del Derecho Internacional* no solo en el ámbito físico sino, también, en el plano digital a través de un ciberespacio global, abierto y seguro, en el que se promueva el comportamiento responsable de los Estados sobre la base del respeto de los derechos humanos fundamentales.

Respecto a la definición de un *marco normativo europeo para el ciberespacio*, la clave es la unidad de acción para tratar de vertebrar la respuesta coordinada y conjunta frente a los nuevos riesgos emergentes a través de diferentes programas, estructuras y herramientas, entre las que merece la pena destacar la *Directiva SRI*, la *Estrategia de Ciberseguridad de la UE para la Década Digital,* el *Plan de Acción sobre las sinergias entre las industrias civil, de la defensa y espacial,* y la *Ley de Cibersolidaridad de la UE,* entre otras.

Sobre estos dos pilares ha construido la Unión su estrategia de ciberdefensa, con el objetivo a medio y largo plazo de recuperar su soberanía digital, para lo cual cuenta con el compromiso de sus veintisiete integrantes que, desde la corresponsabilidad, han advertido que *la ciberamenaza es una preocupación supranacional con efectos a todos los niveles, que requiere de una respuesta multidimensional y cooperativa*.

4. El modelo de seguridad español frente a los desafíos de seguridad tradicionales y emergentes

La *Constitución española contempla el concepto de seguridad desde diferentes puntos de vista* y lo proyecta sobre ámbitos tan dispares como la protección ciudadana, las relaciones de trabajo o la sanidad, que no dejan de ser sino partes del todo que conforma el amplio espacio de la *seguridad de las personas*. En este sentido, podemos

Ediciones Universidad de Salamanca | CC BY-NC-ND

decir que la seguridad española evoluciona al ritmo y en la línea marcada por la comunidad internacional, haciendo suyos conceptos como el de la *seguridad humana* y el más reciente *modelo integral de la seguridad* que sustenta retos mundiales como los ODS, claves en la interpretación de la forma de vida en paz, en libertad y con respeto a los derechos fundamentales que propugna la democracia.

Ello explica que España pueda desarrollar una norma tan avanzada como la *Ley de Seguridad Nacional de 2015*, determinante para la adaptación de su política de seguridad frente a los nuevos desafíos que presenta un panorama internacional globalizado, interdependiente y altamente tecnologizado, en el que entran con fuerza la ciberseguridad y las amenazas híbridas.

Desde esta perspectiva innovadora se define la *esencia tripartita del concepto de seguridad nacional*, integrado por la *seguridad individual* de las personas, la *seguridad colectiva* del Estado y la *seguridad global* de la comunidad internacional. A partir de ella cobran protagonismo novedosos enfoques jurídicos como el que permite la consideración de *amenaza para la seguridad nacional* de aquellos *ciberataques* que, aunque no afecten a un sector estratégico o esencial, tengan por sujeto pasivo a personas físicas o jurídicas determinadas, en atención a la *gravedad de la agresión, la transversalidad de sus efectos, la dimensión o volumen de su perjuicio y la urgencia generada para la reparación del quebrando producido*, variables en las que también tiene cabida el análisis de la *motivación del ataque* como indicador de esa posible afectación a la seguridad nacional.

Partiendo de este planteamiento define la LSN 2015 la estructura del *Sistema de Seguridad Nacional* como el conjunto coherente y ordenado de órganos e instituciones, métodos y procedimientos legales que, desde la colaboración, dan soporte a las acciones de respuesta frente a los retos y amenazas a España. A su vez, se vincula con la *cultura de seguridad nacional* en la convicción de que la sociedad, en su conjunto, es corresponsable de su propia seguridad y de la preservación del modelo de democracia y libertad en la que se desarrolla su vida y su actividad económica. Este *compromiso ciudadano con la autoprotección y la resiliencia* adquiere un carácter prioritario para la defensa nacional por cuanto que la amenaza actual, multidimensional, global y tecnificada, parte de actores de diversa naturaleza y con complejas motivaciones que, para alcanzar sus objetivos estratégicos, aprovechan las oportunidades tanto en el plano físico como en el virtual.

Esta interpretación amplia de la seguridad nacional que hace la LSN 2015 toma como base las consideraciones referidas a la amenaza que presentan las dos primeras Estrategias de Seguridad Nacional españolas. Centrándonos en el ámbito de la ciberamenaza, la primera de ellas, la Estrategia de Seguridad Nacional de 2011, ya recoge una referencia explícita a las amenazas emergentes, entre ellas la proveniente del ciberespacio como *factor de riesgo* por las graves consecuencias que puede tener sobre la prestación de los servicios esenciales y la consiguiente afectación a la seguridad de los ciudadanos. En la misma línea interpretativa, la ESN 2013 cifra como uno de sus objetivos garantizar el uso seguro de las redes y los sistemas de información frente a los ciberataques y otros desafíos como la desinformación que, por su transversalidad,

Ediciones Universidad de Salamanca | CC BY-NC-ND

pueden tener un alto impacto en la seguridad nacional. Por ello se comienza a trabajar en la línea de la *cultura de ciberseguridad*, donde la concienciación de ciudadanos, profesionales y empresas en el uso responsable de la tecnología y los servicios asociados es la pieza clave de la política de prevención.

Será la ESN 2017 la que presente el *modelo integral de gestión de crisis* en el que la respuesta a la ciberamenaza involucra a todos los sectores, públicos y privados, y a la ciudadanía, puesto que el objetivo de un ciberespacio seguro y fiable, como común global, requiere de un compromiso de todos los ciudadanos con el uso responsable de las tecnologías y los servicios ofrecidos en la red, al tiempo que un compromiso con la UE y la comunidad internacional para fomentar la cooperación y el cumplimiento del Derecho Internacional, base legal aplicable en el ciberespacio.

De manera específica, la Estrategia Nacional de Ciberseguridad de 2019 se refiere al *ciberespacio como una nueva dimensión a la que atender para la adecuada defensa de los valores y principios constitucionales y democráticos, así como de los derechos fundamentales de los ciudadanos*, especialmente referidos a la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad. Conforme a ello, *la ciberamenaza se clasifica en cuatro grandes tipologías delictivas* de acuerdo con la naturaleza del actor que la impulsa, su motivación e impacto -ciberespionaje, amenazas híbridas, cibercrimen y hacktivismo-. Merece la pena destacar que una de las claves de la respuesta a la ciberamenaza se cimenta sobre la resiliencia en su doble vertiente, como una característica de los sistemas de información, redes de comunicaciones e infraestructuras críticas que conforman la base de la actividad de los servicios esenciales del país y, por otro lado, de los ciudadanos como corresponsables de su seguridad mediante el uso consecuente de las tecnologías y los servicios ofrecidos en la red.

En último lugar la ESN 2021, actualmente en vigor, nace enmarcada en el contexto de la pandemia del COVID-19 y la eclosión de las narrativas desinformadoras como instrumento para alentar la polarización social, alimentar las teorías conspirativas y atacar la legitimidad de las instituciones democráticas. El principal valor de esta Estrategia es su novedoso enfoque respecto a cuestiones que, o bien, eran afrontadas de diferente manera por las anteriores o, directamente, no las trataban. En este sentido debemos referirnos en primer lugar a su perspectiva de origen, multinivel y diferenciada, dando entrada a las Comunidades y Ciudades Autónomas de Ceuta y Melilla, así como a una amplia variedad de especialistas, públicos y privados, para definir las líneas estratégicas de actuación frente a los diferentes tipos de amenaza. En segundo lugar, el análisis de las amenazas como variables interconectadas, profundamente tecnologizadas y con amplio predominio de las estrategias híbridas, frente a las que se esgrime una visión integral de la seguridad nacional que, al tiempo, se integra en un contexto europeo, mediterráneo y atlántico. La tercera novedad de la ESN 2021 radica en la inclusión de las campañas de desinformación y la injerencia extranjera como riesgos para la seguridad nacional de singular componente híbrido, con alta capacidad de impacto en la ciudadanía y la estructura institucional del Estado democrático, a través de las cuales los actores implicados buscan alcanzar sus objetivos mediante estrategias orientadas a la coerción política y la polarización social. Finalmente, la definición de un

Ediciones Universidad de Salamanca | CC BY-NC-ND

modelo integral de gestión de crisis articulado sobre la base del Sistema de Seguridad Nacional que se asienta en el compromiso de todas las administraciones junto con la sociedad civil, y en la resiliencia como una de sus claves de garantía de resistencia, transformación y recuperación ante un ataque.

Ante esta nueva amenaza que aprovecha el ciberespacio como dominio en el que el dato y la información son elementos de poder e influencia, la ESN 2021 aplica la *soberanía digital* como principio rector de la *política de seguridad nacional* a través de la cuál incorporar su amplia visión de la seguridad a ámbitos tan dispares, pero vinculados entre sí, como la protección de las personas, el desarrollo industrial, la innovación tecnológica, la defensa nacional o, incluso, la salvaguarda del ámbito académico como núcleo del conocimiento y el talento nacional.

Todo este planeamiento estratégico tiene su correspondiente *desarrollo táctico y operacional a través de las normas de segundo nivel* que, de la mano de los *Comités especializados*, logran la capilaridad del sistema para llegar a cada uno de los ámbitos de especial interés referidos a la seguridad marítima, energética, aeroespacial, frente al crimen organizado y el terrorismo, la protección civil, la ciberseguridad y, desde enero de 2025, las campañas de desinformación, todos ellos nuevos horizontes de riesgo.

5. La evolución de las amenazas a la seguridad y su vinculación con el ciberespacio

La amenaza evoluciona conforme lo hace la sociedad a la que afecta. La *guerra*, parte consustancial de la relación entre Estados que, en nuestro caso, contempla el artículo 63.3 CE, se ha ido transformando de la mano de la política, la evolución social y la innovación tecnológica desde un enfoque estatocéntrico clásico, donde representa un medio legítimo de defensa, hasta la actual representación de la *guerra híbrida* como un estilo de confrontación propia del siglo XXI, donde se combinan e integran de manera simultánea todo tipo de procedimientos, medios y tácticas aprovechando los dominios terrestre, marítimo, aéreo, espacial y cibernético, en las tres posibles dimensiones que pueden alcanzar sus efectos: física, virtual y cognitiva. En la guerra híbrida entran en juego las denominadas *operaciones multidominio* para tratar de aprovechar cualquier tipo de ventaja frente al enemigo.

Es en este contexto donde adquieren relevancia el ciberespacio y las acciones ofensivas y defensivas que en él se llevan a cabo, a tenor de lo cual se plantea la cuestión de si, en las guerras actuales, como por ejemplo la de Rusia y Ucrania, la clave que puede determinar la inclinación de la balanza a favor de uno u otro de los contendientes es la capacidad ofensiva en el quinto dominio, en detrimento de las acciones cinéticas convencionales. La contestación a esta pregunta divide a los teóricos de la guerra, entre los que ven la ciberguerra como sustitutiva del clásico enfrentamiento parametrizado por Clausewitz, los que entienden las ciberoperaciones como una herramienta más que complementa a las armas convencionales y, finalmente, los que consideran que las operaciones en el ciberespacio evolucionan de manera autónoma e independiente a las acciones de guerra que se desarrollan en el resto de dominios físicos.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Semejante disyuntiva se presenta al estudiar el terrorismo internacional y la instrumentalización que hace del ciberespacio para sus fines criminales y el proselitismo propagador de su mensaje.

En cualquier caso, el ciberespacio como nuevo escenario de conflicto, es interpretado de distinta forma e integrado de diferente manera en la estrategia geopolítica de los Estados, por lo que es cuestión determinante convenir la manera de aplicar el Derecho Internacional en el quinto dominio. Es esta una labor en la que se ha implicado activamente NNUU con la creación de grupos de trabajo *ad hoc*, y que también ha merecido la atención de expertos internacionales en diferentes proyectos. Los desafíos que comporta interpretar el Derecho Internacional para adaptarlo a la actividad en el ciberespacio son fuente de discusión doctrinal, pues hay que recurrir en no pocas ocasiones a la *adaptación caso por caso de conceptos y principios cruciales* como el de ataque, soberanía, uso de la fuerza, debida diligencia o, incluso, el marco de protección de los derechos humanos para ver cómo, desde el ciberespacio, se relacionan los Estados.

A la vista de los resultados alcanzados hasta el momento podemos convenir que la interpretación del cuerpo normativo internacional existente no parece tarea fácil tal y como confirma, por ejemplo, la aprobación sin votación por parte de la Asamblea General de NNUU, en noviembre de 2024, de la resolución de *Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.* En cualquier caso, el progreso, los conflictos y las relaciones humanas son inseparables, por lo que avanzar en el acuerdo de puntos de encuentro es esencial para mantener el orden mundial y, para ello, el Derecho Internacional debe avanzar conforme exija la realidad del momento.

6. El desafío de seguridad en la Zona Gris

La *Zona Gris* (ZG) representa el amplio e indefinido *marco del conflicto no cinético* que abarca desde los límites que conforman las *relaciones de paz* hasta el preciso momento en que se declara la *guerra*. Como tal, goza de una naturaleza propia definida por su ambigüedad, la naturaleza híbrida de las acciones que en él se llevan a cabo, la asimetría y el gradualismo de su rango operacional y la relevancia de la población civil para la consecución de sus objetivos, siempre de alto contenido estratégico para el actor atacante. De esta forma, los protagonistas principales del conflicto en la Zona Gris solían ser los Estados pero el siglo XXI, con la globalización y la interdependencia de las relaciones internacionales, ha traído consigo la apertura hacia nuevos actores no estatales que interactúan en ella con sus propios intereses de variada naturaleza, mayormente vinculados a la consecución de influencia en el ámbito económico, político o ideológico, entre otros.

La propia naturaleza de la ZG hace que su utilización sea especialmente ventajosa para los Estados con objetivos revisionistas y estructuras de gobierno autocráticas, cuyos líderes buscan la continuidad de sus regímenes y la remodelación del contexto geopolítico de acuerdo a sus intereses con el fin de aumentar su *cuota de poder relativo*. Debido a la alta relevancia estratégica que este tipo de acciones en la ZG, el *control de*

Ediciones Universidad de Salamanca | CC BY-NC-ND

la escalada es pieza clave tanto para la identificación del nivel de la agresión como para determinar la *respuesta* que permita recuperar el control de la situación, sin que haya opción a réplica por parte del atacante que suponga cruzar el límite hacia un probable escenario de conflicto abierto. No obstante, la dificultad para detectar la agresión en la ZG, la delicada coyuntura en la que debe aplicarse la medida disuasoria y la exigencia de un enfoque holista y multidisciplinar de la estructura operativa de respuesta, no facilita la gestión de las opciones de réplica sin escalar la tensión ante un ataque híbrido.

En este particular contexto prospera la *desinformació*n que, aunque ha existido a lo largo de la historia como medio para alcanzar objetivos de poder y dominio que se ha ido beneficiando de los cambios evolutivos experimentados en las comunicaciones y la tecnología, ha encontrado en el siglo XXI los elementos idóneos para alcanzar una dimensión y un impacto nunca antes vistos que la han convertido en el paradigma de la amenaza híbrida de alcance global. *La amenaza desinformativa es la principal amenaza para las democracias* por cuanto penetra sutilmente en ellas afectando a la calidad de la convivencia y a la seguridad nacional de los Estados a través de la desafección ciudadana, el desgaste de las instituciones y el descrédito de sus procesos, auspiciando planteamientos que devienen en la polarización social derivada del fomento de posturas intolerantes, radicales y de odio.

Para medir el impacto de esta compleja amenaza híbrida que representa la desinformación y poder responder adecuadamente ante ella, *la UE ha generado un marco analítico y una metodología propia* que, al amparo de su Brújula Estratégica para la Seguridad y la Defensa, dan soporte a una serie de herramientas con las que poder afrontar la interferencia extranjera en los procesos electorales y apoyar la aplicabilidad del Derecho Internacional a la manipulación informativa en cualquiera de sus manifestaciones en la ZG. Al mismo tiempo, junto a este procedimiento y sus herramientas, la Unión ha desarrollado una política de regulación que garantiza la protección de los derechos y libertades que conforman su esencia democrática, y se ha volcado en la comunicación estratégica para comprometer a la sociedad civil, las empresas, las instituciones y organizaciones públicas y privadas en la tarea de alcanzar una adecuada alfabetización digital y mediática de los ciudadanos con el objetivo de fomentar su pensamiento crítico y la participación reflexiva en los procesos que sustancian la democracia.

Únicamente desde la comprensión de la verdadera naturaleza de la democracia, con sus debilidades y fortalezas, puede abordarse la *estrategia de defensa frente a la desinformación*, que requiere un enfoque holista de la seguridad y de las conexiones con los principios y valores que sustentan aquella, para no caer en excesos que puedan encubrir censuras o quiebras de derechos inapelables como la libertad de expresión o la libertad de información.

7. La estrategia de la Unión Europea frente a la amenaza desinformativa

El complejo entramado de intereses que subyace en las relaciones internacionales en el actual contexto geopolítico, junto con la cada vez mayor presencia de acciones en la ZG que condicionan aquellas, reclaman un enfoque conjunto y multifacético de la

Ediciones Universidad de Salamanca | CC BY-NC-ND

comunidad internacional en la lucha contra las estrategias híbridas y, en concreto, la desinformación como principal vía de entrada del discurso del odio, la radicalización y de las teorías conspirativas que tanto impacto han demostrado tener en las interacciones sociales, políticas y culturales a nivel global.

Por esta razón, tanto NNUU como la OTAN, estructuras de naturaleza totalmente diferente pero que comparten su vocación internacional, coinciden al señalar como objetivo de máximo interés la defensa de la integridad de la información. En este sentido, NNUU pone su mirada en el respeto de los derechos humanos y la salvaguarda de la libertad de expresión y del acceso a la información, abogando por el compromiso de las plataformas digitales en esta labor. Por su parte, la OTAN ha dado un paso adelante en la visión integral de la defensa de sus aliados frente a los diferentes vectores de ataque al equiparar las operaciones hostiles en los cinco dominios de forma que, desde el Concepto Estratégico de Madrid, las estrategias híbridas son calificadas como arma ofensiva en su marco de gestión cooperativa de la seguridad noratlántica.

En lo que respecta a la UE, cuyo ideal de defensa se fundamenta en la colaboración con NNUU y la OTAN para garantizar la estabilidad y el orden mundial desde el multilateralismo arbitrado por el Derecho Internacional, la *lucha contra las amenazas híbridas es uno de sus objetivos prioritarios* cuya responsabilidad recae en cada uno de sus Estados miembros, por su componente de seguridad nacional, pero que como desafío común se complementa a través de la respuesta coordinada europea con base en los principios de solidaridad y asistencia mutua de sus Tratados.

Conforme a ello, a partir de 2015 la respuesta de la Unión frente al desafío híbrido y la desinformación se viene construyendo desde la creación de un *marco normativo común y el desarrollo de herramientas orientadas a la detección temprana y la generación de inteligenci*a que, en conjunto, permitan el aumento del efecto disuasorio y la mejora de la resiliencia social e institucional. En este contexto se encuadra la creación de herramientas, estructuras y grupos de trabajo como el *East StratCom* del SEAE, el *Centro Europeo de Excelencia contra las Amenazas Híbridas* o la *EU Hybrid Toolbox*, así como el desarrollo de iniciativas entre las que cabe destacar el *Plan de Acción contra la Desinformación* o el *Código de Buenas Prácticas* -y su posterior versión reforzada-, que suponen la constatación del enfoque integral europeo frente esta amenaza que atiende no solo a la penalización de los comportamiento ilegítimos sino que, también, potencia la defensa de los derechos y valores de la democracia desde el compromiso del conjunto de los ciudadanos y resto de actores involucrados -públicos y privados-, donde los verificadores y las propias plataformas digitales tienen un relevante papel que cumplir.

El segundo de los objetivos prioritarios de la UE en el marco de la amenaza híbrida es el referido a la injerencia extranjera en sus procesos electorales, por cuanto estos son vistos por los Estados autocráticos -China y Rusia a la cabeza- como una oportunidad para promover sus intereses desde la ZG, recurriendo a la desinformación y la manipulación de la información para desprestigiar a las figuras políticas no afines a sus ideas, apoyar a los candidatos que más les favorezcan, instrumentalizar la problemática social y política existente en el Estado objetivo o, en definitiva, minar la credibilidad de las democracias y sus instituciones.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Para contrarrestar la injerencia extranjera, que la Unión reconoce como amenaza directa a la seguridad nacional de sus Estados miembros, se publica en 2020 el *Plan de Acción para la Democracia Europea* como pilar de su estrategia para la promoción de elecciones libres y justas, a través de la protección del derecho de los ciudadanos a una información veraz y libre de condicionamientos falseados, los cuales vician el debate público en torno a las elecciones e impiden la toma de decisiones consecuentes y contrastadas.

En este sentido, el *Marco de Respuesta FIMI* del SEAE ofrece una serie de herramientas para levantar la defensa de los procesos de elecciones democráticas europeas frente a las injerencias extranjeras, que se entienden en el conjunto de medidas articuladas para tratar de alcanzar un marco normativo europeo adaptado a la realidad de la amenaza junto con la gestión de la comunicación estratégica desde todos los organismos implicados.

No solo se trata de *definir una línea de actuación coordinada e integral* que reduzca la vulnerabilidad frente a este tipo de ataques sino que, al mismo tiempo, se busca *generar un compromiso resiliente de la ciudadanía y del sector privado* como remedio fundamental para contrarrestar la profunda tecnologización de estos procesos esenciales de las democracias, donde la sutil selección de los mensajes políticos, la categórica segmentación de los destinatarios y la retroalimentación permanente del flujo de información lleva a algunos autores a referirse a la *deshumanización de las elecciones.*

Es este elemento de *responsabilidad ciudadana* imbricado con el libre acceso a la información veraz el que determina la importancia de preservar la seguridad de los procesos electorales, máxima expresión de la voluntad popular en democracia. En este sentido, no puede obviarse el hecho de que la democracia atribuye la soberanía a la voluntad mayoritaria libremente conformada. De ahí la atención prestada por la UE al impacto que la desinformación y la influencia de terceros Estados, potenciado por el elevado nivel de digitalización y tecnologización de las campañas políticas, pueda tener en la estructura organizativa del sistema democrático y, a la postre, en su propia subsistencia.

8. La respuesta española frente a la desinformación con afectación a la seguridad nacional

España asienta su arquitectura de seguridad nacional sobre la LSN 2015 que, en su artículo 3, consagra la *dimensión ampliada de la seguridad nacional* en base a tres círculos concéntricos de protección que se complementan entre sí: la seguridad *personal*, la seguridad *colectiva* de la nación y, en su nivel exterior, la seguridad de nuestros socios y aliados en el *ámbito internacional*. Desde esta perspectiva tridimensional se atiende al amplio espectro de formatos de la amenaza en la ZG, área indefinida que cada vez ocupa más espacio en la relación entre Estados, donde la *desinformación fructifica como riesgo asociado a la seguridad nacional*.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Desde la constatación de la injerencia rusa en el proceso independentista catalán de 2017, España viene ofreciendo una respuesta legal y operativa a esta amenaza enmarcada en la estrategia definida por la UE a través del *Plan de Acción contra la Desinformación,* donde deben entenderse iniciativas españolas como la creación de la *Comisión Permanente contra la Desinformación,* el *Procedimiento de actuación contra la desinformación* y el *Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional*, a través de las cuáles se constata el posicionamiento de España respecto a la plena vigencia del Derecho Internacional como *corpus iuris* aplicable en el ciberespacio, la relevancia que merece la alfabetización mediática y la cultura de seguridad para afrontar las campañas de desinformación, y su singularidad como democracia avanzada que ejerce de punto de encuentro entre América Latina y Europa.

En este mismo sentido, debemos señalar a la *ESN 2021 como la primera Estrategia española que incluye las campañas de desinformación y la injerencia extranjera entre los riesgos que*, con alto componente tecnológico e híbrido, *amenazan a la seguridad nacional*, considerando esenciales para afrontarla la colaboración público-privada y la formación que estimule la participación ciudadana generando conocimiento y cultura crítica de seguridad. Sin embargo, esta línea de acción programática *no encuentra reflejo en el ciudadano medio español* que, aunque conoce el riesgo genérico que suponen la desinformación y la injerencia extranjera, no es consciente del alcance y los efectos que conllevan. Entre las distintas causas que pueden explicarlo se encuentran la falta de conciencia sobre la corresponsabilidad ciudadana en la lucha contra la desinformación, así como la erosión de la legitimidad de las instituciones responsables de la comunicación estratégica que alimente esa cultura. Como consecuencia, *el ciudadano entiende que su seguridad es asunto del Estado*, considerando que él solo encarna el rol de sujeto pasivo, incluso de víctima, a quien no le compete su defensa. Esta falta de *conciencia de corresponsabilidad* va necesariamente unida a la falta de *sensibilización ante amenazas* como la desinformativa que, o bien, no se valoran como creíbles o, directamente, se desconocen.

Es por ello que, en septiembre de 2024, se publique el *Plan de Acción por la Democracia* para, entre otros objetivos, proteger la democracia ante la erosión que sufre de cara a los ciudadanos y mejorar la transparencia y la rendición de cuentas del Gobierno, de los medios de comunicación y del poder legislativo, los tres pilares sobre los que construir la estrategia de respuesta española frente a esta amenaza. De las treinta y una medidas propuestas merece especial atención la referida a la redacción de una *Estrategia Nacional contra las Campañas de Desinformación*, como marco de desarrollo de los objetivos y líneas de acción para limitar el impacto de esta amenaza a la seguridad nacional, que se concreta en el Acuerdo del CSN de 28 de enero de 2025 para iniciar el consiguiente proceso de redacción de la misma.

En cuanto a la articulación operativa de la respuesta española contra la desinformación, debemos referirnos a la *corresponsabilidad de un amplio elenco de órganos y autoridades* que tienen entrada a través de *cuatro niveles de actuación complementarios*, quienes se distribuyen las partes técnica, táctica y estratégica del procedimiento. En el primero de estos niveles, en el que se encuadran las funciones de prevención, detección e investigación de la amenaza, se inscriben tres actores

Ediciones Universidad de Salamanca | CC BY-NC-ND

principales: el DSN, el CNI y las Unidades especializadas de las FCSE. En el segundo de ellos, es la Comisión Permanente contra la Desinformación la que se ocupa de la integración de la respuesta de los órganos afectados, así como de apoyar el proceso de toma de decisiones que, ya a nivel estratégico, deban llevarse a cabo.

Finalmente, debemos una vez más resaltar que en todo este proceso secuencial e integrado ocupa un lugar prioritario la corresponsabilidad del sector privado y la sociedad civil, por cuanto la primera línea de defensa contra la amenaza desinformativa se encuentra en sus propios destinatarios: los ciudadanos. Es por ello que la sociedad en su conjunto deba apostar por la resiliencia y el pensamiento crítico como base desde la que ejercer sus derechos en democracia y, por ende, garantizar la voluntad soberana del pueblo. Como dice el lema de la ESN 2021, *la seguridad nacional es un proyecto compartido.*

Ediciones Universidad de Salamanca | CC BY-NC-ND

Bibliografía

ABA CATOIRA, A. (2024). Respuestas normativas ante la inteligencia artificial generativa: ¿son suficientes? En F. CAAMAÑO, & D. JOVE VILLARES, *Tecnologías abusivas y derecho.* Valencia: Tirant lo Blanch.

ABAD QUINTANA, G., & PRIEGO MORENO, A. (enero-marzo de 2003). La división entre seguridad interior e internacional y la transformación del concepto de seguridad. (M. d.-D. Policía, Ed.) *Ciencia Policial*(67), 49-65.

ADÁN GARCÍA, Á. J. (4 de Abril de 2019). 70 años de evolución estratégica en la OTAN. (M. d. Defensa, Ed.) *Documento Marco - Instituto Español de Estudios Estratégicos*(4/2019). Obtenido de https://www.ieee.es/Galerías/fichero/docs_marco/2019/DIEEE04_2019ANGADA-OTAN.pdf

AGUIRRE DE CÁRCER Y GARCÍA DEL ARENAL, M. (2017). La adaptación de la OTAN: 2014-2017. En *OTAN: presente y futuro* (Vol. Cuadernos de Estrategia 191 del Instituto Español de Estudios Estratégicos, págs. 15-50). Ministerio de Defensa.

ALAMINOS HERVÁS, M. Á. (septiembre-diciembre de 2018). *Las estrategias de seguridad de la Unión Europea (2003, 2016): contexto político, cambios esenciales y evolución de las prioridades políticas europeas relativas a África en materia de seguridad.* Recuperado el 20 de octubre de 2023, de Universidad de la Rioja, en https://dialnet.unirioja.es: https://revistas.comillas.edu/index.php/internationalrelations/article/view/10694

ALBALADEJO CAMPOS, F. (2011). El Programa de Estocolmo de la Unión Europea. En *La seguridad en Europa tras el Tratado de Lisboa* (pág. 247). Madrid: Fundación Policía Española.

ALCARO, R. (mayo de 2021). *The constraints on the EU Foreign and Security Policy.* Recuperado el 12 de octubre de 2023, de Joint Project EU, en www.jointproject.eu: https://www.jointproject.eu/2021/05/01/the-constraints-on-the-eu-foreign-security-policy/

ALONSO BERRIO, M. (2003). Los Estados fallidos. En J. FUENTES MONZONÍS VILLALONGA, *Nuevos Riesgos para la sociedad del futuro* (págs. 199-227). Maddrid: Ministerio de Defensa - Instituto Español de Estudios Estratégicos.

ALONSO MOREDA, N. (enero/abril de 2012). *Eurojust, a la vanguardia de la cooperación judicial en materia penal en la Unión Europea.* Recuperado el 18 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es/: https://dialnet.unirioja.es/servlet/articulo?codigo=4019204

ALONSO SECO, J. M. (Agosto de 2020). *Seguridad Social y principio de solidaridad.* (U. N. (UNED), Ed.) Recuperado el 19 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://revistas.uned.es/index.php/derechopolitico/article/view/27997/21774

ÁLVAREZ ROBLES, T. (2023). *El derecho de acceso a Internet. Especial referencia al constitucionalismo español.* Valencia: Tirant Lo Blanch.

ÁLVAREZ ROBLES, T. (2024). Digital Sovereignty, Cybersecurity and Geopolitical Implications. En E. CELESTE, *Digital Sovereignty and Green Transition.*

Ediciones Universidad de Salamanca | CC BY-NC-ND

ÁLVAREZ ROBLES, T. (2024). La ciberseguridad: la seguridad integral y descentralizada del estado digital. En F. CAAMAÑO, & D. JOVE VILLARES, *Tecnologías abusivas y derecho.* Valencia: Tirant lo Blanch.

ÁLVAREZ ROBLES, T. (15 de enero de 2024). *Soberanía digital en el contexto europeo de la ciberseguridad.* Recuperado el 7 de febrero de 2024, de www.ibericonnect.blog: https://www.ibericonnect.blog/2024/01/soberania-digital-en-el-contexto-europeo-de-la-ciberseguridad/

ÁLVAREZ ROBLES, T. (2025). Democracias amenazadas por la manipulación informativa. La desinformación en el ámbito de la seguridad. En J. FERNÁNDEZ RODRÍGUEZ, *Análisis sobre la manipulación informativa. Un desafío para la democracia.* Valencia: Tirant lo Blanch.

ALZAGA VILLAAMIL, O., & ÁLVAREZ RODRÍGUEZ, I. (2021). *Derecho político español según la Constitución de 1978* (7ª ed., Vol. Tomo I). Madrid: Marcial Pons.

AMIOT, E., PALENCIA, I., BAENA, A., & DE POMMEROL, C. (2020). *European Digital Sovereignty. Syncing values and value.* Recuperado el 8 de febrero de 2024, de Oliver Wyman, en https://www.oliverwyman.com: https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html

ANDRÉS SÁENZ DE SANTA MARÍA, M. P. (junio de 2021). *Nosotros los pueblos: las Naciones Unidas cumplen 75 años.* Recuperado el 17 de febrero de 2024, de Revista Electrónica de Estudios Internacionales - REEI, en www.reei.org: http://www.reei.org/index.php/revista/num41/tribuna

ANGUITA OSUNA, J. (2021). *La seguridad interior en la Unión Europea: del Acuerdo de Schengen 1985 a la Estrategia para una Unión de la Seguridad 2020* (Primera edición ed.). Cizur Menor (Navarra): Aranzadi SAU.

AREN, E., SANZ, D., & CAMPOS, M. (Diciembre de 2020). Departamento de Seguridad Nacional. Un proyecto compartido. *Policía*(349), 4-15.

ARGÉS, J. R. (enero-junio de 2021). *Las resoluciones de la Asamblea General de Naciones Unidas y la costumbre internacional.* Recuperado el 17 de febrero de 2024, de SciELO México, en www.scielo.org: http://www.scielo.org.co/pdf/rfdcp/v51n134/0120-3886-rfdcp-51-134-239.pdf

ARRIETA-LÓPEZ, M. (enero-diciembre de 2022). Evolución del derecho humano a la paz en el marco de las Naciones Unidas y de las Organizaciones de la Sociedad Civil. *Jurídicas CUC, 18*(1), 519-554. doi:http://dx.doi.org/10.17981/juridcuc.18.1.2022.21

ARTEAGA MARTÍN, F. (21 de abril de 2010). *La Estrategia de Seguridad Interior de la Unión Europea.* Recuperado el 12 de noviembre de 2023, de Real Instituto Elcano, en www.realinstitutoelcano.org: https://media.realinstitutoelcano.org/wp-content/uploads/2010/04/ari75-2010-arteaga-estrategia-seguridad-interior-union-euorpea.pdf

ARTEAGA MARTÍN, F. (27 de junio de 2011). *¿Qué son las estrategias de seguridad nacional?* Recuperado el 28 de diciembre de 2023, de Real Instituto Elcano, en www.realinstitutoelcano.org: https://www.realinstitutoelcano.org/comentarios/sobre-la-estrategia-espanola-de-seguridad/

ARTEAGA MARTÍN, F. (29 de junio de 2016). *¿La Estrategia Global de la UE?... déjela ahí.* Recuperado el 15 de octubre de 2023, de Real Instituto Elcano, en

Ediciones Universidad de Salamanca | CC BY-NC-ND

www.realinstitutoelcano.org: https://www.realinstitutoelcano.org/blog/la-estrategia-global-de-la-ue-dejela-ahi/

ARTEAGA, F., & SIMÓN, L. (7 de julio de 2022). *El Concepto Estratégico de Madrid: una (auto)evaluación de los resultados.* Recuperado el 12 de septiembre de 2024, de Real Instituto Elcano, en https://www.realinstitutoelcano.org: https://www.realinstitutoelcano.org/analisis/el-concepto-estrategico-de-madrid-una-autoevaluacion-de-los-resultados/

ARTEAGA, F., & SIMÓN, L. (31 de julio de 2023). *La OTAN tras la Cumbre de Vilna.* Recuperado el 12 de marzo de 2024, de Real Instituto Elcano, en https://www.realinstitutoelcano.org: https://www.realinstitutoelcano.org/analisis/la-otan-tras-la-cumbre-de-vilna/

ÁVILA, E. (2 de julio de 2018). *Ciberespacio: el dominio del desarrollo humano.* Recuperado el 22 de febrero de 2024, de Fundación Ortega-Marañón, en https://ortegaygasset.edu: https://ortegaygasset.edu/ciberespacio-el-dominio-del-desarrollo-humano/

AZNAR FERNÁNDEZ-MONTESINOS, F. (2011). *Entender la guerra en el siglo XXI* (1ª ed.). Madrid: Editorial Complutense S.A. y Ministerio de Defensa. Recuperado el febrero de 2024

AZNAR FERNÁNDEZ-MONTESINOS, F. (17 de Septiembre de 2024). *El retorno de la guerra*. Recuperado el 19 de Septiembre de 2024, de El Diario Montañés, en https://www.eldiariomontanes.es: https://www.eldiariomontanes.es/opinion/federico-aznar-retorno-guerra-20240917071453-nt.html

AZNAR FERNÁNDEZ-MONTESINOS, F. (2024). *La guerra. Teoría para comprender los conflictos del siglo XXI.* Barcelona: El Viejo Topo.

B.M.J. PIJPERS, P. (Febrero de 2024). *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats.* Recuperado el 4 de marzo de 2024, de https://www.hybridcoe.fi/: https://www.hybridcoe.fi/wp-content/uploads/2024/02/20240222-Hybrid-CoE-Paper-19-Legal-powerplay-in-cyberspace-WEB.pdf

BADILLO MATOS, A., BALDI, V., ARTEAGA, F., PAISANA, M., CRESPO, M., CARDOSO, G., . . . MOLINA SOLANA, M. (2023, marzo). *Analysis of the impact of disinformation on political, economic, social and security issues, governance models and good practices: the cases of Spain and Portugal.* Retrieved enero 12, 2025, from IBERIFIER Iberian Media Research & Fact-Checking, en https://iberifier.eu: https://iberifier.eu/2023/06/21/report-analysis-impact-disinformation-june-2023/

BADILLO, Á. (14 de mayo de 2019). *La sociedad de la desinformación: propaganda, fake news y la nueva geopolítica de la información.* Recuperado el 7 de diciembre de 2024, de Real Instituto Elcano, en www.realinstitutoelcano.org: https://www.realinstitutoelcano.org/wp-content/uploads/2021/10/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion.pdf

BADILLO, Á., & ARTEAGA, F. (2024). *El impacto estratégico de la desinformación en España.* Comisión Europea.

BALLESTEROS MARTÍN, M. Á. (20 de diciembre de 2017). *Las novedades de la Estrategia de Seguridad Nacional 2017.* (M. d. Defensa, Ed.) Recuperado el 3 de

Ediciones Universidad de Salamanca | CC BY-NC-ND

junio de 2023, de Instituto Español de Estudios Estratégicos: https://www.ieee.es/Galerias/fichero/docs_analisis/2017/DIEEEA74-2017_Novedades_ESN2017_MABM.pdf

BALLESTEROS MARTÍN, M. Á. (Diciembre de 2020). Departamento de Seguridad Nacional: un proyecto compartido. *Revista Policía*, 12-15. (D. SANZ, & M. CAMPOS, Entrevistadores) Dirección General de la Policía.

BALLESTEROS MARTÍN, M. A. (2016). *En busca de una Estrategia de Seguridad Nacional.* Madrid: Ministerio de Defensa - Secretaría General Técnica.

BAQUÉS QUESADA, J. (2021). *De las guerras híbridas a la zona gris* (1ª ed.). Madrid: Universidad Nacional de Educación a Distancia (UNED). Recuperado el febrero de 2024

BAQUÉS QUESADA, J. (2022). De la geopolítica a la reconfiguración del orden mundial. En G. C. Piella, *La guerra de Ucrania. Los 100 días que cambiaron Europa.* Madrid: Los libros de la catarata.

BAQUÉS QUESADA, J. (2023). *La construcción de una política exterior y de seguridad común en Europa. ¿Por qué es tan problemática?* (Vols. Colección Investigación y Debate - EJERCITOS). Madrid: Catarata.

BAQUÉS QUESADA, J., & FOJÓN LAGOA, E. (2023). *La realidad geopolítica de España. Hacia el estatus de actor estratégico.* Madrid: Universidad Nacional de Educación a Distancia.

BARBÉ IZUEL, E. (12 de julio de 2004). *Orden internacional: ¿uno o varios? Neoimperialismo, caos y posmodernidad.* Recuperado el 2 de abril de 2023, de Universidad del País Vasco, en www.ehu.eus: https://www.ehu.eus/es/web/cursosderechointernacionalvitoria/-/orden-internacional-uno-o-varios-neoimperialismo-caos-y-posmodernidad

BAVARESCO, A. (2003). La crisis del estado-nación y la teoría de la soberanía en Hegel. *Recerca. Revista de Pensament I Anàlisi*(3), 55-80. Recuperado el marzo de 2023

BAY, S. (marzo de 2024). *Contrarrestar las amenazas híbridas a las elecciones: desde la actualización normativa al establecimiento de redes de colaboración.* Recuperado el 13 de mayo de 2024, de Hybrid CoE, en https://www.hybridcoe.fi: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/

BECK, U. (2003). *Sobre el terrorismo y la guerra.* (R. CARBO, Trad.) Barcelona: Paidós Ibérica.

BLANCO, R. (Abril-junio de 2014). Del mantenimiento de la paz al proceso de formación del Estado: un esbozo de los esfuerzos de la ONU para la paz internacional. *Foro Internacional, LIV*(2), 266-318.

BLOCKMANS, S., & FALEG, G. (febrero de 2015). *More Union in European Defence. Report of a CEPS Task Force.* Obtenido de Centre for European Policy Studies, en https://www.ceps.eu: https://cdn.ceps.eu/wp-content/uploads/2015/03/TFonEuropeanDefence.pdf

BORRELL FONTELLES, J. (3 de diciembre de 2020). *Por qué es importante la autonomía estratégica europea.* Recuperado el 6 de octubre de 2023, de European Union External Action, en www.eeas.europa.eu:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.eeas.europa.eu/eeas/por-qué-es-importante-la-autonomía-estratégica-europea_es
BORRELL FONTELLES, J. (27 de julio de 2022). *La ampliación y la profundización: los imperativos geopolíticos para la UE.* Recuperado el 3 de octubre de 2023, de European Union External Action, en www.eeas.europa.eu: https://www.eeas.europa.eu/eeas/la-ampliación-y-la-profundización-los-imperativos-geopoliticos-para-la-ue_es
CABREJAS MARTÍNEZ, P. (30 de octubre de 2023). *La amenaza yihadista del Sahel Occidental se expande al Golfo de Guinea.* Recuperado el 17 de marzo de 2024, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/publicaciones-new/documentos-de-opinion/2023/DIEEEO91_2023_PAUCAB_Sahel.html
CALDERÓN FERNÁNDEZ, J. (2003). Los servicios de inteligencia. En *Terrorismo Internacional en el siglo XXI.* Mnisterio de Defensa.
CALVO ALBERO, J. (2022). Amenazas híbridas y Fuerzas Armadas frente a la estrategia híbrida. *XLVII Curso de Defensa Nacional del CESEDEN.* Madrid.
CALVO ALBERO, J. (2022). Primeras impresiones militares. En G. C. Piella, *La guerra de Ucrania. Los 100 días que cambiaron Europa.* Madrid: Los libros de la catarata.
CALVO GONZÁLEZ-REGUERAL, C. (2021). *Política europea de seguridad y defensa y sus efectos enla industria de la defensa.* Recuperado el 18 de febrero de 2024, de Revista de Estudios en Seguridad Internacional, en www.seguridadinternacional.es: https://www.seguridadinternacional.es/resi/index.php/revista/article/view/373
CAPODIFERRO CUBERO, D. (septiembre/diciembre de 2017). *La libertad de información frente a Internet.* Recuperado el 19 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=6238886
CARLÓN RUIZ, M. (19 de noviembre de 2020). *Veracidad v. Verdad. Información v. Desinformación. Algunas reflexiones al hilo del "Procedimiento de actuación contra la desinformación aprobado el 6 de octubre de 2020.* Recuperado el 7 de diciembre de 2024, de Iustel Diario de Derecho, en www.iustel.com: https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1204931
CARLINI, A. (1 de diciembre de 2015). *ISIS: una nueva amenaza en la Era Digital.* Recuperado el 24 de marzo de 2024, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-2015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf
CARMENT, D., & BELO, D. (octubre de 2018). *War´s future: the risks and rewards of Grey-Zone conflict and Hybrid Warfare.* Recuperado el 3 de mayo de 2024, de Canadian Global Affairs Institute, en www.cgai.ca: https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare
CASANOVAS Y LA ROSA, O., & RODRIGO HERNÁNDEZ, Á. (2016). *Casos y textos de Derecho Internacional Público* (7ª ed.). Madrid: TECNOS. Recuperado el 12 de abril de 2024

Ediciones Universidad de Salamanca | CC BY-NC-ND

CASTELLÓN MORENO, J. (diciembre de 2015). *Entrevista a Joaquín Castellón, Director Operativo del DSN.* (Bormart, Ed.) Recuperado el 28 de diciembre de 2024, de Securitecnia. Revista decana independiente de seguridad, en https://www.seguritecnia.es: https://www.seguritecnia.es/revistas/seg/426/2/index.html

CASTELLANOS CLARAMUNT, J. (3 de diciembre de 2023). *Sobre los desafíos constitucionales ante el avance de la Inteligencia Artificial. Una perspectiva nacional y comparada.* Recuperado el 16 de diciembre de 2024, de UNED. Revista de Derecho Político, en https://revistas.uned.es: https://revistas.uned.es/index.php/derechopolitico/article/view/39105

CAZORLA PRIETO, L. M. (2018). *Estudios de Derecho Militar* (Vol. 2). Madrid: Ministerio de Defensa. Recuperado el febrero de 2024

CHINCHILLA MARÍN, C. (1986). *Prólogo a la primera edición de Legislación sobre Fuerzas y Cuerpos de Seguridad.* Madrid: Tecnos. Recuperado el 19 de febrero de 2024

CHOMSKY, N. (1994). *El Nuevo Orden Mundial (y el Viejo).* (C. CASTELLS, Trad.) Editorial Planeta.

CLAUSEWITZ, C. (2021). *De la Guerra* (1ª ed.). Barcelona: Obelisco.

COELLO DE PORTUGAL, J. (2020). *La jefatura del Estado.* Cizur Menor, Navarra, España: Aranzadi.

COELLO DE PORTUGAL, J. (18 de septiembre de 2023). *Sobre la nueva denominación del Ejército del Aire y del Espacio y su paradoja: una norma inconstitucional que anuncia una deseable reforma de la Constitución.* Recuperado el 11 de marzo de 2024, de UNED. Revista de Derecho Político, en https://revistas.uned.es: https://revistas.uned.es/index.php/derechopolitico/issue/view/1780

COELLO DE PORTUGAL, J. (2024). La política de seguridad y defensa de la Unión Europea: ¿parte de su identidad constitucional? En J. FERNÁNDEZ-MIRANDA FERNÁNDEZ-MIRANDA, O. GODOY VÁZQUEZ, M. J. ROCA FERNÁNDEZ, J. M. COELLO DE PORTUGAL, C. DE FUENTES GARCÍA ROMERO DE TEJADA, R. GONZÁLEZ DE ZÁRATE LORENTE, & C. FERRER MARTÍN DE VIDALES, *Identidad constitucional de la Unión Europea y elemento cultural.* Tirant Lo Blanch.

COLOM PIELLA, G. (2006). *Dialnet.* Recuperado el 8 de marzo de 2024, de www.dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=4574803

COLOM PIELLA, G. (junio de 2018). *Guerras híbridas: cuando el contexto lo es todo.* Recuperado el 7 de marzo de 2024, de Universidad de Granada, en https://www.ugr.es: https://www.ugr.es/~gesi/Guerras-hibridas.pdf

COLOM PIELLA, G. (28 de octubre de 2021). *Instituto Español de Estudios Estratégicos.* Recuperado el 13 de enero de 2024, de www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO121_2021_GUICOL_Planeamiento.pdf

COLOM PIELLA, G. (30 de noviembre de 2023). *Pensamiento militar ruso y suposiciones sobre la zona gris y la guerra en Ucrania.* Recuperado el 20 de abril de 2024, de Dialnet, en www.dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=9286046

COLOM PIELLA, G. (4 de septiembre de 2023). *Wagner y su "marcha por la libertad": los dos días que estremecieron al Kremlin.* Recuperado el 18 de febrero de

Ediciones Universidad de Salamanca | CC BY-NC-ND

2024, de Instituto Español de Estudios Estratégicos: https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO70_2023_GUICOL_Wagner.pdf
COLOM PIELLA, G., & CÓZAR MURILLO, B. (septiembre de 2022). *Deusto Facultad de Ciencias Sociales y Humanas.* Recuperado el 18 de febrero de 2024, de https://ced.revistas.deusto.es: https://ced.revistas.deusto.es/article/view/2521
COLOM PIELLA, G., & CÓZAR MURILLO, B. (2023). Prólogo. En B. CÓZAR MURILLO, & G. COLOM PIELLA, *La guerra de Ucrania II. De la conquista de Lugansk a la contraofensiva ucraniana.* Madrid: Los libros de la catarata.
COLOM PIELLA, G., & VALES CALDERÓN, R. (2023). Innovaciones militares y revoluciones en los asuntos militares. En A. BUENO, & G. COLOM PIELLA, *La transformación de la guerra en el siglo XXI. Estudios estratégicos para su comprensión* (1ª edición octubre 2023 ed., págs. 75-93). Madrid: UNED.
COLOM PIELLA, G., FATJO GÓMEZ, P., FURLÁN, L., GALLEGO COSME, M., GARCÍA MORENO, L., GIL, J., . . . VILLANUEVA LÓPEZ, C. (2022). *Geopolítica de las bases militares.* Madrid: Ministerio de Defensa.
COLOM PIELLA, G., MEDINA IBORRA, I., & PEÑA RAMOS, J. (2017). *Dialnet.* Recuperado el 18 de febrero de 2024, de https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=5885503
COLOMINA, J. (2022). La Alianza y su aproximación 360º a la seguridad. En *El futuro de la OTAN tras la Cumbre de Madrid 2022 - Cuadernos de Estrategia 211* (Vol. Cuadernos de Estrategia 211, págs. 85-96). Madrid: Ministerio de Defensa - Instituto Esañol de Estudios Estratégicos.
CONGRESO DE LOS DIPUTADOS. (4 de abril de 2023). Recuperado el 4 de abril de 2023, de www.congreso.es: https://www.congreso.es
CORN, G. (3 de septiembre de 2020). *Cyber operations and the imperfect art of "translating" the law of war to new technologies.* Recuperado el 8 de abril de 2024, de Lieber Institute West Point, en www.lieber.westpoint.edu: https://lieber.westpoint.edu/cyber-operations-imperfect-translating-law-war-new/
CORREDOIRA Y ALFONSO, L. (11 de julio de 2024). *Garantías de la libertad de expresión en redes sociales y medios. Doctrina de la Junta Electoral Central durante los comicios españoles celebrados en 2023.* Recuperado el 14 de enero de 2025, de Revista de Derecho Político de la UNED, en https://revistas.uned.es: https://revistas.uned.es/index.php/derechopolitico/article/view/41767
COSTIGAN, S., & HENNESSY, M. (Junio de 2024). *Hybrid Threats and Hybrid Warfare Reference Curriculum.* Recuperado el 22 de Noviembre de 2024, de North Atlantic Treaty Organization, en https://www.nato.int/: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf
COTINO HUESO, L. (2022). *Quién, cómo y qué regular (o no regular) frente a la desinformación.* Recuperado el 5 de enero de 2025, de Dialnet, en https://dialnet.unirioja.es/: https://dialnet.unirioja.es/servlet/articulo?codigo=8450040
CRESPO-PAZMIÑO, D. (julio de 2020). *Ciberseguridad y Derechos Humanos: respuestas estatales e individuales a las revelaciones de espionaje de Snowden.*

Ediciones Universidad de Salamanca | CC BY-NC-ND

Recuperado el 28 de Febrero de 2024, de Revista del Centro Andino de Estudios Internacionales, en https://revistas.uasb.edu.ec/: https://revistas.uasb.edu.ec/index.php/comentario/article/view/1544/1315

CRISTIAN VELILLA, J. (Noviembre de 2022). Comisarías Europeas: fuerzas renovadas para un proyecto consolidado. (D. G. Policía, Ed.) *Policía - Revista Oficial de la Policía Nacional*, 20-27.

DACOBA CERVIÑO, F. (24 de marzo de 2021). *Autonomía Estratégica Europea: ni contigo, ni sin tí...* Recuperado el 3 de octubre de 2023, de Instituto Español de Estudios Estratégicos, en www.ieee.es: http://www.ieee.es/Galerias/fichero/docs_analisis/2021/DIEEEA13_2021_FRANDAC_Autonomia.pdf

DE ANTÓN LÓPEZ, J. (2000). *Historia de la Policía Española* (Primera ed.). (J. DE ANTON LOPEZ , Ed.) Madrid: Privada del autor.

DE AREILZA Y MARTÍNEZ DE RODAS, J. M. (6 de octubre de 1992). *Sobre el Nuevo Orden Mundial y el "Gendarme Universal"*. Recuperado el 17 de febrero de 2024, de Biblioteca BOE, en https://www.boe.es: https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-M-1993-10000900016

DE CARLOS IZQUIERDO, J. (30 de septiembre de 2016). *La nueva Estrategia de Seguridad Europea 2016.* Recuperado el 12 de octubre de 2023, de Instituto Español de Estudios estratégicos, en www.ieee.es: https://www.ieee.es/en/Galerias/fichero/docs_marco/2016/DIEEEM16-2016-EstrategiaSeguridad_DeCarlos.pdf

DERSHOWITZ, A. (2004). *¿Por qué aumenta el terrorismo?. Para comprender la amenaza y responder al desafío.* (G. ROSÓN, Trad.) Ediciones Encuentro.

DÍAZ FERNÁNDEZ, A. M. (junio de 2012). *Evolución de la cooperación europea en inteligencia.* (B. Fundación para el Apoyo a la Investigación del Estado de São Paulo, Ed.) Recuperado el 12 de noviembre de 2023, de SciELO Biblioteca Científica Electrónica en Línea, en www.scielo.org: https://www.scielo.br/j/vh/a/tTgvTYKGpW78t33zgxWPnxB/?lang=es&format=pdf

DÍAZ FERNÁNDEZ, A. M. (2013). *El papel de la inteligencia estratégica en el mundo actual.* Recuperado el 13 de enero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=4275959

DÍAZ FERNÁNDEZ, A., ABAD, M. F., ALONSO, R., ARCOS, R., ARROYO, S., BOLTAINA, X., . . . VIAMONTE, A. (2013). *Inteligencia y Seguridad* (1ª ed.). (J. BRUNET, Trad.) Madrid: LID Editorial Empresarial y Ministerio de la Presidencia. Gobierno de España. Recuperado el febrero de 2024

DÍAZ RODRÍGUEZ, J. (31 de mayo de 2018). *La Política Común de Seguridad y Defensa de la UE: una renovada estrategia para un nuevo escenario europeo y global.* Recuperado el 29 de octubre de 2023, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO65-2018_PCSD_JoelDiaz.pdf

DÍAZ RODRÍGUEZ, J. (2 de octubre de 2020). *La OTAN después de los 70: desafíos y redefinición de la alianza.* Recuperado el 22 de julio de 2023, de ieee.es:

Ediciones Universidad de Salamanca | CC BY-NC-ND

http://www.ieee.es/Galerias/fichero/docs_marco/2020/DIEEEM08_2020JOEDIA_OTAN70.pdf
DIEZ ALCALDE, J. (9 de enero de 2024). *África: visión y cooperación desde Europa y España.* Recuperado el 9 de enero de 2024, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_analisis/2024/DIEEEA01_2024_JESDIE_Africa.pdf
DÍEZ-PICAZO, L. (octubre de 2008). *La naturaleza de la Unión Europea.* Recuperado el 22 de noviembre de 2023, de InDret. Revista para el análisis del Derecho, en www.indret.com: https://indret.com/la-naturaleza-de-la-union-europea/
Dirección de Estudios, Análisis y Publicaciones de la Secretaría General del Congreso de los Diputados. (2022). Qué es el Congreso de los Diputados. 63. Madrid: Departamento de Publicaciones del Congreso de los Diputados.
ECHEVERRÍA JESÚS, C. (2019). *Relaciones Internacionales III. Paz, seguridad y defensa en la sociedad internacional.* Madrid: Universidad Nacional de Educación a Distancia - UNED.
ENSEÑAT Y BEREA, A. (2004). *La Estrategia Europea de Seguridad.* (IEEE, Ed.) Recuperado el 23 de octubre de 2023, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=2203899
ESTRADA RODRÍGUEZ, J. (mayo-agosto de 2013). Democracia, Estado y seguridad ciudadana. *Alegatos*(84). Obtenido de https://alegatosenlinea.azc.uam.mx
EXPÓSITO GUISADO, J. (2024). La ciberguerra que no fue: el conflicto entre Rusia y Ucrania visto desde el dominio cibernético. En B. CÓZAR MURILLO, & C. VILLANUEVA LÓPEZ, *La guerra de Ucrania III. De la reconquista de Jersón al estancamiento.* Madrid: Los libros de la catarata.
FERNÁNDEZ BARALLOBRE, J. E. (Junio de 2023). Celadores Reales. (D. G. Policía, Ed.) *Policía*(377), 48-53.
FERNÁNDEZ DE CASADEVANTE ROMANI, C., CARRERA HERNÁNDEZ, F. J., GARRIDO REBOLLEDO, V., & GONZÁLEZ MARÍN, A. M. (2023). *Nociones Básicas de Derecho de la Unión Europea* (6ª edición ed.). Madrid: Editorial Centro de Estudios Ramón Areces.
FERNÁNDEZ FERREÑO, A. (20 de diciembre de 2022). *El nuevo Concepto Estratégico de la OTAN: perspectivas de la Alianza frente al ascenso chino.* Recuperado el 31 de julio de 2023, de Instituto español de Estudios Estratégicos ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO114_2022_ALEFER_Concepto.pdf
FERNÁNDEZ-MIRANDA CAMPOAMOR, A. (septiembre - diciembre de 2003). *El Estado social.* Recuperado el 16 de marzo de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=802674
FERNÁNDEZ-MIRANDA FERNÁNDEZ-MIRANDA, J. (2024). La cultura jurídica como elemento vertebrador de la identidad constitucional de la Unión Europea. En J. FERNÁNDEZ-MIRANDA FERNÁNDEZ-MIRANDA, O. GODOY VÁZQUEZ, M. J. ROCA FERNÁNDEZ, J. M. COELLO DE PORTUGAL, C. FUENTES GARCÍA ROMERO DE TEJADA, R. GONZÁLEZ DE ZÁRATE LORENTE, . . . B. RODRÍGUEZ, *Identidad constitucional de la Unión Europea y elemento cultural.* Valencia: Tirant lo Blanch.

Ediciones Universidad de Salamanca | CC BY-NC-ND

FERNÁNDEZ RODRÍGUEZ, J. (2024). ¿La manipulación informativa destruirá a la democracia? A Coruña: Editorial Colex S.L.

FLORIDI, L. (12 de febrero de 2024). *El giro hardware en el discurso digital: análisis, explicación y riesgo potencial.* Recuperado el 21 de febrero de 2024, de CEDE (Centro de ética digital), en https://ssrn.com: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723312

FONT, T., & ORTEGA, P. (2012). Seguridad nacional, seguridad multidimensional, seguridad humana. *Papeles de relaciones ecosociales y cambio global*(119), 161-172.

FREEDMAN, L. (2019). *Estrategia. Una historia* (3ª ed.). Madrid: La Esfera de los Libros. Recuperado el febrero de 2024

FREIXES SANJUÁN, T., & REMOTTI CARBONELL, J. C. (1995). *La configuración constitucional de la seguridad ciudadana.* Recuperado el 19 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=27316

FUENTE COBO, I. (abril de 2022). *La OTAN y el ciberespacio: un nuevo dominio para las operaciones.* Recuperado el 22 de febrero de 2024, de Instituto Español de Estudios Estratégicos, en https://www.ieee.es: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf

FUENTE COBO, I. (2022). Los ocho conceptos estratégicos de la historia aliada. En *El futuro de la OTAN tras la cumbre de Madrid 2022 - Cuadernos de Estrategia 211* (Vol. 211, págs. 25-44). Madrid: Ministerio de Defensa.

FUENTE COBO, I. (8 de noviembre de 2023). *Hacia una nueva visión de la cooperación europea con África.* Recuperado el 8 de noviembre de 2023, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_analisis/2023/DIEEEA76_2023_IGNFUE_Africa.pdf

FUENTES MONZONÍS-VILLALONGA, J. (29 de junio de 2011). *La defensa europea del Tratado de Bruselas de 1948 al de Lisboa 2010.* Recuperado el 16 de agosto de 2023, de Instituto Español de Estudios Estratégicos, en https://www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO50_2011DefensaEuropea.pdf

FUKUYAMA, F. (2015). *¿El fin de la Historia? y otros ensayos* (Segunda reimpresión 2017 ed.). Madrid, España: Alianza Editorial S.A.

GALÁN, C. (13 de diciembre de 2018). *Amenazas híbridas: nuevas herramientas para viejas aspiraciones.* Recuperado el 28 de marzo de 2024, de Real Instituto Elcano, en www.realinstitutoelcano.org: https://www.realinstitutoelcano.org/wp-content/uploads/2021/10/dt20-2018-galan-amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones.pdf

GARCÍA ARNAIZ, F. J. (Diciembre de 2017). La estructura de mando de la Alianza Atlántica (NCS). (M. d. Técnica., Ed.) *Cuadernos de Estrategia. OTAN: presente y futuro*(191), 51-83. Obtenido de https://publicaciones.defensa.gob.es/

GARCÍA CANTALAPIEDRA, D. (2023). Hacia un nuevo concepto de seguridad: la crisis de los Estudios de Seguridad en el declive del orden internacional liberal multilateral. En C. ESTRADA VILLASEÑOR, M. J. HERRERA CEBALLOS, D. GARCÍA CANTALAPIEDRA, Y. MOLINERO GERBEAU, J. N. NUÑEZ CALVO, N. FERRE TRAD,

Ediciones Universidad de Salamanca | CC BY-NC-ND

. . . J. A. MORA TEBAS, *Crisis migratorias como elemento de coerción internacional - Cuadreno de Estrategia 222* (págs. 47-86). Madrid: Ministerio de Defensa. Recuperado el 21 de diciembre de 2023, de www.ieee.es

GARCÍA GARCÍA, R. (octubre de 2019). *El derecho de reunión virtual, netstrike o cibermanifestación. Un análisis jurídico.* Recuperado el 26 de abril de 2024, de Revista General de Derecho Constitucional, en https://www.iustel.com: https://www.iustel.com//v2/revistas/detalle_revista.asp?id=3&numero=30

GARCÍA GUINDO, M., & MARTÍNEZ-VALERA GONZÁLEZ, G. (15 de febrero de 2015). *La guerra híbrida: nociones preliminares y su repercusión en el planeamiento de los países y organizaciones occidentales.* Recuperado el 26 de marzo de 2024, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/en/Galerias/fichero/docs_trabajo/2015/DIEEET02-2015_La_Guerra_Hibrida_GUindo_Mtz_Glez.pdf

GARCÍA HERNÁN, D., & CATALÁ MARTÍNEZ, I. (2012). *Historia de la guerra.* Madrid: Editorial Síntesis.

GARCÍA SÁNCHEZ, F. (2019). Introducción a la Agenda 2030 y los ODS: Nueva arquitectura para la seguridad. En G. d. España (Ed.), *La Agenda 2030 y los ODS: Nueva arquitectura para la seguridad.* Madrid.

GARCÍA SAN PEDRO, J. (1º semestre de 2006). *La cooperación policial en la Unión Europea.* Recuperado el 14 de noviembre de 2023, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=2514171

GARCÍA SERVET, R. C. (2015). *El vínculo transatlántico en seguridad y defensa, ayer, hoy, "¿mañana?".* Recuperado el 18 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=5255545

GARCÍA VALDECASAS, I. (27 de Diciembre de 2005). *El rechazo al proyecto de Constitución Europea: un análisis retrospectivo.* Recuperado el 18 de febrero de 2024, de Real Instituto Elcano, en www.realinstitutoelcano.org: https://www.realinstitutoelcano.org/analisis/el-rechazo-al-proyecto-de-constitucion-europea-un-analisis-retrospectivo/

GARCÍA VARGAS, J. (1993). *El futuro de la Alianza en un contexto de seguridad expandido.* Recuperado el 18 de febrero de 2024, de Dialnet, en www.dialnet.unirioja.es: file:///Users/carlosgajero/Downloads/Dialnet-ElFuturoDeLaAlianzaEnUnContextoDeSeguridadExpandid-4768821.pdf

GARCÍA, F., & TIRADO, F. J. (enero de 2022). La Policía Nacional y la financiación a través de los Fondos Europeos. *Policía*(361), 4-15.

GARRIDO FALLA, F. (1959). *Los medios de la policía y la teoría de las sanciones administrativas.* Recuperado el 19 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=2112386

GARRO, I. (2019). Hacia un nuevo multilateralismo que impulse los ODS. En G. d. España (Ed.), *La Agenda 2030 y los ODS: nueva arquitectura para la seguridad* (págs. 65-86). Madrid.

GERASIMOV, V. (27 de febrero de 2013). *НОВОСТИ ВПК.* Recuperado el 3 de mayo de 2024, de https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html

Ediciones Universidad de Salamanca | CC BY-NC-ND

GIANNOPOULOS, G., SMITH, H., & THEOCHARIDOU, M. (5 de febrero de 2021). *The Landscape of Hybrid Threats: A Conceptual Model.* Recuperado el 26 de agosto de 2024, de Hybrid CoE, en https://www.hybridcoe.fi: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

GIRÓN TOMÁS, M. (mayo de 2017). *Análisis de la Ley de Seguridad Nacional en España como ley de seguridad integral. Propuesta de la inclusión de la seguridad en las vías terrestres como ámbito de especial interés para la seguridad nacional.* Recuperado el 26 de diciembre de 2024, de Revista del Instituto Español de Estudios Estratégicos, en https://revista.ieee.es: https://revista.ieee.es/article/view/194/320

GISEL, L., RODENHÄUSER, T., & DÖRMANN, K. (marzo de 2021). *Veinte años después: el derecho internacional humanitario y la protección de las personas civiles de los efectos de las ciberoperaciones durante los conflictos armados.* Recuperado el 14 de abril de 2023, de International Review of the Red Cross, en https://international-review.icrc.org: https://international-review.icrc.org/es/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913

GÓMEZ CASTRO, E. (2017). Introducción. En *OTAN:presente y futuro - Cuadernos de Estrategia 191* (págs. 9-14). Madrid: Ministerio de Defensa - Instituto Español de Estudios Estratégicos.

GÓMEZ PATIÑO, D. P. (Julio-diciembre de 2011). El pacto global de las Naciones Unidas: sobre la responsabilidad social, la anticorrupción y la seguridad. *Revista Prolegómenos - Derechos y Valores, 14*(28), 217-231.

GONZÁLEZ HERNÁNDEZ, E. (enero de 2019). *Interés general de España.* Recuperado el 24 de enero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=6876354

GONZÁLEZ MONTES, Á. (17 de Octubre de 2024). *La gran desconexión: jóvenes, TikTok y el futuro de nuestras democracias.* Recuperado el 17 de Noviembre de 2024, de Agenda Pública, en https://agendapublica.es/: https://agendapublica.es/noticia/19403/gran-desconexion-jovenes-tiktok-futuro-nuestras-democracias

GÖRLITZ, A. (1980). *Diccionario de Ciencia Política.* Madrid: Alianza.

GRANDE-MARLASKA, F., LESMES SERRANO, C., ÓNEGA LÓPEZ, F., SEGARRA CRESPO, M., SILVA AMADOR, L., & URREA CORRES, M. (2019). *Policía Nacional y Constitución española.* Madrid: Fundación Policía Española.

GRAVES, L., & CHERUBINI, F. (23 de noviembre de 2016). *The rise of fact-checking sites in Europe.* Recuperado el 11 de octubre de 2024, de Reuters Institute for the Study of Journalism, en https://reutersinstitute.politics.ox.ac.uk: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/The%2520Rise%2520of%2520Fact-Checking%2520Sites%2520in%2520Europe.pdf

GUEHAM, F. (febrero de 2017). *Digital sovereignty - steps towards a new system of internet governance.* Recuperado el 8 de febrero de 2024, de Fondation pour l`innovation politique, en www.fondapol.org: https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/

Ediciones Universidad de Salamanca | CC BY-NC-ND

GUILLÓ ROT , R. (11 de abril de 2024). *Desinformación con potencial desestabilizador.* Recuperado el 27 de octubre de 2024, de Instituto Español de Estudios Estratégicos, en https://revista.ieee.es/: https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/boletin_ieee_34.pdf

GUTIÉRREZ DE LEÓN, B. (31 de julio de 2021). *Amenazas híbridas y zona gris. OTAN, Unión Europea y España ante esta nueva forma de enfrentamiento.* Recuperado el 2 de mayo de 2024, de Global Strategy, en https://global-strategy.org: https://global-strategy.org/amenazas-hibridas-y-zona-gris-otan-union-europea-y-espana-ante-esta-nueva-forma-de-enfrentamiento/

GUTIÉRREZ DE LEÓN, B. (30 de marzo de 2022). *Entendiendo las estrategias híbridas.* Recuperado el 5 de mayo de 2024, de Global Strategy, en www.global-strategy.org: https://global-strategy.org/entendiendo-las-estrategias-hibridas/

HEGEL, G. (1965). Filosofía del Derecho. En W. EBENSTEIN, *Los grandes pensadores políticos. De Platón hasta hoy* (E. TIERNO GALVAN, Trad., págs. 738-748). Madrid: Revista de Occidente.

HERNÁNDEZ GARCÍA, L. A. (febrero de 2024). *Tecnologías de alto impacto para la defensa en el entorno operativo 2035: introducción.* Recuperado el 8 de marzo de 2024, de Ministerio de Defensa, en https://publicaciones.defensa.gob.es: https://publicaciones.defensa.gob.es/tecnologias-de-alto-impacto-para-la-defensa-en-el-entorno-operativo-2035-libros-pdf.html

HERRERO FERNÁNDEZ-QUESADA, M. D., & TURRADO VIDAL, M. (2023). *Los origenes de la Policía Española. Dos siglos al servicio de la sociedad (1824-2024)* (Primera edición (junio 2023) ed.). (B. O. Ministerio del Interior, Ed.) Madrid: Boletín Oficial del Estado.

HOBBES, T. (2013). *Leviathan o la materia, forma y poder de una República eclesiástica y civil.* (E. TIERNO GALVÁN, Ed., S. DIAZ HELLIN SEPULVEDA, A. CATRYSSE, & M. SANCHEZ SARTO, Trads.) Madrid: Tecnos.

HORCADA RUBIO, I. (2017). Futuro de la transformación en la Alianza. En *OTAN:presente y futuro* (Vol. Cuadernos de Estrategia 191, págs. 83-118). Ministerio de Defensa.

HUNTINGTON, S. (1997). *El choque de civilzaciones y la reconfiguración del orden mundial.* (J. TOSAUS ABADIA, Trad.) Barcelona: Paidós Ibérica S.A.

JELLINEK, G. (2000). *Teoría general del Estado.* (F. DE LOS RIOS, Trad.) México D.F.: Fondo de Cultura Económica.

JIMÉNEZ OLMOS, J. (4 de septiembre de 2013). *La Estrategia de Seguridad Nacional 2013.* Recuperado el 19 de febrero de 2024, de Cátedra Paz, Seguridad y Defensa de la Universidad de Zaragoza, en https://catedrapsyd.unizar.es: https://catedrapsyd.unizar.es/en/archivos/obs_opina/javier_jimenez_04_09_2013.pdf

JORDÁN ENAMORADO, J. (2018). *El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo.* Recuperado el 29 de abril de 2024, de Dialnet, en www.dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=6733549

JORDÁN ENAMORADO, J. (6 de mayo de 2019). *Cómo contrarrestar estrategias híbridas.* Recuperado el 2 de mayo de 2024, de Global Strategy, en

Ediciones Universidad de Salamanca | CC BY-NC-ND

www.global.strategy.org: https://global-strategy.org/como-contrarrestar-estrategias-hibridas/
JORDÁN ENAMORADO, J. (3 de marzo de 2020). *La escalada en las estrategias híbridas y en el conflicto en la zona gris.* Recuperado el 4 de mayo de 2024, de Global Strategy, en www.global-strategy.org: https://global-strategy.org/la-escalada-en-las-estrategias-hibridas-y-en-los-conflictos-en-la-zona-gris/
JORDÁN ENAMORADO, J. (29 de julio de 2022). *La disuasión en la zona gris: una exploración teórica.* (R. E. Política, Ed.) Recuperado el 2 de mayo de 2024, de Dialnet, en www.dialnet.unirioja.es: https://doi.org/10.21308/recp.59.03
JORDANA DE POZAS, L. (1949). Ensayo de una teoría del fomento en el Derecho Administrativo. *Revista de Estudios Políticos*(48), 41-54.
JORDANA DE POZAS, L. (1951). El problema de los fines de la actividad administrativa. *Revista de Adminstración Pública*(4), 11-28.
JURI, Y. E. (2019). Teología y ley natural en la concepción de la soberanía de Jean Bodin. *Enfoques, XXXI*(2), 69-86.
KALENSKY, J., & OSADCHUK, R. (24 de Enero de 2024). *Informe de investigación híbrido del CoE n.° 11: Cómo Ucrania lucha contra la desinformación rusa: colmena contra mamut.* Recuperado el 22 de Noviembre de 2024, de Hybrid CoE, en https://www.hybridcoe.fi/publications: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-11-how-ukraine-fights-russian-disinformation-beehive-vs-mammoth/
KLEY, A. (2010). Monopolio Estatal de la Violencia Origen y futuro en términos de historia de las ideas. *Pensamiento Jurídico*(28), 219-236.
KRAHMANN, E. (2009). *Private security companies and the state monopoly on violence: a case of norm change?* . (8. PRIF Reports, Productor, & Frankfurt am Main: Hessische Stiftung Friedens- und Konfliktforschung.) Recuperado el 20 de marzo de 2023, de SSOAR Open Access Repository : https://nbn-resolving.org/urn:nbn:de:0168-ssoar-292745
LABORIE IGLESIAS, M. (28 de 01 de 2010). *La cooperación OTAN-UE en el futuro concepto estratégico de la Alianza Atlántica.* Recuperado el 14 de octubre de 2023, de Real Instituto Elcano, en www.realinstitutoelcano.org: https://media.realinstitutoelcano.org/wp-content/uploads/2010/01/ari25-2010-lobirie-cooperacion-otan-ue-concepto-estrategico.pdf
LABORIE IGLESIAS, M. (1 de junio de 2011). *La evolucion del concepto de seguridad.* Recuperado el 7 de mayo de 2023, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf
LABORIE IGLESIAS, M. (2011). La evolución del concepto de seguridad. *Documento marco 05/2011 del Instituto Español de Estudios Estratégicos*(Pre-bie 3, número 3, 2011). Obtenido de https://dialnet.unirioja.es
LABORIE IGLESIAS, M. (2013). *La privatización de la seguridad. Las empresas militares y de seguridad privadas en el entorno estratégico actual.* Ministerio de Defensa. Secretaría General Técnica.
LAPUENTE, V., COSTAS, E., CORTINA, A., HIDALGO, M., PARRADO, S., SIMÓN, P., . . . VILLORIA, M. (2020). *Cómo salvar las democracias liberales.* Recuperado el 6 de octubre de 2024, de Círculo de empresarios, en

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://circulodeempresarios.org/: https://circulodeempresarios.org/app/uploads/2020/06/Libro-Democracias-Liberales-OK-paginas.pdf

LAQUEUR, W. (2003). *Una historia del terrorismo.* (T. FERNANDEZ AUZ, & B. EGUIBAR, Trads.) Barcelona: Paidós Ibérica.

LASOEN, K. (diciembre de 2022). *Realising the EU Hybrid Toolbox: opportunities and pitfalls.* Recuperado el 28 de agosto de 2024, de Clingendael; Netherlands Institute of International Relations, en www.clingendael.org: https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf

LEJARZA ILLARO, E. (15 de septiembre de 2015). *Terrorismo islamista en las redes - La yihad electrónica.* Recuperado el 25 de marzo de 2024, de Dialnet, en www.dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=7687270

LEVITSKY, S., & ZIBLAT, D. (2021). *Cómo mueren las democracias* (Quinta edición (junio 2023) ed.). (G. DEZA GUIL, Trad.) Barcelona: Planeta.

LÓPEZ CORDÓN, M. (1982). España en las Conferencias de La Haya de 1899 y 1907. *Revista de Estudios Internacionales*(3), 703-708.

LÓPEZ GUERRA, L. (1983). *Prólogo de la Constitución Española de 1978* (4ª edición ed.). Madrid: Tecnos.

LUCAS MURILLO DE LA CUEVA, P. (2021). *Estudio introductorio. Presente y futuro de la Constitución Española de 1978.* Madrid: Reus.

LUENGO ALFONSO, L. (Enero-febrero de 2000). Cooperación policial en la Unión Europea. (M. d.-D. Policía, Ed.) *Ciencia Policial*(52), 121-132.

MALONE, D., & DAY, A. (2021). *La organización de las Naciones Unidas a los 75 años. Cómo los retos de hoy configurarán los siguientes 25 años.* Recuperado el 17 de febrero de 2024, de SciELO Mexico, en www.scielo.org: https://www.scielo.org.mx/pdf/fi/v61n3/0185-013X-fi-61-03-581.pdf

MANGAS MARTÍN, A., & LIÑÁN NOGUERAS, D. J. (noviembre de 2016). *Instituciones y Derecho de la Unión Europea* (9ª edición ed.). Tecnos.

MAQUIAVELO, N. (1994). *El Príncipe.* (E. LEONETTI JUNGL, Trad.) Madrid: Espasa Calpe.

MARAÑÓN GÓMEZ, R., & ARÉVALO GUTIÉRREZ, A. (2019). Introducción a la Constitución española de 1978. Recuperado el 19 de febrero de 2024, de https://bv.unir.net:2610/#!/search?bookMark=eNqFzEsOgjAUheFrfETR7sABGzDphVLpVILRxKFzUqDGRtIa2i7AuD0WJQPmDs__JScCIoN_KuN1I71qZxDlDNOEUc74HIg45tNOKF9BhJgKJnLk-RqIc7qmo7BU0GwD2dX43rahabQdPiaWcSfjwhrntQ9TU-4tzfC1o7QqxvF-B8uH7JwisPB9UFvYn8t7cTkEo_tK1da-XFXeToj

MARAVALL CASESNOVES, J. (1986). *Estado Moderno y mentalidad social (Siglos XV a XVII)* (1ª ed., Vol. II). Madrid: Alianza.

MARTÍN REBOLLO, L. (2012). *Constitución Española (Texto y contexto).* Cizur Menor (Navarra): Aranzadi.

MARTÍNEZ ATIENZA, G. (2020). *La defensa nacional y su protección penal.* (E. Experiencia, Ed.) Recuperado el 20 de febrero de 2024, de Universidad de la Rioja, en https://bv.unir.net: https://bv.unir.net:2769/es/ereader/unir/167810

Ediciones Universidad de Salamanca | CC BY-NC-ND

MARTÍNEZ QUINTEIRO, M. E. (2018). *La expansividad del discurso sobre el "derecho humano de seguridad", un "derecho síntesis". Concreciones y etiología.* (U. d. Salamanca, Ed.) doi:http://dx.doi.org/10.14201/shhc2018363570

MARTÍNEZ VALERA, G. (1 de febrero de 2021). *China: Zona gris y confrontación de modelos políticos.* Recuperado el 3 de mayo de 2024, de Global Strategy, en www.global-strategy.org: https://global-strategy.org/china-zona-gris-y-confrontacion-de-modelos-politicos/

MASLOW, A. H. (2007). *El hombre autorrealizado. Hacia una psicología del Ser.* (R. RIBE, Trad.) Barcelona: Editorial Kairós.

MATTIS, J., & HOFFMAN, F. (noviembre de 2005). *Future Warfare: The Rise of Hybrid Wars.* Recuperado el 7 de marzo de 2024, de U.S. Naval Institute, en https://www.usni.org: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

MAYER, S., & WEINLICH, S. (2007). Internationalization of intervention? UN and EU security politics and the modern state. En A. HURRELMANN, S. LEIBFRIED, K. MARTENS, & P. MAYER, *Transforming the Golden-Age Nation State* (págs. 42-62). London: Palgrave Macmillan.

MEINECKE, F. (2014). *La idea de la razón de Estado en la Edad Moderna* (4ª edición ed.). (E. D. Calles, Ed., & F. GONZALEZ VICEN, Trad.) Madrid, España: Centro de Estudios Políticos y Constitucionales.

MEJÍA MOLINA, D. (Enero de 2009). Efectos para Colombia de los debates en torno a la seguridad del Estado y a la seguridad humana. (U. ICESI, Ed.) *CS*(3), 109-123.

MÉNDEZ CHANG, E. (2017). El reto de la ONU frente a la solución pacífica de las controversias internacionales. *Derecho y Sociedad*(49).

MIGUEL-GIL, J. (2023). La ciberguerra: conceptualización e implicaciones estratégicas. En A. BUENO, & G. COLOM PIELLA, *La transformación de la guerra en el siglo XXI. Estudios estratégicos para su comprensión* (Primera ed.). Madrid: Universidad Nacional de Educación a Distancia.

MILLER, G., & MEKKENNET, S. (20 de noviembre de 2015). *Inside the surreal world of the Islamic State´s propaganda machine.* Recuperado el 23 de marzo de 2024, de The Washington Post, en www.washingtonpost.com: https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b_story.html

MIRALLES CASTELLANOS, A. (2003). Naciones... Unidas? *Nómadas*(19), 200-207.

MOLINAS, C., & RAMÍREZ MAZARREDO, F. (2017). *La crisis existencial de Europa* (1ª edición (noviembre 2017) ed.). Barcelona: Centro Libros PAPF, SLU - Deusto - Grupo Planeta.

MOLOEZNIK GRUER, M. (2019). Seguridad interior, un concepto ambiguo. *Ius: Revista del Instituto de Ciencias Jurídicas de Puebla*, 149.

MONAGHAN, S., & et al. (2019). *Countering Hybrid Warfare.* MCDC Countering Hybrid Warfare Project - UK Gov.

MONAGHAN, S., & McDONALD, T. (octubre de 2023). *Campaigning in the Grey Zone. Towards a Systems Approach to Countering Hybrid Threats.* Recuperado el 30 de abril de 2024, de The Hague Centre for Strategic Studies, en https://hcss.nl:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://hcss.nl/report/campaigning-grey-zone-towards-systems-approach-countering-hybrid-threats/
MONGARDINI, C. (2007). *Miedo y sociedad.* (J. LINARES DE LA PUERTA, Trad.) Madrid: Alianza Editorial.
MONTOYA BARREIROS, M. (19 de enero de 2023). *El orden mundial*. Recuperado el 26 de marzo de 2024, de www.elordenmundial.com: https://elordenmundial.com/que-es-destruccion-mutua-asegurada/
MORA BENAVENTE, E. (diciembre de 2017). *La OTAN y la UNIÓN EUROPEA: ¿por fin una cooperación eficaz?* (M. d. Defensa, Ed.) Recuperado el 18 de febrero de 2024, de Dialnet, en www.dialnet.es: https://dialnet.unirioja.es/servlet/articulo?codigo=6317256
MORENO-GIL, V., & SALGADO DE DIOS, F. (3 de abril de 2023). *El cumplimiento del código de principios de la International Fact-Checking Network en las plataformas de verificación españolas. Un análisis cualitativo.* Recuperado el 12 de octubre de 2024, de Revista de Comunicación, en https://revistadecomunicacion.com: https://revistadecomunicacion.com/article/view/2971/2621
MORET MILLÁS , V. (enero-junio de 2017). *La defensa nacional y la Ley de Seguridad Nacional: un nuevo entorno jurídico para la Defensa.* (M. d. Defensa, Ed.) Recuperado el 26 de diciembre de 2024, de Revista Española de Derecho Militar, en https://publicaciones.defensa.gob.es: https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/e/redem_107.pdf
MOYA CÁNOVAS, L. E. (16 de septiembre de 2019). *La Iniciativa Europea de Intervención, la Cooperación Permanente Estructurada e ingeniería institucional francesa.* Recuperado el 1 de noviembre de 2023, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO79_2019LUIMOY_UEDef.pdf
MOYNIHAN, H. (17 de diciembre de 2020). *La aplicación del derecho internacional a los ciberataques estatales. Soberanía y no intervención.* Recuperado el 22 de marzo de 2024, de Chatham House, en https://www.chathamhouse.org: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/7-conclusions-and-recommendations
MUJICA RUIZ, G., BARBOSA DE MIGUEL, B., GARCÍA ALAS, T., & MARTÍN PÉREZ, A. (junio de 2017). Europol: una idea antigua de plena actualidad. (M. d.-D. Policía, Ed.) *Policía*(311), 25-28.
MUÑOZ MARTINEZ, M. (16 de noviembre de 2022). *Estrategia de la Unión de la seguridad de la Unión Europea.* Recuperado el 11 de diciembre de 2023, de Instituto Español de Estudios Estratégicos, en https://www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_investig/2022/DIEEEINV05_2022_EstrategiasdeSeguridad.pdf
NIETO FERNÁNDEZ, I. (junio de 2012). *Revolución en asuntos militares (RAM).* Recuperado el 31 de marzo de 2024, de Dialnet, en www.dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=4025116
NIETO FERNÁNDEZ, I. (17 de octubre de 2021). *El papel de las Fuerzas Armadas en la zona gris.* Recuperado el 12 de mayo de 2024, de Global Strategy, en

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://global-strategy.org/: https://global-strategy.org/el-papel-de-las-fuerzas-armadas-en-la-zona-gris/
NIMMO, B. (septiembre de 2020). *The Breakout Scale: measuring the impact of influence operations.* Recuperado el 24 de noviembre de 2024, de Brookings Institution, en https://www.brookings.edu: https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations/
NÚÑEZ VILLAVERDE, J. A. (2022). *Cambios geoestratégicos: una visión europea.* Recuperado el 18 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=8520853
NYE, J. (2004). *Soft Power: the means to success in world politics* (1ª edición ed.). New York, United States of America: PublicAffairs.
OTERO SORIANO, J. (2011). Policía científica y cooperación policial internacional. El Tratado de Prüm. En *La seguridad en Europa tras el Tratado de Lisboa* (págs. 121-127). Madrid: Fundación Policía Española.
OTTONE, E. (2017). *Civilización o barbarie. Ensayo sobre la convivencia global.* Santiago de Chile: Fondo de Cultura Económica.
OUTRIVE, L. (junio de 2001). *Historia del Acuerdo y del Convenio de Schengen.* Recuperado el 18 de febrero de 2024, de CIDOB Barcelona Centre For International Affairs, en https://www.cidob.org/: https://www.cidob.org/es/articulos/revista_cidob_d_afers_internacionals/historia_del_acuerdo_y_del_convenio_de_schengen
PALACIO, A. (2020). Prologue: European Defence and Security at a Time of Global Mutation. En J. B. J. Martín Ramírez (Ed.), *European Defence and Security at a Time of Global Mutation.* Cham, Switzerland: Springer.
PARDO DE SANTAYANA, J. (17 de diciembre de 2024). *La inteligencia artificial y la guerra de Ucrania.* Recuperado el 16 de enero de 2025, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=9666375
PARIS, R. (2004). *At war´s end. Building peace after civil conflict* (Primera ed.). United States of America: Cambridge University Press.
PAVÓN PÉREZ, J. A. (1999). El Acta Fundacional OTAN-Rusia: ¿un nuevo desafío para la seguridad Europea en el umbral del Siglo XXI? *Anuario de la Facultad de Derecho. Universidad de Extremadura*(17), 215-232.
PEREIRA MENAUT, A. (2001). *Después de la soberanía.* Recuperado el 7 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=57302
PÉREZ RUBALCABA, A. (2011). Conferencia inaugural Curso Verano El Escorial 2011. En *La seguridad en Europa tras el Tratado de Lisboa* (págs. 13-18). Madrid: Fundación Policía Española.
PÉREZ TRIANA, J. (2023). La "otra" guerra: la guerra de Ucrania en las redes sociales. En B. CÓZAR MURILLO, & G. COLOM PIELLA, *La guerra de Ucrania II. De la conquista de Lugansk a la contraofensiva ucraniana.* Madrid: Los libros de la catarata.
PETERS, G., & PIERRE, J. (2005). ¿Por qué ahora el interés por la gobernanza? En A. C. Martínez, *La gobernanza hoy: 10 textos de referencia* (págs. 37-56). Madrid: Instituto Nacional de Administración Pública.

Ediciones Universidad de Salamanca | CC BY-NC-ND

POHLE, J., & THIEL, T. (17 de diciembre de 2020). *Digital Sovereignty.* doi:https://doi.org/10.14763/2020.4.1532

PONS RAFOLS, X. (junio de 2022). La Guerra de Ucrania, las Naciones Unidas y el Derecho Internacional: algunas certezas sistémicas insostenibles. *Revista electrónica de estudios internacionales*(43). doi:10.17103/reei.43.08

PULIDO PULIDO, G. (2023). El espacio y la guerra multidominio y mosaico en Ucrania. En B. CÓZAR MURILLO, & G. COLOM PIELLA, *La guera de Ucrania II. De la conquista de Lugansk a la contraofensiva ucraniana.* Madrid: Los libros de la catarata.

RAMÍREZ, A. (2005). *Estrategias sociales de policía.* Madrid: Dykinson.

RAMONET, I. (2022). *La era del conspiracionismo. Trump, el culto a la mentira y el asalto al Capitolio.* Madrid: Siglo Veintiuno - Clave Intelectual.

REAL, B. (11 de Septiembre de 2011). *La cuestión de la representación única de la Unión Europea en el Consejo de Seguridad de las Naciones Unidas.* Recuperado el 18 de febrero de 2024, de Universidad de Navarra, en https://dadun.unav.edu: https://dadun.unav.edu/bitstream/10171/34871/4/AEDI%2027-2011.pdf

RICO, J. (1983). El poder discrecional de la policía y su control. En J. M. Rico, & A. Editorial (Ed.), *Policía y sociedad democrática.* Madrid: Dirección de la Seguridad del Estado - Ministerio del Interior.

RICO, J. (1983). Presupuesto para una reforma de la policía. En J. M. Rico, & A. Editorial (Ed.), *Policía y sociedad democrática.* Madrdid: Dirección de la Seguridad del Estado.

RICO, J., & SALAS CALERO, L. (1988). *Inseguridad ciudadana y Policía.* Madrid: Tecnos. Recuperado el 19 de febrero de 2024

RID, T. (2021). *Desinformación y guerra política.* (Y. FONTAL, Trad.) Barcelona: Planeta.

RIDAURA MARTÍNEZ, M. J. (diciembre de 2014). La seguridad ciudadana como función del Estado. *Estudios de Deusto, 6*(2), 319-346.

RIVAS LARA, L. (2007). El terrorismo en la España contemporánea. El caso del anarquismo. En *Reflexiones sobre el terrorismo en España* (págs. 227-259). Madrid: Fundación Policía Española.

ROMERO JUNQUERA, A. (12 de abril de 2023). *Estrategia Europea de Seguridad Marítima. Seguimos navegando en régimen de "avante poca".* Recuperado el 14 de enero de 2024, de Instituto Español de Estudios Estratégicos, en www.ieee.es/: https://www.ieee.es/en/Galerias/fichero/docs_analisis/2023/DIEEEA26_2023_ABEROM_Estrategia.pdf

RUBIO DAMIÁN, F. (diciembre de 2012). *Necesidad de una nueva Estrategia Europea de Seguridad.* Recuperado el 22 de octubre de 2023, de Universidad de Zaragoza, en http://catedrapsyd.unizar.es: http://catedrapsyd.unizar.es/archivos/documentacion/necesidad_de_una_nueva_ees.pdf

RUBIO MUÑOZ, T. (2006). El integrismo islamista en España después del 11-M. En *Islamismo, democracia y seguridad.* Ministerio de Defensa.

RUBIO NUÑEZ, R. (11 de diciembre de 2024). *Corta el cable rojo. Anular las elecciones en tiempos de desinformación.* Recuperado el 13 de diciembre de 2024, de Letras Libres, en https://letraslibres.com:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://letraslibres.com/politica/corta-el-cable-rojo-anular-las-elecciones-en-tiempos-de-desinformacion/11/12/2024/
RUBIO NUÑEZ, R., FRANCO ALVIM, F., & DE ANDRADE MONTEIRO, V. (2024). *Inteligencia artificial y campañas electorales algorítmicas. Disfunciones informativas y amenazas sistémicas de la nueva comunicación política.* Madrid: Centro de Estudios Políticos y Constitucionales.
RUSHKOFF, D. (2000). *Coerción. Por qué hacemos caso a lo que nos dicen.* Barcelona: La Liebre de Marzo.
SABATER QUINTO, F., BELMONTE MARTÍN, I., & LLORET IRLES, D. (1 de enero de 2025). *Respuestas públicas a la desinformación en la UE y España (2015-2023): una cuestión abierta.* Recuperado el 2 de marzo de 2025, de Universidad de Alicante. Revista Mediterránea de Comunicación, en https://rua.ua.es: https://rua.ua.es/dspace/bitstream/10045/150323/1/ReMedCom_16_01_27371_ES.pdf
SALAZAR ALBORNOZ, M. (25 de octubre de 2022). *El Derecho internacional aplicable al ciberespacio.* Recuperado el 10 de abril de 2024, de OEA - Organización de Estados Americanos, en https://www.oas.org: https://www.oas.org/es/sla/cji/docs/CJI-doc_671-22_rev2_ESP.pdf
SANAHUJA, J. A. (2019). La Agenda 2030 y los ODS: sociedades pacíficas, justas e inclusivas como pilar de la seguridad. En G. d. España (Ed.), *La Agenda 2030 y los ODS: Nueva arquitectura para la seguridad.* Madrid.
SÁNCHEZ BARRILAO, J. (mayo-agosto de 2020). *Sociedad del miedo y desafección constitucional.* Recuperado el 26 de noviembre de 2024, de Uned, Revista de Derecho Político, en https://revistas.uned.es: https://revistas.uned.es/index.php/derechopolitico/article/view/27995
SÁNCHEZ HERRÁEZ, P. (2022). *El Sahel: epicentro yihadista en África Occidental.* Recuperado el 17 de marzo de 2024, de Dialnet, en www.dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=8756243
SÁNCHEZ PELÁEZ, L. (1 de junio de 2021). *El COSI, una década dedicada a la política de seguridad interior de la Unión Europea.* Recuperado el 18 de febrero de 2024, de Revista del Instituto Español de Estudios Estratégicos, en https://revista.ieee.es/: https://revista.ieee.es/article/view/3735/4888
SANSÓ-RUBERT PASCUAL, D. (2024). *Los servicios de inteligencia al servicio de la sociedad democrática y el orden constitucional.* Barcelona: Atelier.
SANTIAGO OROPEZA, T. (10 de diciembre de 2004). *Kant y su proyecto de una paz perpetua (en el bicentenario de su muerte).* Recuperado el 12 de septiembre de 2023, de Revista Digital Universitaria UNAM, en revista.unam.mx: https://www.revista.unam.mx/vol.5/num11/art77/dic_art77.pdf
SCHILDE, K., ANDERSON, S., & GARNER, A. (7 de mayo de 2019). *A more martial Europe? Public opinion, permissive consensus, and EU defence policy.* Recuperado el 30 de octubre de 2023, de Routledge Taylor & Francis Group, en https://www.tandfonline.com/: https://doi.org/10.1080/09662839.2019.1617275
SCHMITT, M. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (1ª 2017 ed.). New York: Cambridge University Press.
SCHMITT, M. (22 de julio de 2022). *The law of cyber conflict: quo vadis?* Recuperado el 7 de abril de 2024, de Lieber Institute West Point, en

Ediciones Universidad de Salamanca | CC BY-NC-ND

www.lieber.westpoint.edu: https://lieber.westpoint.edu/law-cyber-conflict-quo-vadis/

SENSERRICH SOGUES, R. (2024). *Por qué se rompió Estados Unidos. Populismo y polarización en la era Trump* (Primera edición ed.). Barcelona: Penguin Random House.

SERRA CRISTÓBAL, R. (20 de abril de 2015). *La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional.* Recuperado el 24 de marzo de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=5050060

SERRA CRISTÓBAL, R. (20 de marzo de 2023). *Noticias falsas (fake news) y derecho a recibir información veraz. Dónde se fundamenta la posibilidad de controlar la desinformación y cómo hacerlo.* Recuperado el 12 de junio de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=8859896

SIMANCAS, M. (2003). El espacio de libertad, seguridad y justicia. *Ciencia Policial, 67*, 35-47.

STEFFEK, J. (2007). Breaking the Nation State Shell: Prospect for Democratic Legitimacy in the International Domain. En S. L. Achim Hurrelmann, *Transforming The Golden-Age Nation State* (págs. 109-129). London: Palgrave Macmillan.

SUN TZU. (2007). *El arte de la guerra* (5ª ed.). (N. TUCCI, Trad.) Madrid: Ediciones Librería Argentina.

TANDOC , E., THOMAS, R., & BISHOP, L. (3 de febrero de 2021). *What Is (Fake) News? Analyzing News Values (and More) in Fake Stories.* Recuperado el octubre de 6 de 2024, de Cogitatiopress, en https://www.cogitatiopress.com/: https://www.cogitatiopress.com/mediaandcommunication/article/view/3331

TAPIA ROJO, M. (4 de enero de 2016). *Instituto Español de Estudios Estratégicos.* Recuperado el 24 de marzo de 2024, de www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO02-2016_Comunicacion_ISIS_EugeniaTapia.pdf

TOCQUEVILLE, A. (1980). *La democracia en América. Ed. Alianza. Madrid, 1980. Pag. 54-57.* Madrid: Alianza.

TORRES CAZORLA, M. (2008). *El derecho de veto en el Consejo de Seguridad de Naciones Unidas la historia de la válvula de seguridad que paralizó el sistema. Dialnet.* Recuperado el 26 de marzo de 2024, de www.dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=4941863

TORRES SORIANO, M. (12 de enero de 2017). *Lecciones aprendidas de la lucha contra el yihadismo en Internet.* Recuperado el 24 de marzo de 2024, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO04-2017_Lucha_Yihadismo_Internet_MRTorres.pdf

TORRES SORIANO, M. (2023). La guerra de Ucrania y su impacto sobre la teoría y práctica de la ciberguerra. En G. COLOM PIELLA, & J. BAQUÉS QUESADA, *El entorno estratégico tras la guerra de Ucrania.* Tirant Lo Blanch.

TURRADO VIDAL, M. (Diciembre de 2020). La Segunda República. (D. G. Policía, Ed.) *Policía*(349), 44 a 49.

TURRADO VIDAL, M. (Febrero de 2021). La etapa democrática. (D. G. Policía, Ed.) *Policía*(351), 40 a 45.

Ediciones Universidad de Salamanca | CC BY-NC-ND

TURRADO VIDAL, M. (ENERO de 2021). La Policía en época franquista. *Policía*(350), 44 a 49.

TURRADO VIDAL, M. (Enero de 2023). 1824: La Policía Nacional una Institución sin fisuras. (D. G. Policía, Ed.) *Revista Policía*(372), 42 a 47.

UGARTEMENDIA ECEIZABARRENA, J. (mayo-agosto de 2006). *El concepto y alcance de la seguridad jurídica en el Derecho constitucional español y en el Derecho comunitario europeo: un estudio comparado.* Recuperado el 22 de abril de 2024, de Cuadernos de Derecho Público, en https://revistasonline.inap.es: https://revistasonline.inap.es/index.php/CDP/article/view/783/838

URIARTE, E. (2003). *Cobardes y rebeldes. Por que pervive el terrorismo.* Madrid: Temas de hoy.

URREA CORRES, M. (enero - marzo de 2016). *Las cláusulas de asistencia mutua y solidaridad tras los atentados de París: la respuesta europea frenta al terrorismo internacional.* Recuperado el 18 de febrero de 2024, de Dialnet, en www.dialnet.unirioja.es: https://www.revistasmarcialpons.es/revistaespanoladerechoeuropeo/article/view/167_clausulas-asistencia-mutua-solidaridad-atentados-paris/184

VAN HEEMSTRA FERNÁNDEZ, A. (Abril-junio de 2023). *La desinformación como amenaza para la democracia: el caso del Brexit.* Recuperado el Octubre de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=9212587

VAN MIDDELAAR, L. (15 de abril de 2021). *El despertar geopolítico de Europa.* (Le Groupe d'études géoplitiques, Ed.) Recuperado el 11 de noviembre de 2023, de Groupe d´tudes géopolitiques, en htpps://geopolitique.eu: https://geopolitique.eu/en/2021/04/15/europes-geopolitical-awakening/

VARGAS VILLAMIZAR, C. (31 de 12 de 2022). *Seguridad multidimensional. Entre la ambigüedad conceptual y la necesidad pragmática.* Recuperado el 8 de 12 de 2024, de Revista de Relaciones Internacionales, Estrategia y Seguridad, en https://revistas.unimilitar.edu.co: https://revistas.unimilitar.edu.co/index.php/ries/article/view/6140/5406

VEIGA GASALLA, J. (1 de abril de 2024). *Comprendiendo las políticas de seguridad. Cultura estratégica como valor.* Recuperado el 2 de abril de 2024, de Instituto Español de Estudios Estratégicos, en www.ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO32_2024_JAVVEI_Cultura.pdf

VILANOVA, P. (2022). La OTAN: retrovisor y luces largas. En I. E. Estratégicos (Ed.), *El futuro de la OTAN tras la cumbre de Madrid 2022* (Vols. Cuadernos de Estrategia 211 - Instituto Español de Estudios Estrategicos). Madrid: Ministerio de Defensa.

VILLALGORDO GARCÍA, J. A. (2011). Una estrategia de seguridad interior para la Unión Europea. En *La Seguridad en Europa tras el Tratado de Lisboa* (pág. 247). Madrid: Fundación Policía Española.

VILLANUEVA LÓPEZ, C. (19 de julio de 2019). *¿Es la "Zona Gris" el nuevo término de moda?* Recuperado el 3 de mayo de 2024, de Grupo de Estudios en Seguridad Internacional - GESI, en www.seguridadinternacional.es: https://www.seguridadinternacional.es/?q=es/content/%C2%BFes-la-%E2%80%9Czona-gris%E2%80%9D-el-nuevo-t%C3%A9rmino-de-moda

Ediciones Universidad de Salamanca | CC BY-NC-ND

VILLENA SÁNCHEZ, F., & AZNAR FERNÁNDEZ MONTESINOS, F. (Julio-agosto de 2022). El conflicto en la zona gris. *Claves de Razón Práctica*(283), 20-29.

WALKOWSKI, D. (31 de julio de 2019). *¿Qué es la tríada de la CIA?* Recuperado el 9 de abril de 2024, de ComputerWeekly, en www.computerweekly.com: https://www.computerweekly.com/es/opinion/Que-es-la-triada-de-la-CIA

WALZER, M. (2001). *Guerras justas e injustas. Un razonamiento moral con ejemplos históricos* (Tercera edición ed.). (T. FERNANDEZ AUZ, & B. EGUIBAR, Trads.) Barcelona: Paidos Ibérica.

WEBER, M. (2007). La Política como profesión. (págs. Pag. 56-57.). Madrid: Ed. Biblioteca Nueva.

World Economic Forum. (enero de 2025). *The Global Risks Report 2025 - 20th Edition.* Recuperado el 24 de enero de 2025, de World Economic Forum, en https://www.weforum.org/: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

ZAMORA NAVARRO, J. (abril-junio de 2016). *La Ley 36/2015, de Seguridad Nacional.* Recuperado el 12 de diciembre de 2024, de Dialnet, en https://dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=5998266

ZAVALETA HERNÁNDEZ, S. K. (Septiembre de 2015). El concepto de seguridad humana en las relaciones internacionales. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 10*(1), 65-87.

ZILLER, J. (enero-junio de 2007). *El Tratado de Prüm.* Recuperado el 18 de febrero de 2024, de Dialnet, en https://dialnet.unirioja.es/: https://dialnet.unirioja.es/servlet/articulo?codigo=2492889

ZIMMERMANN, J. (2007). The Role of the Nation State in the Internationalization of Accounting Regimes. En A. HURRELMANN, S. LEIBFRIED, K. MARTENS, & P. MAYER, *Transforming the Golden-Age Nation State.* England: Palgrave macmillan.

ZURITA, M. D. (2007). *La Guerra Fría en el marco de las Relaciones Internacionales.* Recuperado el 23 de marzo de 2023, de http://secyt.presi.unip.edu.ar/cyt_htm/ebec07/pdf/zurita.pdf

Ediciones Universidad de Salamanca | CC BY-NC-ND

Webgrafía: normativa, informes y documentos oficiales

Normativa, informes y documentos oficiales internacionales

Declaración de Derechos de Virginia, del 12 de junio de 1776. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2698/21.pdf (16/05/2023).

Declaración de los Derechos del Hombre y del Ciudadano, de 26 de agosto de 1789. Disponible en: https://www.conseil-constitutionnel.fr/sites/default/files/2019-02/20190225_derechosdelhombre_1789_0.pdf (16/05/2023).

Carta de las Naciones Unidas. 26 de junio de 1945, San Francisco. Disponible en: https://www.un.org/es/about-us/un-charter (25/03/2024).

23ª reunión del Consejo de Seguridad de NNUU, 16 de febrero de 1946. Disponible en: https://research.un.org/es/docs/sc/quick/meetings/1946 (26/03/2024).

Tratado del Atlántico Norte, 4 de abril de 1949, Washington DC. Disponible en: https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=es (03/08/2023).

Convenios de Ginebra, de agosto de 1949. Disponibles en: https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/state-parties (29/03/2024).

Tratado de Amistad, Colaboración y Asistencia Mutua (Pacto de Varsovia). 14 de mayo de 1955, Varsovia. Disponible en: https://www.dipublico.org/3602/pacto-de-varsovia-1955/ (03/08/2023).

Three Wise Men Report, de 13 de diciembre de 1956, para la coordinación y cooperación no militar entre los aliados de la OTAN. Disponible en: https://www.nato.int/cps/en/natohq/news_139363.htm (14/08/2023).

Primer informe del Secretario General de la OTAN Lord Hasting Lionel Ismay, de mayo de 1957. Disponible en: https://archives.nato.int/uploads/r/null/1/3/137336/0096_Lord_Ismay_Report_North_Atlantic_Council_1957_ENG.pdf (12/08/2023).

Science for Peace and Securty Progamme (SPS), fundado en 1958. Disponible en: https://www.nato.int/cps/en/natohq/topics_85373.htm (14/08/2023).

Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Disponible en: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (29/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Informe sobre las tareas futuras de la Alianza (Informe Harmel), de 12 de diciembre de 1967. Disponible en: https://www.nato.int/cps/en/natohq/topics_67927.htm (22/08/2023).

Cuarto Concepto Estratégico para la Defensa del Área de la Organización del Tratado del Atlántico Norte, de enero de 1968. Disponible en: https://www.nato.int/docu/stratdoc/eng/a680116a.pdf (22/08/2023).

Protocolo Adicional I a los Convenios de Ginebra de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales, de 1977. Disponible en: https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977 (14/04/2024).

Convención de las NNUU sobre el Derecho del Mar, de 1982. Disponible en: https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf (20/03/2024).

Reunión de Moscú de la Conferencia sobre la dimensión humana de la OSCE, de octubre de 1991. Disponible en: https://www.osce.org/files/f/documents/1/a/14315.pdf (02/02/2024).

Un programa de paz. Diplomacia preventiva, establecimiento de la paz y mantenimiento de la paz. A/47/277 de 17 de junio de 1992, del cuadragésimo séptimo período de sesiones de la Asamblea general. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N92/259/64/PDF/N9225964.pdf?OpenElement (26/10/2023).

Resolución de la Asamblea General 48/141, de 7 de enero de 1994. Alto Comisionado para la promoción y la protección de todos los derechos humanos. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N94/012/59/PDF/N9401259.pdf?OpenElement (25/01/2024).

Informe sobre Desarrollo Humano 1994. Programa de las Naciones Unidas para el Desarrollo. Publicado por el Fondo de Cultura Económica. Disponible en: https://hdr.undp.org/system/files/documents/hdr1994escompletonostats.pdf (02/02/2024).

Resolución aprobada por la Asamblea General de Naciones Unidas sobre medidas para eliminar el terrorismo internacional. A/RES/51/210, de 16 de enero de 1997. Disponible en: https://www.un.org/depts/dhl/resguide/r51_resolutions_table_es.htm (10/03/2024).

Resolución aprobada por la Asamblea General -sobre la base del informe de la Primera Comisión (A/53/576)-, relativa a los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/53/70, de 4 de enero de 1999. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F53%2F70&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

Resolución de la Asamblea General de Naciones Unidas de 18 de septiembre de 2000. Declaración del Milenio de las Naciones Unidas. Disponible en: https://documents.un.org/doc/undoc/gen/n00/559/51/pdf/n0055951.pdf?OpenElement (02/02/2024).

Resolución aprobada por la Asamblea General –sobre la base del informe de la Sexta Comisión (A/56/589 y Corr. 1)- Responsabilidad del Estado por hechos internacionalmente ilícitos. A/RES/56/83, de 28 de enero de 2002. Disponible en: https://international.vlex.com/vid/resolucion-aprobada-asamblea-general-248406 (09/04/2024).

Resolución aprobada por la Asamblea General de Naciones Unidas sobre medidas para eliminar el terrorismo internacional. A/RES/59/46, de 16 de diciembre de 2004. Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2005/3461.pdf (10/03/2024).

Asamblea General de las Naciones Unidas, A/59/2005/add.1, de 23 de mayo de 2005. Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos. Informe del Secretario General. Disponible en: https://www2.ohchr.org/spanish/bodies/hrcouncil/docs/gaA.59.2005.Add.1_Sp.pdf (02/02/2024).

Asamblea General de las Naciones Unidas, A/RES/60/01, de 24 de octubre de 2005, Documento Final de la Cumbre Mundial 2005. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/487/63/PDF/N0548763.pdf?OpenElement (02/02/2024).

Resolución aprobada por la Asamblea General de Naciones Unidas el 8 de septiembre de 2006. Estrategia global de las Naciones Unidas contra el terrorismo. A/RES/60/288, de 20 de septiembre de 2006. Disponible en: https://www.un.org/counterterrorism/es/un-global-counter-terrorism-strategy (10/03/2024).

Directiva 2009/81/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009 , sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE. Diario Oficial de la Unión Europea. L 216/76 de 20.8.2009. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32009L0081 (23/03/2025).

Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/65/201, de 30 de

Ediciones Universidad de Salamanca | CC BY-NC-ND

julio de 2010. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F65%2F201&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

Resolución A/RES/66/24 de las Naciones Unidas sobre Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Disponible en: https://documents.un.org/doc/undoc/gen/n11/460/29/pdf/n1146029.pdf?token=KNBRoMvxWIIp1PUtNA&fe=true (22/02/2024).

Resolución aprobada por la Asamblea General el 2 de diciembre de 2011 -sobre la base del informe de la Primera Comisión (A/66/407)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/66/24, de 13 de diciembre de 2011. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F66%2F24&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

Resolución aprobada por la Asamblea General de NNUU el 10 de septiembre de 2012. A/RES/66/290, de 25 de octubre de 2012, sobre el Seguimiento del párrafo 143, relativo a la seguridad humana, del Documento Final de la Cumbre Mundial de 2005. Disponible en: https://www.un.org/es/ga/66/resolutions.shtml (02/02/2024).

Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/68/98*, de 24 de junio de 2013. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F68%2F98&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

Reglamento Financiero y Reglamentación Financiera Detallada de las Naciones Unidas, ST/SGB/2013/4, de 1 de julio de 2013. Disponible en: https://documents.un.org/doc/undoc/gen/n13/408/60/pdf/n1340860.pdf?token=bxdBD7qIsjh7YozNHV&fe=true (26/03/2024).

Resolución aprobada por la Asamblea General el 27 de diciembre de 2013 -sobre la base del informe de la Primera Comisión (A/68/406)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/68/243, de 9 de enero de 2014. Disponible en: https://documents.un.org/doc/undoc/gen/n13/454/06/pdf/n1345406.pdf?token=LwFmQKlkDjKtsaIiTB&fe=true (09/04/2024).

Resolución 2178 (2014) aprobada por el Consejo de Seguridad en su 7272ª sesión, celebrada el 24 de septiembre de 2014. S/RES/2178 (2014). Disponible en: https://www.un.org/securitycouncil/es/s/res/2178-%282014%29 (10/03/2024).

Resolución aprobada por el Consejo de Derechos Humanos 28/16. El derecho a la privacidad en la era digital. Asamblea General. A/HRC/RES/28/16. 1 de abril de 2015.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Disponible en: https://documents.un.org/doc/undoc/gen/g15/068/81/pdf/g1506881.pdf?token=eXb0gJGhrPqnSyVKYd&fe=true (03/03/2024).

Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/70/174, de 22 de julio de 2015. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False (09/04/2024).

Resolución aprobada por la Asamblea General de NNUU 25 de septiembre de 2015. A/RES/70/01, de 21 de octubre de 2015. Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible. Disponible en: https://unctad.org/system/files/official-document/ares70d1_es.pdf (02/02/2024).

Resolución 70/237 de la Asamblea General de NNUU aprobada el 23 de diciembre de 2015. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/70/237. Disponible en: https://www.un.org/es/ga/70/resolutions.shtml (29/02/2024).

Acuerdo de París, firmado en diciembre de 2015 en la Conferencia de las NNUU sobre el Cambio Climático (COP21). Disponible en: https://unfccc.int/sites/default/files/spanish_paris_agreement.pdf (03/11/2023).

Manual de Seguridad Humana. Un enfoque integrado para la consecución de los Objetivos de Desarrollo Sostenible y los ámbitos de acción prioritarios de la comunidad internacional y el sistema de las Naciones Unidas. Fondo Fiduciario de las Naciones Unidas para la Seguridad Humana. Enero de 2016. Disponible en: https://www.un.org/humansecurity/wp-content/uploads/2023/02/HS-handbook-Spanish.pdf (16/03/2024).

MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. January 2017. Disponible en: https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf (02/05/2024).

Resolución aprobada por la Asamblea General de Naciones Unidas el 15 de junio de 2017. Refuerzo de la capacidad del sistema de las Naciones Unidas de ayudar a los Estados miembros en la aplicación de la Estrategia Global de las Naciones Unidas contra el terrorismo. A/RES/71/291, de 19 de junio de 2017. Disponible en: https://documents.un.org/doc/undoc/gen/n17/172/62/pdf/n1717262.pdf (10/03/2024)

Resolución aprobada por la Asamblea General el 5 de diciembre de 2018 -sobre la base del informe de la Primera Comisión (A/73/505)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/73/27, de

Ediciones Universidad de Salamanca | CC BY-NC-ND

11 de diciembre de 2018. Disponible en: https://www.un.org/es/ga/73/resolutions.shtml (09/04/2024).

Resolución aprobada por la Asamblea General el 5 de diciembre de 2018 -sobre la base del informe de la Primera Comisión (A/73/505)-. Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. A/RES/73/266, de 2 de enero de 2019. Disponible en: https://www.un.org/es/ga/73/resolutions.shtml (09/04/2024).

Resolución de la Asamblea General de NNUU de 19 de diciembre de 2018 (73/195). Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/452/03/PDF/N1845203.pdf?OpenElement (18/07/2023).

Resolución de la Asamblea General de 17 de diciembre de 2018 (73/151). Disponible en: https://www.acnur.org/media/oficina-del-alto-comisionado-de-las-naciones-unidas-resolucion-aprobada-por-la-asamblea (20/07/2023).

MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare. March 2019. Disponible en: https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf (02/05/2024).

Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital. Informe del Secretario General. Asamblea General. A/74/821. 29 de mayo de 2020. Disponible en: https://documents.un.org/doc/undoc/gen/n20/102/54/pdf/n2010254.pdf?token=MzAlFTNn7EzLLZ0wkk&fe=true (03/03/2024).

Resolución aprobada por la Asamblea General el 27 de diciembre de 2019. Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Asamblea General. A/RES/74/247, 20 de enero de 2020. Disponible en: https://documents.un.org/doc/undoc/gen/n19/440/32/pdf/n1944032.pdf?token=aLMLC4D6DPQGL1vShC&fe=true (29/02/2024).

Resolución de la Asamblea General de 21 de septiembre de 2020 (A/75/L.1), aprobando la Declaración sobre la conmemoración del 75º aniversario de las Naciones Unidas. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/248/84/PDF/N2024884.pdf?OpenElement (27/10/2023).

Estrategia Europea de Ciberseguridad para la Década Digital. Comisión Europea y Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 16 de diciembre de 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (17/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Proyecto de informe sustantivo (borrador preliminar). A/AC.290/2021/L2, de 19 de enero de 2021. Disponible en: https://documents.un.org/doc/undoc/ltd/n20/378/97/pdf/n2037897.pdf?token=3hbyOaT0dPfWANsJxK&fe=true (09/04/2024).

Resolución aprobada por la Asamblea General el 31 de diciembre de 2020 -sobre la base del informe de la Primera Comisión (A/75/394, párr. 17)-. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/75/240, de 4 de enero de 2021. Disponible en: https://international.vlex.com/vid/res-75-240-resolution-861186671 (09/04/2024).

Developments in the field of information and telecommunications in the context of international security. Note by the Secretary-General. 18 March 2021. A/75/816. Disponible en: https://documents.un.org/doc/undoc/gen/n21/068/72/pdf/n2106872.pdf (01/03/2024).

Informe de la Dependencia Común de Inspección de Naciones Unidas, JIU/REP/2021/3. Disponible en: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf (22/02/2024).

EEAS (2021) 706 REV4. European Union Military Vision and Strategy on Cyberspace as a Domain of Operations. Disponible en: https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf (07/04/2024).

Russia´s Strategy in Cyberspace. NATO Strategic Communications Centre of Excellence & NATO Cooperative Cyber Defence Centre of Excellence. June 2021. Disponible en: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf (05/03/2024).

Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional. A/76/135. 14 de julio de 2021. Disponible en: https://documents.un.org/doc/undoc/gen/n21/075/89/pdf/n2107589.pdf?token=wXs1DUNUVgApEXlef4&fe=true (09/04/2024).

Nuevo Concepto Estratégico de la OTAN. Madrid, 29 de junio de 2022. Disponible en: https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf (22/02/2024).

Resolución A/77/L.5 de la Asamblea General de Naciones Unidas, sobre la necesidad de poner fin al bloqueo económico, comercial y financiero impuesto por los Estados Unidos de América contra Cuba. Nota de prensa y resolución. Disponible en: https://news.un.org/es/story/2022/11/1516617 (12/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Contrarrestar la desinformación para promover y proteger los derechos humanos y las libertades fundamentales. Informe del Secretario General de Naciones Unidas. Asamblea General. 12 de agosto de 2022. A/77/287. Disponible en: https://documents.un.org/doc/undoc/gen/n22/459/27/pdf/n2245927.pdf (23/11/2024).

Air Force Doctrine Publication 3-12. Cyberspace Operations. U.S. Air Force, 1 February 2023. Disponible en: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf (01/04/2024).

Campaigning in the Grey Zone. Towards a Systems Approach to Countering Hybrid Threats. The Hague Centre for Strategic Studies. Octubre 2023. Disponible en: https://hcss.nl/report/campaigning-grey-zone-towards-systems-approach-countering-hybrid-threats/ (30/04/2024).

Directrices para la gobernanza de las plataformas digitales: salvaguardar la libertad de expresión y el acceso a la información mediante un enfoque de múltiples partes interesadas. Publicado en 2023 por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000387360 (23/11/2024).

Our Common Agenda Policy Brief 8: Information Integrity on Digital Platforms. June 2023. Disponible en: https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf (23/11/2024).

Proyecto de Resolución 23-20614 (S) - A/ES-10/L.25, para la protección de los civiles y cumplimiento de las obligaciones jurídicas y humanitarias, por las medidas ilegales israelíes en la Jerusalén Oriental Ocupada y el resto del Territorio Palestino Ocupado, de 26 de octubre de 2023. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/319/23/PDF/N2331923.pdf?OpenElement (30/10/2023).

Resolución aprobada por la Asamblea General el 4 de diciembre de 2023. Programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. A/RES/78/16, de 6 de diciembre de 2023. Disponible en: https://digitallibrary.un.org/record/4029924/files/A_RES_78_16-ES.pdf (09/04/2024).

Principios globales de las Naciones Unidas para la integridad de la información. Recomendaciones para la acción de las partes interesadas. Disponible en: https://www.un.org/sites/un2.un.org/files/principios_globales_onu_integridad_informacion.pdf (23/11/2024).

Resolución 2728 (2024), aprobada por el Consejo de Seguridad en su 9586ª sesión, celebrada el 25 de marzo de 2024. S/RES/2728 (2024). Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.un.org/securitycouncil/es/content/resoluciones-aprobadas-por-el-consejo-de-seguridad-de-las-naciones-unidas-en-2024 (01/04/2024).

Mensaje sobre el lanzamiento de los Principios Universales para la Integridad de la Información. António Guterres. Secretario General de Naciones Unidas. 24 de junio de 2024. Disponible en: https://mexico.un.org/es/272346-mensaje-sobre-el-lanzamiento-de-los-principios-universales-para-la-integridad-de-la (25/10/2024).

Hybrid Threats and Hybrid Warfare Reference Curriculum. NATO Headquarters Brussels, June 2024. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf (23/11/2024).

Proyecto de convención de las Naciones Unidas contra la ciberdelincuencia. Fortalecimiento de la cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves. 7 de agosto de 2024. A/AC291/L15. Disponible en: https://ciberprisma.org/wp-content/uploads/2024/08/v2405509-espanol.pdf (19/09/2024).

Proyecto de Resolución 23-20614 (S) A/ES-10/L.25 para la protección de los civiles y cumplimiento de las obligaciones jurídicas y humanitarias ante las medidas ilegales israelíes en la Jerusalén Oriental Ocupada y el resto del territorio Palestino Ocupado. Disponible en: https://news.un.org/en/story/2023/10/1142932 https://twitter.com/UN_News_Centre/status/1717992371906839005/photo/2 (29/10/2023).

Detección de narrativas y modelado de temas en los países bálticos. 14 de mayo de 2024. Disponible en: https://stratcomcoe.org/publications/narrative-detection-and-topic-modelling-in-the-baltics/303 (22/11/2024).

Manipulación de redes sociales a la venta: Experimento sobre las capacidades de la plataforma para detectar y contrarrestar interacciones no auténticas en las redes sociales. 4 noviembre de 2024. Disponible en: https://stratcomcoe.org/publications/social-media-manipulation-for-sale-experiment-on-platform-capabilities-to-detect-and-counter-inauthentic-social-media-engagement/311 (22/11/2024).

Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. 27 de noviembre de 2024. Asamblea General. A/79/460. Disponible en: https://documents.un.org/doc/undoc/gen/n24/372/07/pdf/n2437207.pdf (14/01/2025).

Normativa, informes y documentos oficiales supranacionales-europeos

Tratado de colaboración en materia económica, social y cultural y de legítima defensa colectiva, firmado en Bruselas el 17 de marzo de 1948, enmendado por el Protocolo por

Ediciones Universidad de Salamanca | CC BY-NC-ND

el que se modifica y completa el Tratado de Bruselas, firmado en París el 23 de octubre de 1954. Disponible en: https://www.dipublico.org/121077/tratado-de-colaboracion-en-materia-economica-social-y-cultural-y-de-legitima-defensa-colectiva-firmado-en-bruselas-el-17-de-marzo-de-1948-y-enmendado-por-el-protocolo-que-modifica-y-completa-el-trat-2/ (29/10/2023).

Tratado de París, constitutivo de la Comunidad Europea del Carbón y del Acero (CECA), firmado el 18 de abril de 1951. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:xy0022 (17/10/2023).

Tratado de Roma, de 25 de marzo de 1957. Disponible en: https://www.europarl.europa.eu/about-parliament/es/in-the-past/the-parliament-and-the-treaties/treaty-of-rome (17/10/2023).

Preámbulo del Tratado constitutivo de la Comunidad Económica Europea, firmado en Roma el 25 de marzo de 1957. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:11957E/TXT (21/10/2023).

Informe Birkelbach, de 19 de diciembre de 1961, sobre los aspectos políticos e institucionales de la adhesión de España a la Comunidad Europea. Disponible en: https://www.cvce.eu/obj/informe_de_willi_birkelbach_sobre_los_aspectos_politicos_e_institucionales_de_la_adhesion_o_de_la_asociacion_a_la_comunidad_19_de_diciembre_de_1961-es-2d53201e-09db-43ee-9f80-552812d39c03.html (22/10/2023).

Acta del Consejo Europeo de Roma de 1975. Disponible en: https://www.consilium.europa.eu/media/20809/1975_december_rome__eng_.pdf (12/11/2023).

Acta del Consejo de Bruselas de 22/07/1976. Disponible en: https://www.consilium.europa.eu/media/20797/bruxelles_july_1976__eng_.pdf (12/11/2023).

Acta Única Europea, firmada en Luxemburgo el 17/02/1986 y en La Haya el 28/02/1986. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:11986U/TXT (21/10/2023).

Convenio de Aplicación del Acuerdo de Schengen, firmado el 19 de junio de 1990. Diario Oficial de la Unión Europea L239/1, Consejo de 22/09/2000. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:42000A0922(02) (15/11/2023).

Tratado de Maastricht, firmado en Maastricht el 7 de febrero de 1992. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:11992M/TXT (21/10/2023).

Acción Común 95/73/JAI, de 10 de marzo de 1995, relativa a la Unidad de Drogas de Europol. Diario Oficial de las Comunidades Europeas L 62 de 20.3.1995. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:l14005a (15/11/2023).

Acto del Consejo, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K3 del Tratado de la Unión, por el que se crea una Oficina Europea de Policía (Convenio Europol). Diario Oficial de las Comunidades Europeas 95/C 316/01, de 27/11/1995 Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995F1127(01) (21/11/2023).

Tratado de Ámsterdam, de 2 de octubre de 1997. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:1997:340:FULL (21/10/2023).

Protocolos anejos al Tratado de la Unión Europea y al Tratado Constitutivo de la Comunidad Europea, de 10 de noviembre de 1997. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:C:1997:340:TOC (21/10/2023).

Declaración de Saint Malo, de 4 de diciembre de 1998. Disponible en: https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf (27/10/2023).

Conclusiones de la Presidencia, Consejo Europeo de Tampere 15 y 16 de octubre de 1999. Disponible en: https://www.europarl.europa.eu/summits/tam_es.htm (18/11/2023).

Acervo de Schengen. Diario Oficial de las Comunidades Europeas DO núm. L239, de 22 de septiembre de 2000. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:2000:239:TOC (21/10/2023).

Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985. Diario Oficial de la Unión Europea L239/1, Consejo de 22/09/2000. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:42000A0922(02) (15/11/2023).

Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de las Comunidades Europeas, 18.12.2000. C 364/1. Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf (07/09/2024).

Tratado de Niza por el que se modifica el Tratado de la Unión Europea, los Tratados Constitutivos de las Comunidades Europeas y determinados actos conexos, firmado en Niza el 26 de febrero de 2001. Publicado en Diario Oficial de las Comunidades Europeas 2001/C 80/01, de 10 de marzo de 2001. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2001:080:FULL&from=PT (18/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Convenio de Budapest sobre la Ciberdelincuencia, de 23 de noviembre de 2001. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/convention-on-cybercrime.html (14/03/2024).

Decisión 2002/187/JAI del Consejo de 28 de febrero de 2002 por la que se crea Eurojust para reforzar la lucha contra las formas graves de la delincuencia. Diario Oficial de las Comunidades Europeas L 63 de 06/03/2002. Disponible en: https://www.boe.es/doue/2002/063/L00001-00013.pdf (25/11/2023).

Decisión Marco del Consejo de 13 de junio de 2002, sobre la lucha contra el terrorismo. 2002/475/JAI. DO L 164 de 22.6.2002. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002F0475:20081209:ES:PDF (10/03/2024).

Proyecto de Tratado por el que se instituye una Constitución para Europa. Diario Oficial de la Unión Europea 2003/C 169/01, de 18 de julio de 2003. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52003XX0718(01)&qid=1700322244878 (18/11/2023).

Orden europea de detención y entrega. Disponible en: https://e-justice.europa.eu/content_european_arrest_warrant-90-es.do (18/11/2023).

Tratado de Atenas, firmado el 16 de abril de 2003. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=OJ%3AL%3A2003%3A236%3ATOC (22/10/2023).

Convenio del Consejo de Europa para la Prevención del Terrorismo, de 16 de mayo de 2005. Diario Oficial de la Unión Europea 22.6.2018, L 159/3. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22018A0622(01)&from=ES (22/03/2024).

Estrategia de la Unión Europea de Lucha contra el Terrorismo, del Consejo de la Unión Europea, 14469/4/05. Bruselas, 30 de noviembre de 2005. Disponible en: https://data.consilium.europa.eu/doc/document/ST%2014469%202005%20REV%204/ES/pdf

Tratado de Lisboa, de 17 de diciembre de 2007. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12007L/TXT (22/10/2023).

Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza. Diario Oficial de la Unión Europea L210/1 de 06/08/2008. Disponible en: eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008D0615 (21/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Decisión 2008/616/JAI, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI. Diario Oficial de la Unión Europea L210/12 de 06/08/2008. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:ES:PDF (21/11/2023).

Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, por la que se modifica la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo. DOUE L 330/21, de 9.12.2008. Disponible en: https://www.boe.es/doue/2008/330/L00021-00023.pdf (10/03/2024).

Preámbulo de D. Javier Solana al "Informe sobre la aplicación de la Estrategia Europea de Seguridad: ofrecer seguridad en un mundo en evolución", de diciembre de 2008. Disponible en: https://www.consilium.europa.eu/media/30808/qc7809568esc.pdf (20/10/2023).

Informe sobre la Aplicación de la Estrategia Europea de Seguridad: ofrecer seguridad en un mundo en evolución. Bruselas 11/12/2008. Disponible en: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/ES/reports/104637.pdf (20/04/2023).

Decisión del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol). Diario Oficial de la Unión Europea 2009/371/JAI L121/37. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:ES:PDF (21/11/2023).

Decisión del Consejo de 25 de febrero de 2010 por la que se crea el Comité permanente de cooperación operativa en materia de seguridad interior. Diario Oficial de la Unión Europea L52/50 de 03/03/2010. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010D0131&qid=1700337686330 (18/11(2023).

Consejo de la Unión Europea, Secretaría General del Consejo, Estrategia de seguridad interior para la Unión Europea – Hacia un modelo de seguridad europeo. Marzo de 2010. Disponible en: https://data.europa.eu/doi/10.2860/87810 (23/11/2023).

Directiva 2010/13/UE del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual. Diario Oficial de la Unión Europea, de 15.4.2010. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010L0013&from=EN (12/10/2024).

Programa de Estocolmo –una Europa abierta y segura que sirva y proteja al ciudadano, del Consejo Europeo. Diario Oficial de la Unión Europea 2010/C 115/01, de 04/05/2010. Disponible en: https://eur-

Ediciones Universidad de Salamanca | CC BY-NC-ND

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:es:PDF (23/11/2023).

Programa de Seguimiento de la Financiación del Terrorismo, conforme al Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo**.** 22010A0727(01). Diario Oficial n° L 195 de 27/07/2010 p. 5 – 14. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A22010A0727%2801%29 (28/02/2024).

Proyecto de conclusiones del Consejo sobre la concepción de una policía científica europea para 2020, con la creación de un espacio europeo de policía científica y el desarrollo de infraestructuras para dicha policía en Europa, 12391/2/11 REV 2 ENFOPOL 229 COPEN 209, de 1 de diciembre de 2011. Disponible en: https://data.consilium.europa.eu/doc/document/ST-17537-2011-INIT/es/pdf (02/12/2023).

Protocolo (nº 10) sobre la cooperación estructurada permanente establecida por el artículo 42 del Tratado de la Unión Europea. DO C 326 de 26.10.2012, p. 275–277. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A12012M%2FPRO%2F10 (27/10/2023).

Resolución del Parlamento Europeo, de 23 de octubre de 2013, sobre la suspensión del Acuerdo TFTP a raíz de la vigilancia de la NSA (2013/2831(RSP)). (2016/C 208/14). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52013IP0449 (28/02/2024).

Informe sobre el enfoque integral de la UE y sus implicaciones para la coherencia de la acción exterior de la UE, de 21 de febrero de 2014, de la Comisión de Asuntos Exteriores del Parlamento Europeo. Disponible en: https://www.europarl.europa.eu/doceo/document/A-7-2014-0138_ES.html (26/10/2023).

Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior. 2013/2188(INI). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52014IP0230 (28/02/2024).

Estrategia revisada de la UE para luchar contra la radicalización y la captación de terroristas, del Consejo de la Unión Europea, 9956/14. Bruselas, 19 de mayo de 2014. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/es/pdf (17/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

European Council meeting (19 and 20 March 2015) – Conclusions. Brussels, 20 March 2015 (OR. En). EUCO 11/15. Disponible en: https://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/en/pdf (27/08/2024).

Conclusiones del Consejo sobre relaciones exteriores, de 19/20 de marzo de 2015). Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2015/03/19/conclusions-russia-ukraine-european-council-march-2015/pdf/ (27/08/2024).

Resolución aprobada por el Consejo de Derechos Humanos 28/16. El derecho a la privacidad en la era digital. Asamblea General. A/HRC/RES/28/16. 1 de abril de 2015. Disponible en: https://documents.un.org/doc/undoc/gen/g15/068/81/pdf/g1506881.pdf?token=eXb0gJGhrPqnSyVKYd&fe=true (03/03/2024).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Agenda Europea de Seguridad. Estrasburgo, 28.4.2015. COM (2015) 185 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0185&rid=1 (02/12/2023).

Conclusiones de la Reunión del Consejo Europeo (25 y 26 de junio de 2015). Bruselas, 26 de junio de 2015. EUCO 22/15. Disponible en: https://www.consilium.europa.eu/media/21701/euco-conclusions_26062015_es.pdf (22/05/2024).

Resolución del Parlamento Europeo, de 9 de julio de 2015, sobre la Agenda Europea de Seguridad (2015/2697(RSP). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2015-0269_ES.html (02/12/2023).

Hacia una estrategia global de la UE: antecedentes, proceso, referencias. Septiembre de 2015. European Union Institute for Security Studies. Disponible en: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Towards_an_EU_Global_Strategy_0_0.pdf (27/10/2023).

Comunicación conjunta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo y al Consejo sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea. JOIN (2016) 18 final, de 6.4.2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018 (03/12/2023).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679 (14/03/2024).

Reglamento 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo. Diario Oficial de la Unión Europea L135/53, de 24/05/2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0794 (21/11/2023).

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union´s Foreign And Security Policy. June 2016. Disponible en: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (15/03/2024).

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Diario Oficial de la Unión Europea. 19.7.2016. L 194/1. Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf (06/03/2024).

Plan de Implementación de Seguridad y Defensa, del Consejo de la Unión Europea. Bruselas 14 de noviembre de 2016. 14392/16. Disponible en: https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf (1/11/2023).

Conclusiones del Consejo sobre la aplicación de la Estrategia Global de la UE en materia de Seguridad y Defensa, de 14 de noviembre de 2016. Disponible en: https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf (26/10/2023).

Comunicado de Prensa de 30 de noviembre de 2016, de la Comisión Europea, sobre el Plan de Acción Europeo de Defensa: hacia un Fondo Europeo de Defensa. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_16_4088 (011/11/2023).

Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión Marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo. DOUE L 88/6. 31.3.2017. Disponible en: https://www.boe.es/doue/2017/088/L00006-00021.pdf (10/03/2024).

Conclusiones del Consejo relativas al Informe sobre la Ciudadanía de la Unión de 2017, adoptada el 11 de mayo. Documento 9080/17. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9080-2017-INIT/es/pdf (13/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Proyecto de Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas ("conjunto de instrumentos de ciberdiplomacia"). Consejo de la Unión Europea 9916/17, de 7.7.2017. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/es/pdf (03/12/2023).

Informe conjunto al Parlamento Europeo y al Consejo relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas – Una respuesta de la Unión Europea. Bruselas, 19.7.2017. JOIN(2017) 30 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=JOIN%3A2017%3A30%3AFIN (19/08/2024).

Comunicación Conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 13.09.2017. JOIN(2017) 450 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017JC0450 (06/03/2024).

Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea. Diario Oficial de la Unión Europea L283/1 de 31 de octubre de 2017. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017R1939 (19/11/2023).

Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones el Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares, como respuesta ante el avance tecnológico de la actual amenaza terrorista. COM/2017/0610 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52017DC0610 (19/08/2024).

Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe report DGI(2017)09. Claire Wardle, PhD and Hossein Derakhshan. Disponible en: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html (06/10/2024).

Proyecto FANDANGO (FAke News Discovery and propagation from big Data ANalysis and artificial intelliGence Operations), 2018-2021. Disponible en: https://cordis.europa.eu/project/id/780355/es (14/05/2024).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción de Educación Digital. Bruselas, 17.1.2018. COM(2018) 22 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0022&from=EN (27/08/2024).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La Lucha contra la desinformación en línea:

Ediciones Universidad de Salamanca | CC BY-NC-ND

un enfoque europeo. Bruselas, 26.4.2018. COM(2018) 236 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236 (26/08/2024).

Comunicación conjunta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo y al Consejo sobre aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas. JOIN (2018) 16 final, de 13.6.2018. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0016 (03/12/2023).

Informe conjunto de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo, al Consejo Europeo y al Consejo relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas de julio 2017 a junio de 2018. Bruselas, 13.6.2018. JOIN(2018) 14 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0014R(01) (03/12/2023).

Código de Buenas Prácticas en materia de desinformación, de la Comisión Europea, publicado el 16 de junio de 2018. Disponible en: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (02/09/2024).

Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Garantizar unas elecciones europeas libres y justas. Contribución de la Comisión Europea a la reunión de los dirigentes en Salzburgo los días 19 y 20 de septiembre de 2018. Bruselas, 12.9.2018. COM(2018) 637 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2018%3A637%3AFIN (31(08/2024).

Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (DO L 295/138 de 21/11/2018). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1727 (25/11/2023).

Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n. 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018). Disponible en: https://www.boe.es/doue/2018/312/L00056-00106.pdf (16/11/2023).

Comunicación Conjunta de la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción contra la desinformación. Bruselas 5.12.2018. JOIN(2018) 36 final. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036 (31/08/2024).

Nota de prensa del SEAE en su página web oficial, de 05.12.2018. Intensificar la respuesta europea coordinada a la desinformación. Disponible en: https://www.eeas.europa.eu/node/54897_en (08/09/2024).

Europol Strategy 2020+, 5 de febrero de 2019. Disponible en: https://www.europol.europa.eu/publications-events/publications/europol-strategy-2020 (23/11/2023).

Conclusiones del Consejo y de los Estados miembros sobre Garantizar unas elecciones europeas libres e imparciales. Bruselas, 19 de febrero de 2019. Disponible en: https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/es/pdf https://www.consilium.europa.eu/en/press/press-releases/2019/02/19/securing-free-and-fair-european-elections-council-adopts-conclusions/ (19/08/2024).

The European Union´s Global Strategy. Three years on, looking forward. Disponible en: https://www.eeas.europa.eu/sites/default/files/eu_global_strategy_2019.pdf (26/10/2023).

Reglamento (UE) 2019/1148 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre la comercialización y la utilización de precursores de explosivos, por el que se modifica el Reglamento (CE) n.º 1907/2006 y se deroga el Reglamento (UE) n.º 98/2013. PE/46/2019/REV/1. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32019R1148 (19/08/2024).

Una nueva agenda estratégica para la UE 2019-2024. Documento del Consejo Europeo, de 20 de junio de 2019. Disponible en:https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/ (25/08/2024).

Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Diario Oficial de la Unión Europea, 11.07.2019, L 186/57. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R1150 (08/02/2024).

Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats - Establishment and adoption of its Terms of Reference. Brussels, 8.7.2019. 10027/19. Disponible en: https://data.consilium.europa.eu/doc/document/ST-10027-2019-INIT/en/pdf (25/08/2024).

Una Unión que se esfuerza por lograr más resultados. Mi agenda para Europa. Orientaciones políticas para la próxima Comisión Europea 2019-2024. Úrsula von der Leyen. Disponible en: https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_es?filename=political-guidelines-next-commission_es.pdf (25/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Conclusiones sobre las acciones complementarias para aumentar la resiliencia y luchar contras las amenazas híbridas. Consejo de la Unión Europea. Bruselas, 10 de diciembre de 2019. 14972/19. Disponible en: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/es/pdf (08/09/2024).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el despliegue seguro de la 5G en la UE – Aplicación de la caja de herramientas de la UE. Bruselas, 29.1.2020. COM (2020) 50 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0050 (03/12/2023).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Configurar el futuro digital de Europa. Bruselas, 19.2.2020. COM (2020) 607 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0067 (28/02/2024).

Comisión Europea. Comunicación conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La lucha contra la desinformación acerca de la COVID-19: contrastando los datos. JOIN(2020) 8 final. Bruselas, 10.6.2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020JC0008 (01/09/2024).

Decisión del Parlamento Europeo de, 18 de junio de 2020, sobre la constitución, competencias, composición numérica y duración del mandato de la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación (2020/2683(RSO)). Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020DP0161 (24/10/2024).

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE para una Unión de la Seguridad. Bruselas 24.07.2020, COM(2020) 605 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0605 (03/12/2023).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Agenda y Plan de Acción de la UE en materia de Lucha contra la Droga 2021-2025. Bruselas, 24.7.2020. COM(2020) 606 final. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:6e3562ed-cfee-11ea-adf7-01aa75ed71a1.0015.02/DOC_1&format=PDF (03/12/2023).

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE para una Unión de la Seguridad, Bruselas 24.07.2020, COM (2020) 605 Final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0605 (03/12/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores. COM (2020) 607 final, de 24.7.2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0607 (03/12/2023).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción de la UE sobre el Tráfico de Armas de Fuego 2020-2025. Bruselas, 24.7.2020. COM(2020) 608 final. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:65f0454e-cfef-11ea-adf7-01aa75ed71a1.0014.02/DOC_1&format=PDF (03/12/2023).

Commission Staff Working Document. Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement. Brussels, 10.9.2020. SWD(2020) 180 final. Disponible en: https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement (08/09/2024).

Plan de Educación Digital 2021-2027, recogido en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Plan de Acción de Educación Digital 2021-2027: Adaptar la educación y la formación a la era digital. Bruselas, 30.9.2020. COM(2020) 624 final. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/digital-education-action-plan-2021-2027.html (27/08/2024).

Decisión (PESC) 2020/1639 del Consejo de 5 de noviembre de 2020 por la que se establecen las condiciones generales en las que se podrá invitar excepcionalmente a terceros Estados a participar en proyectos individuales de la Cooperación Estructurada Permanente. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020D1639 (01/11/2023).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción para la Democracia Europea. Bruselas, 3.12.2020. COM(2020) 790 final. Página 21. Disponible en: https://commission.europa.eu/document/63918142-7e4c-41ac-b880-6386df1c4f6c_es (27/08/2024).

Comunicación Conjunta al Parlamento Europeo y al Consejo. La Estrategia de Ciberseguridad de la UE para la Década Digital. Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 16.12.2020. JOIN(2020) 18 final. Disponible en: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (03/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Fondo de Seguridad Interior para el Marco Financiero Plurianual 2021-2027. Disponible en: https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-de-seguridad-interior/ (18/11/2023).

Fondo de Asilo, Migración e Integración para el Marco Financiero Plurianual 2021-2027. Disponible en: https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-asilo-migracion-e-integracion/ (18/11/2023):

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción sobre las sinergias entre las industrias civil, de la defensa y espacial. Comisión Europea. Bruselas, 22 de febrero de 2021. COM (2021) 70 final. Disponible en: https://commission.europa.eu/document/2353ded9-0e39-4d35-a46c-67c62779afe1_es (01/11/2023).

Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. General Assembly. Conference room paper. A/AC.290/2021/CRP.2. 10/03.2021. Disponible en: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (03/03/2024).

Strategic communications as a key factor in countering hybrid threats. European Parliamentary Research Service. March 2021. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656323/EPRS_STU(2021)656323_EN.pdf (27/08/2024).

Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales. Bruselas, 21 de marzo de 2022. 7371/22. Disponible en: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf (08/11/2023).

Decisión (PESC) 2021/509 del Consejo de 22 de marzo de 2021, por la que se crea un Fondo Europeo de Apoyo a la Paz y se deroga la Decisión (PESC) 2015/528. DOUE núm. 102, de 24 de marzo de 2021. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80367 (07/11/2023).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025. Bruselas, 14.4.2021. COM(2021) 170 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0170 (03/12/2023).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE en la lucha contra la trata de seres humanos 2021-2025. Bruselas, 14.4.2021. COM(2021) 171 final.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0171 (03/12/2023).

Informe del Tribunal de Cuentas Europeo sobre el impacto de la desinformación en la UE. Informe Especial 9/2021 El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada 2021/C 215/06. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SA0009(01) (01/09/2024).

Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea. Bruselas, 3.6.2021. COM(2021) 281 final. 2021/0136(COD). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0281 (16/03/2024).

Joint Communication to the European Parliament and the Council. Report on implementation of the EU´s Cybersecurity Strategy for the Digital Decade. High Representative of the Union for Foreign Affairs and Security Policy. Brussels, 23.6.2021. JOIN(2021) 14 final. 2021/0166 (NLE). Disponible en: https://digital-strategy.ec.europa.eu/en/library/first-implementation-report-eu-cybersecurity-strategy (03/03/2024).

Tribunal de Cuentas Europeo. Informe Especial 9/2021 *El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada*. 2021/C 215/06. Disponible en: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_ES.pdf (22/09/2024).

Objetivos de Alto Valor y Grupos de Acción Operativa de Europol. 14 de diciembre de 2021. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2022-2024.pdf (23/11/2023).

EC3 Informe Cryptocurrency: tracing the evolution of criminal finances (enero 2022). Disponible en: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (23/11/2023).

Informe final -INGE1-, de 9 de marzo de 2022, del primer Comité Especial sobre Injerencia Extranjera en todos los Procesos Democráticos de la Unión Europea. Disponible en: https://www.europarl.europa.eu/committees/es/ing2/home/highlights (20/10/2023).

Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2020/2268(INI)). P9_TA(2022)0064. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022IP0064 (28/08/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Decisión del Parlamento Europeo, de 10 de marzo de 2022, sobre la constitución, competencias, composición numérica y duración del mandato de la Comisión Especial sobre Injerencias Extranjeras en todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación (INGE 2) (2022/2585(RSO)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0070_ES.html (24/10/2024).

Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales. Bruselas, 21 de marzo de 2022. 7371/22. Disponible en: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf (26/08/2024).

Reglamento (UE) 2022/838, de 30 de mayo, del Parlamento Europeo y del Consejo de 30 de mayo de 2022 por el que se modifica el Reglamento (UE) 2018/1727 en lo que respecta a la preservación, análisis y almacenamiento en Eurojust de pruebas relativas al genocidio, los crímenes contra la humanidad, los crímenes de guerra y las infracciones penales conexas. DOUE núm. 148, de 31 de mayo de 2022. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80811 (25/11/2023).

Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Ley de Gobernanza de Datos). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868 (14/03/2024).

Código Reforzado de Buenas Prácticas contra la Desinformación. Junio 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (14/09/2024).

Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, 8 de junio de 2022, por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación. Diario Oficial de la Unión Europea L169, de 27/06/2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R0991 (23/11/2023).

Resolución del Parlamento Europeo, de 9 de junio de 2022, sobre la convocatoria de una convención para la revisión de los Tratados (2022/2705(RSP)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0244_ES.html (22/10/2023).

Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados competitivos y justos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Ley de Mercados Digitales). Disponible en: https://eur-lex.europa.eu/legal-

Ediciones Universidad de Salamanca | CC BY-NC-ND

content/EN/TXT/?toc=OJ%3AL%3A2022%3A265%3ATOC&uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG (16/03/2024).

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). DOUE L 277/1, de 27 de octubre de 2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065 (14/03/2024).

Comunicación Conjunta al Parlamento Europeo y al Consejo sobre la Política de Ciberdefensa de la UE. Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Bruselas, 10.11.2022. JOIN(2022) 49 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022JC0049 (06/03/2024).

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962 (16/03/2024).

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963 (16/03/2024).

Resolución del Parlamento Europeo, de 18 de enero de 2023, sobre la aplicación de la política exterior y de seguridad común: informe anual 2022. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0009_ES.html (20/10/2023).

Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - Analysis of the final compromise text. Brussels, 20 January 2023. 5448/23. Disponible en: https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf (16/03/2024).

Recomendación de la Comisión de 8 de febrero de 2023 sobre los objetivos de resiliencia de la Unión ante catástrofes. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-Z-2023-70010 (12/01/2025).

Primer Informe del SEAE sobre Amenazas de Manipulación e Interferencia de Información Extranjera: hacia un marco para la defensa en red. European Union External Action. Febrero de 2023. Disponible en: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en (28/09/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas. DOUE núm. 63, de 28 de febrero de 2023. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80291 (03/03/2024).

Comunicación Conjunta al Parlamento Europeo y al Consejo relativa a la actualización de la Estrategia de Seguridad Marítima de la UE y su Plan de Acción «Una Estrategia de Seguridad Marítima de la UE reforzada para hacer frente a unas amenazas marítimas cambiantes». Bruselas 10/03/2023. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:9e3d4557-bf39-11ed-8912-01aa75ed71a1.0006.02/DOC_1&format=PDF (14/01/2024).

Reglamento del Parlamento Europeo y del Consejo por el que se establece un marco para garantizar el suministro seguro y sostenible de materias primas fundamentales. Bruselas, 16.3.2023. COM(2023) 160 final. 2023/0079 (COD). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0160 (15/05/2023).

Primer Informe Anual de progreso de la implementación de la BESD. Marzo 2023. Disponible en: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf (06/11/2023).

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos. Expediente interinstitucional 2023/0109(COD). Bruselas, 20 de abril de 2023. 8512/23. Disponible en: https://data.consilium.europa.eu/doc/document/ST-8512-2023-INIT/es/pdf (06/03/2024).

Informe INGE 2 sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación, de 15 de mayo de 2023 (Informe A9-0187/2023; relatora Sandra Kalniete). Disponible en: https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html#_section2 (24/10/2024).

Informe de Injerencias extranjeras en los procesos democráticos de la UE, de mayo de 2023, del Parlamento Europeo. Disponible en: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)747908 (20/10/2023).

Decisión del Consejo, de fecha 23 de mayo de 2023, sobre incorporación de Dinamarca a la UE. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/05/23/eu-defence-cooperation-council-welcomes-denmark-into-pesco-and-launches-the-5th-wave-of-new-pesco-projects/ (29/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Resolución del Parlamento Europeo, de 1 de junio de 2023, sobre la injerencia extranjera en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2022/2075(INI)). DOUE C, C/2023/1226 de 21.12.2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C_202301226 (13/05/2024).

Consolidated Annual Activity Report 2022, analizado en la reunión del Consejo de Administración de Europol de los días 7 y 8 de junio de 2023. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202022.PDF (24/11/2023).

Informe de la EDA sobre desarrollo y ejecución de los proyectos PESCO, de julio de 2023. Disponible en: https://eda.europa.eu/news-and-events/news/2023/07/11/pesco-projects-adapt-and-accelerate-amid-shifting-european-security-landscape-eu-report-finds (30/10/2023).

EC3 Informe IOCTA (julio 2023), titulado *Cyber-attacks: the ápex of crime-as-a-service.* Disponible en: https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023 (23/11/2023).

EC3 Informe *The other side of the coin* (2023). Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf (23/11/2023).

Acuerdos de cooperación judicial y de intercambio estratégico de información, con la Fiscalía General de Hungría (abril 2021) y con el Ministerio de Justicia danés (agosto 2023). Disponible en: https://www.eppo.europa.eu/en/members (19/11/2023).

Decisión (UE) 2023/1974 del Consejo de 18 de septiembre de 2023 relativa a la firma, en nombre de la Unión Europea, del Acuerdo en el marco de la Convención de las Naciones Unidas sobre el Derecho del Mar relativo a la conservación y el uso sostenible de la diversidad biológica marina de las zonas situadas fuera de la jurisdicción nacional. DOUE núm. 235, de 25 de septiembre de 2023, páginas 1 a 3. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81321 (20/03/2024).

Reglamento (UE) 2023/2131 del Parlamento Europeo y del Consejo, de 4 de octubre de 2023, por el que se modifican el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo y la Decisión 2005/671/JAI del Consejo en lo que respecta al intercambio de información digital en casos de terrorismo. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81404 (25/11/2023).

Comunicación de la Comisión, de 8 de noviembre de 2023, sobre la concesión a Ucrania del estatuto de candidato a la UE. Disponible en: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-

Ediciones Universidad de Salamanca | CC BY-NC-ND

11/COM_2023_690%20Communication%20on%20EU%20Enlargement%20Policy_and_Annex.pdf (09/11/2023).

Estudio sobre el desarrollo de normas internacionales específicas para FIMI. European Union External Action. Noviembre de 2023. Disponible en: https://www.eeas.europa.eu/eeas/study-international-norms-foreign-information-manipulation-and-interference-fimi_en (28/09/2024).

Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023, por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión. DOUE 18.12.2023. Disponible en: https://www.boe.es/doue/2023/2841/L00001-00027.pdf (22/04/2024).

Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas sobre el acceso equitativo y el uso de datos y por el que se modifica el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Ley de Datos). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1704709568425 (14/03/2024).

EC3 Informe Criminal networks in migrants smuggling (diciembre 2023). Disponible en: https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-migrant-smuggling#:~:text=The%20criminal%20networks%20involved%20are,offered%20by%20migrant%20smuggling%20networks (23/11/2023).

Eurobarómetro Flash 522 - Democracia. Disponible en: https://data.europa.eu/data/datasets/s2966_fl522_eng?locale=en (22/05/2024).

Paquete de Defensa de la Democracia (diciembre 2023). Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6453 (15/05/2024).

Resolución del Parlamento Europeo, de 17 de enero de 2024, sobre las implicaciones en materia de seguridad y defensa de la influencia de China en las infraestructuras críticas en la Unión Europea P9_TA(2024)0028 (2023/2072(INI)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_ES.html#def_1_14 (25/10/2024).

Informe de investigación híbrida del CoE n.° 11: "Cómo Ucrania lucha contra la desinformación rusa: colmena contra mamut". 24 de enero de 2024. Disponible en: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-11-how-ukraine-fights-russian-disinformation-beehive-vs-mammoth/ (22/11/2024).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement. Brussels, 26 January 2024. 5662/24. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf (16/03/2024).

Segundo informe del SEAE sobre Amenazas de Manipulación e Interferencia de Información Extranjera: un marco para la defensa en red. European Union External Action. Enero de 2024. Disponible en: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (29/09/2024).

Informe nº 12 de investigación del Consejo de Europa, de 19 de marzo de 2024. Contrarrestar las amenazas híbridas a las elecciones: de la actualización normativa al establecimiento de redes de colaboración. Disponible en https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/ (13/05/2024).

Conclusiones del Consejo Europeo de 21 de marzo de 2024. Disponible en: https://www.consilium.europa.eu/media/70843/20240321-euco-conclusions-es.pdf (21/04/2024).

Compendium on Elections Cybersecurity and Resilience 2024. Disponible en: https://digital-strategy.ec.europa.eu/en/news/new-cybersecurity-compendium-how-protect-integrity-elections-published (11/01/2025).

Proyecto de Convención de las NNUU contra la Ciberdelincuencia elaborado por el Comité Especial creado *ad hoc* en el seno de NNUU. Disponible en: https://ciberprisma.org/wp-content/uploads/2024/08/v2405509-espanol.pdf (05/09/2024).

Joint White Paper for European Defence Readiness 2030. Brussels, 19.3.2025. JOIN(2025) 120 final. Disponible en: https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf (23/03/2025).

Normativa, informes y documentos oficiales nacionales

Normativa

Real Decreto 1316/1977, de 2 de junio, sobre demarcación territorial y funcional de las Fuerzas de Orden Público. BOE núm. 141, de 14 de junio de 1977. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1977-13819 (24/04/2024).

Ratificación por España el 9 de mayo de 1980, del Convenio Europeo para la Represión del Terrorismo, de fecha 27 de enero de 1977, publicado en BOE 242, de 8 de octubre de 1980, páginas 22357 a 22360. Disponible en: https://www.boe.es/eli/es/ai/1977/01/27/(2) (22/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859 (24/11/2023).

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. BOE núm. 109, de 07/05/2002, referencia BOE-A-2002-8628. Disponible en: https://www.boe.es/eli/es/l/2002/05/06/11/con (14/01/2025).

Acuerdo del Consejo de Ministros del 28 de Mayo de 2004, por el que se crea el Centro Nacional de Coordinación Antiterrorista de la Secretaría de Estado de Seguridad del Ministerio del Interior. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2004/c2805040.aspx#CNCoordAntiterrorista (30/12/2023).

Orden INT/2103/2005, de 1 de julio, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía. Disponible en: https://www.boe.es/boe/dias/2005/07/02/pdfs/A23672-23682.pdf (30/12/2023).

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. BOE número 102, de fecha 29/04/2011, referencia BOE-A-2011-7630. Disponible en: https://www.boe.es/eli/es/l/2011/04/28/8/con (21/01/2025).

Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. Publicado en el BOE-A-2012-9816. Disponible en: https://www.boe.es/eli/es/rd/2012/07/20/1119 (16/12/2023).

Directiva de Defensa Nacional 2012: por una defensa necesaria, por una defensa responsable. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2012.pdf (21/12/2023).

Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. Boletín Oficial del Ministerio de Defensa número 40. Martes, 26 de febrero de 2013. Disponible en: https://emad.defensa.gob.es/Galerias/prensa/noticias/Documentos/20130226_CIBERDEFENSA.pdf (08/04/2024).

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. BOE núm. 233, de 29 de septiembre de 2015. BOE-A-2015-10389. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389 (21/12/2023).

Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional. BOE 38, martes 14 de

Ediciones Universidad de Salamanca | CC BY-NC-ND

febrero de 2017. Disponible en: https://www.boe.es/boe/dias/2017/02/14/pdfs/BOE-A-2017-1460.pdf (16/12/2023).

Orden PRA/29/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se crea y regula el Comité Especializado de no proliferación de armas de destrucción masiva. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-795.pdf (27/12/2023).

Orden PRA/30/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se crea y regula el Comité Especializado de Seguridad Energética. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-796.pdf (27/12/2023).

Orden PRA/31/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Comité Especializado de Inmigración, modifica el Acuerdo original de 2014 en lo relacionado con su naturaleza jurídica, las funciones, la composición -presidencia y procedimiento de designación de sus miembros- y otras previsiones como la emisión de informes, la creación de grupos de trabajo y el reforzamiento del enlace y coordinación con los componentes fundamentales y ámbitos de especial interés para la Seguridad Nacional dentro del marco del Sistema de Seguridad Nacional. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-797.pdf (26/12/2023).

Orden PRA/32/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Comité Especializado de Situación. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-798.pdf (19/12/2023).

Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. BOE número 20 de 23 de enero de 2018. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-799-consolidado.pdf (21/12/2023).

Orden PRA/34/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Seguridad Marítima. BOE número 20, de fecha 23 de enero de 2018. Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-800.pdf (26/12/2023).

Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. BOE núm. 46, de 22 de febrero de 2019. Disponible en: https://www.boe.es/boe/dias/2019/02/22/pdfs/BOE-A-2019-2442.pdf (16/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Orden PCI/168/2019, de 22 de febrero, por la que se publica el Plan Nacional de Biocustodia, aprobado por el Consejo de Seguridad Nacional. BOE número 47 de 23 de febrero de 2019. Disponible en: https://www.boe.es/boe/dias/2019/02/23/pdfs/BOE-A-2019-2553.pdf (27/12/2023).

Orden PCM/219/2020, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se crea y regula el Comité Especializado contra el Terrorismo, en desarrollo de lo previsto en el Capítulo 5 de la Estrategia Nacional contra el Terrorismo 2019, en el que se establece "la creación de un Comité Especializado que aborde el terrorismo y los extremismos violentos" en apoyo al CSN para el cumplimiento de su función asesora al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito referido. BOE número 66 de 14 de marzo de 2020. Disponible en: https://www.boe.es/boe/dias/2020/03/14/pdfs/BOE-A-2020-3639.pdf (28/12/2023).

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. BOE núm. 103, de martes 30 de abril de 2019. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-6347 (14/01/2024).

Orden PCI/488/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Protección Civil, aprobada por el Consejo de Seguridad Nacional. BOE núm. 103, martes 30 de abril de 2019. Disponible en: https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6348.pdf (07/01/2024).

Orden PCI/489/2019, de 26 de abril por la que se publica la Estrategia de Seguridad Aeroespacial Nacional, aprobada por el Consejo de Seguridad Nacional. Disponible en: https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Aeroespacial%202019%20Interactiva.pdf (15/01/2024).

Orden PCM/218/2020, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se crea y regula el Consejo Nacional de Seguridad Aeroespacial, para dar cumplimiento a lo establecido en el Capítulo 4 de la Estrategia de Seguridad Aeroespacial Nacional de 2019, que dispone la creación de un Consejo Nacional de Seguridad Aeroespacial para dar apoyo al CSN en su labor de asistencia al Presidente del Gobierno en lo que en dicho ámbito afecte a la Política de Seguridad Nacional. BOE número 66 de 14 de marzo de 2020. Disponible en: https://www.boe.es/boe/dias/2020/03/14/pdfs/BOE-A-2020-3638.pdf (28/12/2023).

Directiva de Defensa Nacional 2020. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2020.pdf (21/12/2023).

Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-9138 (24/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Orden PCM/1028/2020, de 30 de octubre, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se aprueba el procedimiento para la elaboración de la Estrategia de Seguridad Nacional 2021. BOE núm. 292, de 05/11/2020. Disponible en: https://www.boe.es/buscar/pdf/2020/BOE-A-2020-13661-consolidado.pdf (08/01/2024).

Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Apartado 1. Contexto. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-13663 (06/10/2024).

Orden PCM/575/2021, de 8 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 25 de mayo de 2021, por el que se aprueba el Plan Integral de Cultura de Seguridad Nacional. BOE número 138 de 10 de junio de 2021. Disponible en: https://www.boe.es/boe/dias/2021/06/10/pdfs/BOE-A-2021-9631.pdf (18/12/2023).

Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. BOE núm. 314, de 31 de diciembre de 2021 (referencia BOE-A-2021-21884). Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884 (08/01/2024).

Real Decreto-ley 6/2022, de 29 de marzo, por el que se adoptan medidas urgentes en el marco del Plan Nacional de respuesta a las consecuencias económicas y sociales de la guerra en Ucrania. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-4972 (25/10/2023).

Orden PCM/541/2022, de 10 de junio, por la que se publica el Acuerdo del Consejo de Ministros de 31 de mayo de 2022, por el que se crea el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional y se regula su composición y funcionamiento. BOE número 142 de 15 de junio de 2022. Disponible en: https://www.boe.es/boe/dias/2022/06/15/pdfs/BOE-A-2022-9965.pdf (19/12/2023).

Real Decreto 524/2022, de 27 de junio, por el que se dispone el cambio de denominación del Ejército del Aire por la de Ejército del Aire y del Espacio. BOE núm. 155, de 29 de junio de 2022. BOE-A-2022-10787. Disponible en: https://www.boe.es/eli/es/rd/2022/06/27/524

Orden PCM/714/2022, de 23 de julio, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 21 de junio de 2022, por el que se modifica el de 1 de diciembre de 2017, por el que se regula el Comité de Situación. BOE núm. 180, de 28 de julio de 2022. BOE-A-2022-12585. Disponible en: https://www.boe.es/eli/es/o/2022/07/23/pcm714 (21/12/2023).

Orden PCM/720/2022, de 23 de julio, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 21 de junio de 2022, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia de Seguridad Marítima Nacional. BOE núm. 180,

Ediciones Universidad de Salamanca | CC BY-NC-ND

de 28 de julio de 2022. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-12627 (14/01/2024).

Orden PCM/1051/2022, de 1 de noviembre, por la que se publica el Acuerdo del Consejo de Ministros de 31 de mayo de 2022, por el que se crea el Foro Integral de Seguimiento y Evaluación de la Cultura de Seguridad Nacional y se regula su composición y funcionamiento. BOE número 264 de 3 de noviembre de 2022. Disponible en: https://www.boe.es/boe/dias/2022/11/03/pdfs/BOE-A-2022-18088.pdf (18/12(2023).

Ley 25/2022, de 1 de diciembre, sobre precursores de explosivos -BOE núm. 289, de 2 de diciembre de 2022-. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-20184 (19/08/2024).

Orden INT/859/2023, de 21 de julio, por la que se desarrolla la estructura orgánica y funciones de los servicios centrales y territoriales de la Dirección General de la Policía. BOE núm. 176, de 25/07/2023. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2023-17072 (24/11/2023).

Orden PCM/207/2023, de 2 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para la elaboración de la Estrategia Nacional contra la Proliferación de Armas de Destrucción Masiva. BOE núm. 54, de 4 de marzo de 2023. Referencia BOE-A-2023-5702. Disponible en: https://www.boe.es/eli/es/o/2023/03/02/pcm207 (29/12/2023).

Orden PJC/326/2024, de 14 de abril, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para el desarrollo del Catálogo de Recursos de la Seguridad Nacional. Publicada en BOE núm. 93, de 16/04/2024 (BOE-A-2024_7481). Disponible en: https://www.boe.es/eli/es/o/2024/04/14/pjc326/con (01/12/2024)

Orden PJC/327/2024, de 14 de abril, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba una nueva Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. BOE núm. 93, de martes 16 de abril de 2024. Disponible en: https://www.boe.es/boe/dias/2024/04/16/pdfs/BOE-A-2024-7482.pdf (24/11/2024).

Orden PJC/406/2024, de 7 de mayo, por la que se publica la Estrategia Nacional contra el Terrorismo 2023, aprobada por el Consejo de Seguridad Nacional. BOE núm. 112, de 8 de mayo de 2024. Referencia BOE-A-2024-9149. Disponible en: https://www.boe.es/eli/es/o/2024/05/07/pjc406 (20/03/2024).

Orden PJC/501/2024, de 27 de mayo, por la que se publica la Estrategia Nacional de Seguridad Marítima 2024, aprobada por el Consejo de Seguridad Nacional. BOE número 130, de 29 de mayo de 2024 (BOE-A-2024-10762). Disponible en: https://www.boe.es/eli/es/o/2024/05/27/pjc501 (03/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Orden PCJ/1290/2024, de 13 de noviembre, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se crea y regula el Comité Especializado contra el Crimen Organizado y la Delincuencia Grave. BOE número 278, de 18 de noviembre de 2024 (BOE-A-2024-23946). Disponible en: https://www.boe.es/eli/es/o/2024/11/13/pjc1290/dof/spa/pdf (24/11/2024).

Orden PJC/1430/2024, de 16 de diciembre, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 15 de octubre de 2024, por el que se aprueba la Estrategia Nacional de Protección Civil. BOE núm. 304, de 18 de diciembre de 2024. Disponible en: https://www.boe.es/eli/es/o/2024/12/16/pjc1430 (12/01/2024).

Diarios de Sesiones

Comparecencia del señor director del gabinete del presidente del Gobierno (Moragas Sánchez), para presentar la estrategia de seguridad nacional 2013. A propuesta del Gobierno. (Número de expediente 212/001017). Diario de Sesiones del Congreso de los Diputados, Comisión Constitucional, sesión núm. 16 (extraordinaria), celebrada el martes 9 de julio de 2013. Disponible en: https://www.congreso.es/public_oficiales/L10/CONG/DS/CO/DSCD-10-CO-372.PDF (03/01/2024).

Debate del Proyecto de Ley de Seguridad Nacional. «BOCG. Congreso de los Diputados», serie A, número 158-1, de 29 de mayo de 2015. (Número de expediente 121/000158). Diario de Sesiones del Congreso de los Diputados, sesión plenaria núm. 278 (extraordinaria), de 8 de julio de 2015. Disponible en: https://www.congreso.es/public_oficiales/L10/CONG/DS/PL/DSCD-10-PL-296.PDF (21/12/2023).

Informes, Instrucciones y otros documentos

La curia regia de León de 1188 y sus “Decreta” y constitución. Versión de José M.ª FERNÁNDEZ CATÓN. León. Centro de Estudios e Investigación “San Isidoro” – Archivo Histórico Diocesano, 1993; pp. 93-117. Disponible en: https://www.cultura.gob.es/dam/jcr:5e01f9da-8205-47ee-8053-2c3a68e198ef/decreta-leon-version-espanola.pdf (14/05/2023).

Instituciones de Derecho Público General de España con noticia del Particular de Cataluña, y de las principales reglas de gobierno en cualquier Estado (1800). Ramón Lázaro de Dou y Bassols. Biblioteca Virtual del Patrimonio Bibliográfico. Ministerio de Cultura. Gobierno de España. Disponible en: https://bvpb.mcu.es/es/consulta/registro.cmd?id=403995 (18/05/2023).

Carta de Fernando Castiella, Ministro de Asuntos Exteriores de España, a Maurice Couve de Murville, Presidente del Consejo de Ministros de la CEE, en la que solicita la apertura de negociaciones para examinar una posible vinculación de España con la CEE. Disponible en: https://www.cvce.eu/content/publication/2010/2/25/7e6802dc-c3e7-4715-9c68-b49224a171f7/publishable_es.pdf (22/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Discurso de don José Luis Rodríguez Zapatero en la sesión de investidura como Presidente del Gobierno, el 8 de abril de 2008. Disponible en: https://www.lamoncloa.gob.es/presidente/intervenciones/Paginas/2008/prsp20080408.aspx (29/12/2023).

Nota de prensa de La Moncloa sobre la aprobación de la Estrategia Española de Seguridad 2011. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/paginas/enlaces/24062011enlace2.aspx (29/12/2023).

Reforma del al art. 135 CE para posibilitar el cumplimiento de los compromisos asumidos por España al integrarse en la CEE, de 27 de septiembre de 2011. Disponible en: https://www.congreso.es/docu/constituciones/1978/art135_1978.pdf (21/10/2023).

Estrategia Española de Seguridad: Una responsabilidad de todos. Año 2011. Disponible en: https://www.lamoncloa.gob.es/documents/9BED-CF7A-estrategiaespanoladeseguridad.pdf (16/12/2023).

Directiva de Defensa Nacional 2012: por una defensa necesaria, por una defensa responsable. Presidencia del Gobierno. Madrid. Julio de 2012. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2012.pdf (24/08/2023).

Informes Anuales de Seguridad Nacional, del DSN (desde 2013). Disponibles en: https://www.dsn.gob.es/es/estrategias-publicaciones/informe-anual-seguridad-nacional (16/12/2023).

Estrategia de Seguridad Nacional 2013. Presidencia del Gobierno, Madrid, 2013. Disponible en: https://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf (03/01/2024).
Estrategia de Seguridad Marítima Nacional 2013. Presidencia del Gobierno, Madrid, 2013. Disponible en: https://www.dsn.gob.es/en/node/23415 (14/01/2024).

Estrategia de Seguridad Energética Nacional 2015. Presentación, página II. Presidencia del Gobierno, Madrid, 2015. Disponible en: https://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20seguridad%20energetica%20nacional.pdf (14/01/2024).

Estrategia de Seguridad Nacional 2017. Presidencia del Gobierno, Madrid, 2017. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2017 (08/01/2024).

Estrategia Nacional de Ciberseguridad. Presidencia del Gobierno, Madrid, 2019. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019 (20/04/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023. Presidencia del Gobierno, Madrid, 2019. Disponible en: https://www.dsn.gob.es/sites/dsn/files/ESTRATEGIA%20ESPA%C3%91OLA%20CRIMEN%20ORGANIZADO%20DG.pdf (16/01/2024).

Red de Coordinación para la Seguridad en Procesos Electorales. Disponible en: https://www.europapress.es/nacional/noticia-interior-crea-red-coordinacion-seguridad-procesos-electorales-20190412204535.html (14/05/2024).

Estrategia de Seguridad Nacional 2021 "Un proyecto compartido". Disponible en: https://www.dsn.gob.es/index.php/es/es/actualidad/sala-prensa/estrategia-seguridad-nacional-2021 (14/05/2023).

Nota de prensa del Proyecto KOIOS de inteligencia artificial para la defensa. Disponible en: https://www.defensa.com/otan-y-europa/ct-lidera-proyecto-inteligencia-artificial-koios-apoyado-fondo (07/11/2023).

Informe Anual de Seguridad Nacional 2023, del Departamento de Seguridad Nacional de España. Disponible en: https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2023 (27/03/2024).

La resiliencia en el marco de la seguridad nacional. Presidencia del Gobierno, marzo 2024. NIPO 143-24-031-8. Disponible en: https://www.dsn.gob.es/index.php/node/23443 (11/01/2025).

Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional. Trabajos 2023. Disponible en: https://es.scribd.com/document/694443774/Foro-Campanas-Desinfo-GT-2023-Accesible (20/10/2024).

Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). Informe C: Desinformación en la era digital (2023). Disponible en: www.doi.org/10.57952/j3p6-9086 (07/12/2024).

Plan Operativo de Prevención de la Radicalización Violenta de la Policía Nacional, de diciembre de 2023. Disponible en: https://www.interior.gob.es/opencms/es/servicios-al-ciudadano/plan-estrategico-nacional-de-prevencion-y-lucha-contra-la-radicalizacion-violenta-pencrav/plan-estrategico-nacional/objetivos-mision-vision/ (17/01/2024).

La resiliencia en el marco de la seguridad nacional. Presidencia del Gobierno, marzo 2024. Disponible en: https://www.dsn.gob.es/index.php/node/23443 (17/01/2025).

Plan de Acción por la Democracia, del Gobierno de España, presentado el 17 de septiembre de 2024. Disponible en: https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (04/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Guía de buenas prácticas y procedimientos de ciberseguridad aplicados a software específico. Disponible en: https://www.ccn-cert.cni.es/es/guias?format=html (11/01/2025).

Informe Ciberamenazas y tendencias, de diciembre de 2024. Disponible en: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html (11/01/2025).

Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad. Enero 2025. Disponible en: https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf (18/01/2025).

Datos estadísticos de cibercriminalidad del Ministerio del Interior (2024). Disponible en: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/balances.html (11/01/2025).

Informe Anual de Seguridad Nacional del DSN (2014-2024). Disponible en: https://www.dsn.gob.es/publicaciones/informes-anuales (11/01/2025).

Jurisprudencia

Internacional

Tribunal de la Haya

Laudo arbitral de la Corte Permanente de Arbitraje. Asunto de la Isla de Palmas, Estados Unidos de América vs. Países Bajos. Abril de 1928. Disponible en: https://es.scribd.com/document/440736120/Fallo-Isla-de-Palmas (20/04/2023).

Caso del Canal de Corfú, fallo de la Corte Internacional de Justicia de 9 de abril de 1949. Disponible en: https://www.dipublico.org/115899/caso-del-canal-de-corfu-fondo-del-asunto-fallo-de-9-de-abril-de-1949/ (12/04/2024).

Supranacional Europea

Tribunal de Justicia de la Unión Europea

Dictámen del Tribunal de Justicia de la Comunidades Europeas (TJCE) en el caso Van Gend en Loos, de febrero de 1963. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/the-direct-effect-of-european-union-law.html (21/10/2023).

Sentencia del Tribunal General de 27 de julio de 2022 — RT France/Consejo (Asunto T-125/22) [«Política exterior y de seguridad común — Medidas restrictivas motivadas por acciones de Rusia que desestabilizan la situación de Ucrania — Prohibición temporal de emisión y suspensión de autorizaciones de radiodifusión respecto de los contenidos de determinados medios de comunicación — Inclusión en la lista de entidades a las que se

Ediciones Universidad de Salamanca | CC BY-NC-ND

aplican medidas restrictivas — Competencia del Consejo — Derecho de defensa — Derecho a ser oído — Libertad de expresión e información — Proporcionalidad — Libertad de empresa — Principio de no discriminación por razón de nacionalidad»]. DOUE C 340/40, de 5.9.2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62022TA0125 (03/05/2024).

Sentencia del Tribunal General (Gran Sala) de 27 de julio de 2022 -RT France contra el Consejo de la Unión Europea. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62022TJ0125 (13/05/2024).

Jurisprudencia nacional

Tribunal Constitucional

STC (Pleno), S 05-12-1984, nº 117/1984, BOE 305/1984, de 21 de diciembre de 1984, rec. 371/1982. BOE núm. 305, de 21 de diciembre de 1984. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-1984-27958 (14/03/2024).

STC 52/1983, de 17 de junio. BOE núm. 168, de 15 de julio de 1983. ECLI:ES:TC:1983:52. Disponible en: https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1983-19845.pdf .

STC 13/1985, de 31 de enero. BOE núm. 55, de 05 de marzo de 1985. ECLI:ES:TC:1985:13. Disponible en: https://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1985-3609.pdf (17/11/2024).

Declaración 1/1992, de 1 de julio (BOE núm. 177, de 24 de julio de 1992), del Tribunal Constitucional sobre reforma del artículo 13.2 CE. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/6944#:~:text=%221.,los%20nacionales%20de%20dicho%20Estado. https://www.boe.es/buscar/doc.php?id=BOE-A-1992-20403 (21/10/2023).

STC (Pleno), S 30-09-1999, nº 175/1999, BOE 263/1999, de 3 de noviembre de 1999, rec. 745/1990. BOE núm. 263, de 3 de noviembre de 1999. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-1999-21324 (14/03/2024).

STC (Pleno), S 13-04-2000, nº 104/2000, BOE 119/2000, de 18 de mayo de 2000, rec. 2300/1993. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2000-9229 (23/04/2024).

STC 297/2000, de 11 de diciembre de 2000. Recurso de amparo 1718/1997. BOE núm. 14, de 16 de enero de 2001. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-2001-1136 (12/11/2023).

STC 136/2024, de 5 de noviembre. BOE núm. 294, de 06 de diciembre de 2024. Disponible en: https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/31313#complete_resolucion&completa (14/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Otras sentencias y autos

La Sociedad de las Naciones como antecesora de las Naciones Unidas. Disponible en: https://www.un.org/es/about-us/history-of-the-un/predecessor (25/03/2024).

Pacto de la Liga de las Naciones. Disponible en: https://www.iri.edu.ar/publicaciones_iri/manual/Doc.Naciones%20Unidas/Pacto%20de%20la%20Sociedad%20de%20las%20Naciones.pdf (25/03/2024).

Discurso "Los Pilares de la Paz", pronunciado por Sir Winston Churchill en el Westminster College de Missouri (EE.UU.) el 5 de marzo de 1946. Disponible en: https://historia1imagen.cl/2007/09/11/wiston-churchill-el-telon-de-acero/ (21/07/2023).

Otras referencias web

Declaración Schuman, de 9 de mayo de 1950 sobre la creación de una Comunidad Europea del Carbón y del Acero -CECA-. Disponible en: https://european-union.europa.eu/principles-countries-history/history-eu/1945-59/schuman-declaration-may-1950_es (17/10/2023).

Declaración de independencia del ciberespacio de John Perry Barlow, presentado en Davos el 8 de febrero de 1996. Disponible en: https://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf (26/04/2024).

Acción Contra la Violencia Armada (Action On Armed Violence -AOAV). Disponible en: www.aoav.org.uk (26/03/2024).

Agencia de Información y Comunicaciones de la OTAN (NCI Agency). Disponible en: https://www.ncia.nato.int/ (22/02/2024).

Agencia de la UE para la Ciberseguridad. Disponible en: https://www.enisa.europa.eu/about-enisa/about/es (03/12/2023).

Agenda 2030 para el Desarrollo Sostenible, de Naciones Unidas. Disponible en: https://www.un.org/sustainabledevelopment/es/2015/09/la-asamblea-general-adopta-la-agenda-2030-para-el-desarrollo-sostenible/ (05/11/2023).

Asamblea General NNUU, informes anuales sobre el avance de la ciberamenaza y la utilización de las tecnologías de la información y las comunicaciones, así como su afectación a los derechos humanos, las libertades fundamentales y los principios del Derecho Internacional. Disponible en: https://disarmament.unoda.org/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/ (22/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Authority for European Political Parties and European Political Foundations (APPF). Disponible en: https://www.appf.europa.eu/appf/en/home/the-authority (15/05/2024).

BRICS como foro político y económico que desafía al poder tradicional representado por el G7, en base a ser los países más grandes y más poblados del mundo, y con enormes recursos naturales. Disponible en: https://datosmacro.expansion.com/paises/grupos/brics (11/01/2024).

CCN catálogo de cursos de formación y especialización. Disponible en: https://angeles.ccn-cert.cni.es/es/oferta-formativa (11/01/2025).

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE). Disponible en: https://ccdcoe.org/ (24/08/2023).

Centro de Fusión de Inteligencia de la OTAN (NIFC). Disponible en: https://web.ifc.bices.org/ (24/08/2023).

China Observers in Central and Eastern Europe CHOICE. Disponible en: https://chinaobservers.eu (25/10/2024).

Ciclo de Políticas de la UE EMPACT. Disponible en: https://www.europol.europa.eu/crime-areas-and-statistics/empact (23/11/2023).

Comentario del CICR al artículo 52 del Protocolo Adicional a los Convenios de Ginebra de 12 de agosto de 1949, relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I), de 8 de junio de 1977. Disponible en: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52/commentary/1987 (09/04/2024).

Computer Emergency Response Team de la UE (CERT-UE). Disponible en: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/computer-emergency-response-team-eu-institutions-bodies-and-agencies-cert-eu_es (03/12/2023).

Conferencia anual de Seguridad de Múnich. Disponible en: https://securityconference.org/en/ (24/08/2023).

Congreso de los Diputados. Disponible en: https://www.congreso.es (10/05/2023).

Cooperación Estructurada Permanente (CEP) para profundizar la cooperación en materia de defensa entre los Estados miembros de la UE. Disponible en: https://www.pesco.europa.eu (29/10/2023).

Consejo Económico y Social de las Naciones Unidas (ECOSOC). Disponible en: https://research.un.org/es/docs/ecosoc (22/02/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Contra-Hybrid Specialist Team. Disponible en: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html (25/10/2024).

Cyber Rapid Response Teams. Disponible en: https://crrts.eu/management.html (29/10/2023).

Departamento de Seguridad Nacional (España). Disponible en: www.dsn.gob.es/es (18/12(2023).

Diccionario inglés Britannica. Disponible en: https://www.britannica.com/dictionary/proxy (20/05/2024).

DISARM Foundation. Disponible en: https://www.disarm.foundation/ (22/03/2024).

Discurso del presidente Vladimir Putin en la Conferencia de Seguridad de Múnich de 10 de febrero de 2007. Disponible en: https://equilibriumglobal.com/wp-content/uploads/2018/01/Vladimir-Putin-Conferencia-Seguridad-Munich-2007.pdf (24/08/2023).

Eurojust. Disponible en: https://www.eurojust.europa.eu/es/node/2273 (25/11/2023).

European Forensic Science Area (ENFSI). Disponible en: https://enfsi.eu/ (02/12/2023).

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Disponible en: https://www.hybridcoe.fi/ (04/03/2024).

EUvsDisinfo. Disponible en: https://euvsdisinfo.eu/ (27/08/2024).

Fondo de las Naciones Unidas para la Infancia (UNICEF). Disponible en: https://www.unicef.org/es (02/11/2023).

Organización Mundial para la Salud (OMS). Disponible en: https://www.who.int/es/ (02/11/2023).

IBERIFIER. Disponible en: https://iberifier.eu/ (12/10/2024).

Interpol. Disponible en: https://www.interpol.int/es (10/05/2023).

Iniciativa "*Derecho cibernético internacional: kit de herramientas interactivo",* liderada por el NATO CCDCOE y participación de la National Cyber and Information Security Agency (NÚKIB), del Comité Internacional de la Cruz Roja (CICR), de la University of Exeter, de la Wuhan University y del U.S. Naval War College. Disponible en: https://cyberlaw.ccdcoe.org/wiki/Main_Page?oldid=4044 (07/04/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Joint Intelligence and Security División (JISD). Disponible en: https://www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html (25/10/2024).

MapInfluenceCE. Disponible en: https://mapinfluence.eu (25/10/2024).

Memoria del Consejo de Estado, del año 1992. Disponible en: https://www.consejo-estado.es/wp-content/uploads/2021/05/MEMORIA-1992.pdf (24/04/2024).

Mención a NNUU y su Programa Mundial de Alimentos, por el Comité Noruego del Nobel, con ocasión del premio del año 2020. Disponible en: https://www.un.org/es/about-us/nobel-peace-prize/wfp-2020 (17/07/2023).

NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE). Disponible en: https://ccdcoe.org/ (25/10/2024).

NATO´s Cyber Security Centre (Centro de Seguridad Cibernética de la OTAN). Disponible en: https://www.ncia.nato.int/what-we-do/cyber-security.html (29/09/2023).

NATO Strategic Communications Centre of Excellence (NATO StratCom COE). Disponible en: https://stratcomcoe.org/ (19/09/2023).

Objetivos de Desarrollo del Milenio, de Naciones Unidas. Disponible en: https://research.un.org/es/docs/dev/2000-2015 (02/11/2023).

Observatorio Complutense de Desinformación, de la Universidad Complutense de Madrid. Disponible en: https://www.ucm.es/observatoriodesinformacion/ (24/11/2024).

Observatorio Europeo de Medios Digitales. Disponible en: https://edmo.eu/ (12/10/2024).

Plan de Acción de Educación Digital de la UE. Disponible en: https://education.ec.europa.eu/es/focus-topics/digital-education/action-plan (03/03/2024).

Plan África para luchar contra la inmigración irregular, reforzar la presencia institucional española y luchar contra la pobreza como forma de afianzar la paz y la seguridad en el Continente. Disponible en: https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/Africa/III-Plan-%c3%81frica.aspx https://www.exteriores.gob.es/es/Comunicacion/Noticias/Paginas/Noticias/MICROSITE-FOCO-AFRICA.aspx (12/01/2024).

Poynter, Código de Principios internacionales de verificación profesional. Disponible en: https://www.poynter.org/fact-checking/2018/a-new-home-for-the-ifcn-code-of-principles/ (12/10/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Policía Nacional. Disponible en: https://www.policia.es/_es/tupolicia_conocenos_timeline (15/03/2024).

Politifact. Disponible en: https://www.politifact.com/ (12/10/2024).

Programa Mundial de Alimentos de las Naciones Unidas (WFP). Disponible en: www.es.wfp.org/quienes-somos (12/07/2023).

Proyecto European Medical Command. Disponible en: https://www.bundeswehr.de/en/organization/bundeswehr-medical-service-mmcc-emc- (29/10/2023).

Proyecto Cyber Law Toolkit, del CCDCOE. Disponible en: https://cyberlaw.ccdcoe.org/wiki/Main_Page (09/04/2024).

Red intercontinental de cables submarinos de fibra óptica. Disponible en: https://www.nbr.org/publication/submarine-cables/ (24/01/2025).

Red Internacional de Verificación de Datos. Disponible en: https://www.poynter.org/about/ (12/10/2024).

Red Europea de Normas de Verificación de Datos. Disponible en: https://efcsn.com/ (12/10/2024).

Red Europea de Organizaciones de Enlace para la Cibercrisis (EU-CyCLONe). Disponible en: https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone (22/10/2024).

Red Europea de Cooperación Electoral. Disponible en: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship-and-democracy/democracy-and-electoral-rights/european-cooperation-network-elections_en?prefLang=es (14/05/2024).

Relator Especial sobre el derecho a la privacidad y su mandato. Disponible en: https://www.ohchr.org/es/special-procedures/sr-privacy (03/03/2024).

Reporters´Lab. Disponible en: https://reporterslab.org/ (13/10/2024).

Sistema de Alerta Rápida de la UE contra la amenaza desinformativa. Seguimiento en prensa de su presentación en marzo de 2019. Disponible en: https://elderecho.com/la-ue-lanza-este-semana-sistema-alerta-rapida-la-desinformacion https://www.eitb.eus/es/noticias/sociedad/detalle/6275323/la-ue-lanza-su-sistema-alerta-rapida-desinformacion-18-marzo/ (01/09/2024).

Unidad Cibernética Conjunta de la UE. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit (03/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Viginum, dependiente de la Secretaría General de Defensa y de la Seguridad Nacional del gobierno francés. Disponible en: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361 (04/05/2024).

Atentados del 11 de marzo de 2004, en Madrid. Disponible en: https://elpais.com/diario/2004/03/22/espana/1079910017_850215.html https://edition.cnn.com/2004/WORLD/europe/03/11/spain.blasts/index.html https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2024/060324-marlaska-exposicion-11m.aspx (09/03/2024).

Guerra futura: el auge de las guerras híbridas. Disponible en: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars (09/03/2024).

Atentados del 7 de julio de 2005 en la red de transporte público del centro de Londres. Disponible en: https://web.archive.org/web/20051005095829/http://www.liberation.fr/page.php?Article=309592 https://elpais.com/internacional/2005/07/07/actualidad/1120687212_850215.html (10/03/2024).

Evento del Consejo Económico y Social de las Naciones Unidas, sobre Seguridad cibernética y desarrollo, celebrado en Nueva York en diciembre de 2011. Disponible en: https://www.un.org/es/desa/seguridad-cibernetica (18/02/2024).

El Comité del Premio Nobel subraya la contribución de la UE a la transformación del continente europeo en un entorno pacífico, próspero y democrático. Disponible en: https://www.nobelprize.org/prizes/peace/2012/summary/ https://www.europarl.europa.eu/news/es/headlines/eu-affairs/20121012STO53551/la-union-europea-premio-nobel-de-la-paz-2012 (29/09/2023).

Caso Snowden: filtración de datos secretos de la NSA. Disponible en: https://cnnespanol.cnn.com/2013/06/10/quien-es-edward-snowden-el-hombre-que-filtro-datos-secretos-de-la-nsa/ https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/ https://www.washingtonpost.com/magazine/2020/05/11/2013-edward-snowden-leaked-top-secret-national-security-agency-documents-showing-how-us-was-spying-its-citizens-heres-what-happened-next/ (07/02/2024).

Naufragio de una embarcación con alrededor de 500 personas en las costas de la isla italiana de Lampedusa, el 3 de octubre de 2013 Disponible en: https://www.bbc.com/mundo/noticias/2013/10/131003_lampedusa_migrantes_cuerno_africa_cch.amp (21/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Manifestaciones y disturbios del *Euromaidán* en Kiev, de diciembre de 2013, que finalmente obligan al presidente Yanukovich a huir del país hacia Rusia en febrero del 2014. Disponible en: https://www.lavanguardia.com/internacional/20140222/54401609478/ucrania-yanukovich-elecciones.html https://www.elmundo.es/internacional/2014/02/20/5305d599268e3ecd738b4573.html https://world.time.com/2014/02/22/ukraines-president-flees-protestors-capture-kiev/ (19/09/2023).

Estrategia seguida por Rusia en mayo de 2014 cuando, con el apoyo de tropas rusas no identificadas -los *hombrecillos de verde*-, da cobertura al proceso de autoproclamación de la República de Crimea. Disponible en: https://www.bbc.com/mundo/noticias/2014/03/140311_ucrania_rusia_soldados_crimea_jgc (04/05/2024).

Crisis en Ucrania: condenado el referéndum "ilegal" de Crimea. BBC News 6 marzo 2014. Disponible en: https://www.bbc.com/news/world-europe-26475508 (19/09/2023).

Coalición Internacional contra DAESH, acordada en la cumbre de la OTAN de Gales, celebrada entre los días 4 y 5 de septiembre de 2014. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/lucha-contra-DAESH-un-compromiso-reforzado (15/09/2024).

La Infosfera: el paradigma del nuevo siglo. Disponible en: https://infosfera.com.ar/la_infosfera.asp https://www.bbc.com/mundo/noticias/2014/11/141128_infosfera_filosofia_tecnologia_finde_dv (22/02/2024).

Atentado el 7 de enero de 2015 en las oficinas del semanario satírico Charlie Hebdo y otras zonas de París en los dos días siguientes. Disponible en: https://www.independent.co.uk/news/world/europe/charlie-hebdo-shooting-10-killed-as-shots-fired-at-satirical-magazine-headquarters-according-to-reports-9962337.html https://elpais.com/internacional/2015/02/14/actualidad/1423930814_931343.html https://www.elconfidencial.com/mundo/2015-02-15/un-segundo-tiroteo-en-una-sinagoga-pone-a-copenhague-en-alerta-terrorista-maxima_712337/ (10/03/2024).

Atentados simultáneos el viernes 13 de noviembre de 2015, en la sala Bataclán de París y en el suburbio de Saint-Denis. Disponible en: https://www.lemonde.fr/societe/article/2015/11/13/fusillade-meurtriere-a-paris_4809485_3224.html https://www.rtve.es/noticias/atentados-paris/en-vivo/ (10/03/2024).

Doble atentado en Bruselas del 22 de marzo de 2016, en el aeropuerto internacional de Zaventem y en la estación de metro de Maelbeek. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.dsn.gob.es/es/actualidad/sala-prensa/atentados-terroristas-bruselas-22-marzo-2016
https://www.elmundo.es/internacional/2016/03/22/56f0f2cf22601d20498b4648.html
https://www.lavanguardia.com/internacional/20160328/40714242870/cifra-muertos-atentados-bruselas-eleva-35.html (10/03/2024).

Atentado de Niza del 14 de julio de 2016 en la celebración del Día Nacional de Francia. Disponible en: https://www.bbc.com/mundo/noticias-internacional-36800755
https://www.rtve.es/noticias/atentado-niza/ (10/03/2024).

Campaña de desinformación en las elecciones presidenciales francesas de mayo de 2017, contra el candidato Emmanuel Macron. Disponible en: https://cnnespanol.cnn.com/2017/05/06/hackean-la-campana-de-emmanuel-macron-en-francia/ (13/05/2024).

Atentado perpetrado el 22 de mayo de 2017 en el estadio Manchester Arena. Disponible en: https://www.bbc.com/news/uk-england-manchester-40010124
https://elpais.com/internacional/2017/05/23/actualidad/1495525781_483597.html
https://www.bbc.com/news/uk-england-manchester-40008389 (10/03/2024).

Atentado del 3 de junio de 2017 en el puente de Londres y en Borough Market. Disponible en: https://www.telegraph.co.uk/news/2017/06/05/london-bridge-attack-latest-gunshots-heard-police-launch-fresh/
https://elpais.com/internacional/2017/06/06/actualidad/1496744463_102889.html
(10/03/2024).

Doble atentado en la Rambla de Barcelona y en Cambrils del 17 de agosto de 2017. Disponible en: https://www.dsn.gob.es/en/actualidad/sala-prensa/nota-informativa-sobre-atentados-barcelona-cambrils
https://www.rtve.es/noticias/20170818/atentado-barcelona-directo/1599220.shtml
(10/03/2024).

Inauguración el 2 de octubre de 2017, en Helsinki, del Centro Europeo de Excelencia Contra las Amenazas Híbridas (Hybrid CoE). Disponible en: https://www.lavanguardia.com/politica/20171002/431759376364/otan-y-ue-inauguran-en-helsinki-un-centro-europeo-contra-amenazas-hibridas.html
(15/09/2024).

El Parlamento Europeo advierte de la injerencia rusa en el proceso independentista catalán de octubre de 2017. Disponible en: https://www.elmundo.es/cataluna/2021/11/09/61896962e4d4d840138b458a.html
https://www.elperiodico.com/es/politica/20240207/parlamento-europeo-injerencia-rusia-cataluna-proces-97875532
https://elpais.com/espana/2024-02-06/bruselas-advierte-contra-la-injerencia-rusa-en-el-proces-y-pide-investigar-si-el-kremlin-infiltro-agentes-en-la-ue.html
https://elpais.com/espana/2024-02-26/un-informe-de-la-inteligencia-europea-traza-vinculos-entre-el-independentismo-catalan-y-el-kremlin.html (13/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Atentados en las ciudades francesas de Carcasona y Trèbes del 23 de marzo de 2018. Disponible en: https://www.lavanguardia.com/internacional/20180323/441859630190/hombre-armado-retiene-personas-supermercado-sur-francia.html https://www.france24.com/en/20180323-liveblog-shooting-hostage-taking-southwest-france-carcassone-trebes (10/03/2024).

Atentado del martes 11 de diciembre de 2018 en Estrasburgo. Disponible en: https://www.lefigaro.fr/actualite-france/2018/12/12/01016-20181212ARTFIG00276-cherif-c-un-delinquant-tombe-dans-l-islam-radical.php https://elpais.com/internacional/2018/12/11/actualidad/1544557124_955716.html (10/03/2024).

Consideraciones sobre el presupuesto de NNUU en el ejercicio 2019. Disponible en: https://news.un.org/es/story/2019/10/1463522 https://www.dw.com/es/la-onu-necesita-dinero-por-qu%C3%A9-sus-arcas-est%C3%A1n-vac%C3%ADas/a-50762944 (26/03/2024).

Toma de Baguz, último enclave territorial controlado por DAESH, y fin del califato y la derrota de la organización terrorista tras más de cinco años de combates. Disponible en: https://elpais.com/internacional/2019/03/23/actualidad/1553329466_793785.html https://www.france24.com/es/20190211-siria-fds-estado-islamico-trump (17/03/2024).

Declaración del Alto Representante en nombre de la UE sobre el respeto del orden basado en normas en el ciberespacio de 12 de abril de 2019. Disponible en: https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/ (19/08/2024).

Información sobre la sentencia del procés y la repercusión de los disturbios en Barcelona y resto de Cataluña. Disponible en: https://www.elperiodico.com/es/politica/20191017/barcelona-catalunya-sentencia-proces-directo-7680256 https://www.elconfidencial.com/espana/cataluna/2019-10-27/protestas-barcelona-disturbios-26-octubre-cataluna_2301788/ https://elpais.com/espana/2024-03-18/la-audiencia-nacional-rechaza-el-recurso-de-la-fiscalia-y-avala-seguir-investigando-por-terrorismo-el-caso-tsunami.html https://www.rtve.es/noticias/20240318/audiencia-nacional-avala-investigar-terrorismo-tsunami-democratic/16021204.shtml (19/03/2024).

Atentado en la Prefectura de la Îlle de la Cité en París del 3 de octubre de 2019. Disponible en: https://www.bbc.com/mundo/noticias-internacional-49919687 https://www.lemonde.fr/societe/article/2019/10/04/ce-que-l-on-sait-de-l-attaque-a-la-prefecture-de-police-de-paris_6014194_3224.html (10/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Proyectos financiados por la UE a través de los fondos Horizonte 2020, para educar y concienciar a los ciudadanos frente a las noticias falsas y la desinformación. Disponible en: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_es#proyectos-existentes (14/05/2024).

45º Informe de situación del COVID-19, de marzo de 2020. Disponible en: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4 (07/09/2024).

Operación Balmis, por la que el Ministerio de Defensa desplegó al ejército español en todo el territorio nacional para luchar contra la propagación del COVID-19. Disponible en:https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/defensa/Paginas/2020/240320-visita.aspx (12/05/2024).

Atentado en la basílica católica de Notre-Dame de Niza, el 29 de octubre de 2020. Disponible en: https://www.bbc.com/mundo/noticias-internacional-54732252 https://www.elmundo.es/internacional/2020/10/29/5f9a81effc6c83045b8b45be.html https://www.rtve.es/noticias/20201030/atentado-terrorista-niza-se-sabe-del-ataque-dejo-tres-muertos-iglesia/2050900.shtml (10/03/2024).

Controversia a raíz de la aprobación del Procedimiento de actuación contra la desinformación, de 2020, referida al *Ministerio de la Verdad*. Disponible en: https://www.hayderecho.com/2020/12/19/la-orden-contra-la-desinformacion-y-el-ministerio-de-la-verdad/ https://www.abc.es/espana/abci-sanchez-impone-secreto-reuniones-ministerio-verdad-202104160119_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Fespana%2Fabci-sanchez-impone-secreto-reuniones-ministerio-verdad-202104160119_noticia.html https://www.eldebate.com/espana/20211203/ministerio-verdad-sanchez-descubierto.html (10/12/2024).

Mención a NNUU del Comité Noruego del Nobel, con ocasión del premio del año 2001. Disponible en: https://www.un.org./es/about-us/nobel-peace-prize/kofi-annan-2001 (24/07/2023).

Financiación digital en el marco financiero plurianual 2021-2027. Disponible en: https://digital-strategy.ec.europa.eu/es/activities/funding-digital (03/03/2024).

En marzo de 2021 el buque portacontenedores Ever Given se quedó atascado durante casi una semana en el Canal de Suez, cortando el paso al transporte marítimo mundial que transita por esa ruta y generando con ello pérdidas millonarias. Disponible en: https://www.nytimes.com/es/2021/07/19/espanol/canal-suez-evergiven.html https://www.lavanguardia.com/internacional/20210329/6615967/canal-suez-buque-barco-encallado-ultimas-noticias-en-directo.html (08/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Marruecos llama a consultas a su embajadora en Madrid en mayo de 2021. Disponible en: https://www.europapress.es/nacional/noticia-marruecos-llama-consultas-embajadora-madrid-20210518182948.html
https://elpais.com/espana/2021-05-18/espana-convoca-a-la-embajadora-de-marruecos.html
https://www.elsaltodiario.com/control-fronteras/acuerdo-ue-pesca-externalizacion-fronteras-que-hay-detras-ultima-crisis-migratoria-marruecos-ceuta
https://elpais.com/espana/2021-05-18/el-ejercito-se-despliega-para-controlar-las-calles-de-ceuta-tras-la-entrada-de-5000-inmigrantes.html
https://elpais.com/espana/2021-05-19/que-esta-pasando-en-ceuta-claves-de-la-crisis-entre-espana-y-marruecos.html (04/05/2024).

Fundación Víctimas del Terrorismo, informe sobre víctimas de ETA. Disponible en: https://www.abc.es/espana/abci-historia-cifras-853-asesinatos-3500-atentados-y-mas-7000-victimas-202110200115_noticia.html
https://www.rtve.es/noticias/20211020/cifras-barbarie-eta-mas-850-asesinatos-2600-heridos-casi-90-secuestrados/2195448.shtml
https://fundacionvt.org/fundacion/victimas-mortales-de-eta/ (09/03/2024).

La soberanía digital de Europa: de regulador a superpotencia en la era de la rivalidad entre EE.UU. y China. Telefónica Digital Policy Lab. Disponible en: https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/06/COLECCION-DE-ENSAYOS-FINAL.pdf (03/02/2024).

Comunicado de Prensa del Proyecto PESCO *Movilidad Militar* como área de interés compartido entre socios OTAN y UE. Disponible en: https://www.consilium.europa.eu/en/press/press-releases/2021/05/06/pesco-canada-norway-and-the-united-states-will-be-invited-to-participate-in-the-project-military-mobility/ (01/11/2023).

El Consejo de Seguridad de Naciones Unidas celebra su primer debate de carácter público sobre el mantenimiento de la paz y la seguridad en el ciberespacio. Disponible en: https://news.un.org/es/story/2021/06/1493862
https://www.france24.com/es/minuto-a-minuto/20210629-el-consejo-de-seguridad-de-la-onu-debate-sobre-ciberseguridad-una-preocupaci%C3%B3n-creciente
https://protecdatalatam.com/noticias/ciberseguridad-el-consejo-de-seguridad-de-la-onu-inicia-su-primer-debate-formal-sobre-ciberseguridad/ (22/02/2024).

Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. General Assembly. Conference room paper. A/AC.290/2021/CRP.2. Disponible en: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (29/02/2024).

Iniciativa *Industry Engagement* de la European Defence Agency. Disponible en: https://eda.europa.eu/what-we-do/industry-engagement (01/11/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Russia´s Strategy In Cyberspace, publicado en junio de 2021 por el NATO STRATCOM COE y el NATO Cooperative Cyber Defence COE. Disponible en: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf (01/04/2024).

Maniobras militares estratégicas rusas ZAPAD-21. Disponible en: https://informnapalm.org/es/comienzo-de-las-maniobras-oeste-2021-y-el-traslado-de-los-cazas-rusos-su-30-sm-a-belarus/ (19/09/2023).

Vinculación entre Rusia y el nacionalismo independentista catalán. Disponible en: https://www.elmundo.es/cataluna/2021/11/09/61896962e4d4d840138b458a.html https://www.elmundo.es/cataluna/2024/02/08/65c5394221efa07f538b45a9.html https://www.infobae.com/america/agencias/2024/01/29/un-juez-en-espana-advierte-que-rusia-estaba-dispuesta-a-apoyar-al-independentismo-catalan/ (04/05/2024).

El Kremlin convierte el victimismo en un arma. Disponible en: https://euvsdisinfo.eu/the-kremlin-weaponising-victimhood/ (17/10/2023).

Acelerador de Innovación de Defensa para el Atlántico Norte (DIANA), presentada en la Cumbre de Bruselas de 2021, en el marco de la Agenda OTAN 2030. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/bot__74.pdf (29/09/2023).

El terrorismo en la UE: datos y cifras (2010-2021). Página web del Consejo Europeo/Consejo de la Unión Europea. Disponible en: https://www.consilium.europa.eu/es/infographics/terrorism-eu-facts-figures/ (10/03/2024).

Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts. Colonel Charles J. Dunlap, Jr., USAF. Noviembre de 2021. Disponible en: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=6193&context=faculty_scholarship (16/11/2024).

Desencuentros diplomáticos entre España y Marruecos respecto a los límites de las aguas territoriales de ambos países. Disponible en: https://www.lavanguardia.com/politica/20211124/7886445/espana-protesta-piscifactoria-marroqui.html (13/01/2024).

Estrategia de las maniobras militares ZAPAD 21, iniciadas en septiembre de 2021 en la frontera de Bielorrusia con Ucrania para, meses después, favorecer la invasión. Disponible en: https://es.euronews.com/2022/02/20/rusia-y-bielorrusia-prolongan-sus-maniobras-a-las-puertas-de-ucrania https://informnapalm.org/es/comienzo-de-las-maniobras-oeste-2021-y-el-traslado-de-los-cazas-rusos-su-30sm-a-belarus/ (04/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Acuerdos de Estambul, de marzo de 2022. Disponible en: https://urgente24.com/mundo/acuerdos-estambul-el-plan-ruso-frenar-la-guerra-ucrania-n580406
https://mondiplo.com/la-pista-de-estambul
https://diario-octubre.com/2024/06/18/el-new-york-times-publica-el-tratado-de-paz-firmado-en-2022-por-ucrania-y-rusia/ (14/12/2024).

Conferencia sobre el Futuro de Europa, de 9 de mayo de 2022. Disponible en: https://www.consilium.europa.eu/es/policies/conference-on-the-future-of-europe/ (22/10/2023).

Informe Defending Ukraine: Early Lessons from the Cyber War, de fecha 22 de junio de 2022. Disponible en: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (19/09/2023).

Plataformas que participan y firman el Código Reforzado de Buenas Prácticas contra la Desinformación. Junio de 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation (14/09/2024).

Ejercicios de ciberseguridad Cyber Europe. Disponible en: https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2022-testing-the-resilience-of-the-european-healthcare-sector (12/01/2025).

Análisis del impacto de la guerra de agresión rusa contra Ucrania en la delincuencia y el terrorismo en Europa. Disponible en: https://www.washingtonpost.com/national-security/2022/05/14/ukraine-weapons-trafficking/
https://www.ft.com/content/bce78c78-b899-4dd2-b3a0-69d789b8aee8 (29/12/2023).

Programa WiFI4EU. Disponible en: https://digital-strategy.ec.europa.eu/es/activities/wifi4eu (03/03/2024).

Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil. Disponible en: https://www.dsn.gob.es/ca/node/18297 (14/12/2024).

Sospechas de corrupción entre los europarlamentarios. Disponible en: https://www.europarl.europa.eu/news/es/press-room/20221212IPR64541/escandalo-de-corrupcion-eurodiputados-plantean-cambios-para-mas-transparencia
https://www.bbc.com/mundo/noticias-internacional-63951652
https://elpais.com/internacional/2022-12-13/las-claves-de-qatargate-el-escandalo-de-sobornos-que-ha-sacudido-el-parlamento-europeo.html (20/10/2023).

Conferencia del AR/VP Josep Borrell en Madrid, en la Fundación Carlos de Amberes, el martes 11 de octubre de 2022, en el marco de análisis de la guerra en Ucrania.

Ediciones Universidad de Salamanca | CC BY-NC-ND

Disponible en: https://elpais.com/internacional/2022-10-11/borrell-en-una-autocritica-a-la-ue-nuestra-prosperidad-estaba-basada-en-la-energia-barata-de-rusia-y-las-oportunidades-de-negocio-con-china.html (30/10/2023).

Caso de diputados del Parlamento Europeo investigados por blanqueo de capitales, corrupción y participación en organización delictiva, en base a supuestas transferencias de información y actuaciones que beneficiaban a Qatar. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0448_ES.html https://elpais.com/internacional/2023-03-06/qatargate-la-defensora-del-pueblo-europea-pide-explicaciones-por-los-viajes-pagados-por-qatar-a-un-alto-funcionario-de-la-comision.html https://valenciaplaza.com/qatargate-salpica-corrupcion-gobierno-union-europea (04/05/2024).

Cuestión de la soberanía sobre las ciudades españolas de Ceuta y Melilla. Disponible en: https://en.hespress.com/51054-morocco-has-no-land-borders-with-spain-says-government-assuring-enclaves-are-occupied.html (13/01/2024).

El 22 de noviembre de 2022, la página web oficial del Parlamento Europeo sufre un ataque de denegación de servicio atribuida a un grupo pro-Kremlin. Disponible en: https://es.euronews.com/my-europe/2022/11/23/cae-la-web-del-parlamento-europeo-tras-aprobar-una-resolucion-contra-rusia https://www.elmundo.es/internacional/2022/11/23/637e3186fc6c837b508b45d5.html (18/05/2024).

Documento del Hybrid CoE de noviembre de 2022, titulado Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework DISARM. Disponible en: https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf (28/09/2024).

“Cable news and COVID-19 vaccine uptake”. Disponible en: Matteo Pinna, Léo Picard y Christoph Goessmann. Cable news and COVID-19 vaccine uptake. Sci Rep 12, 16804 (2022). Disponible en: https://doi.org/10.1038/s41598-022-20350-0 (07/09/2024)

Teorías conspirativas y difusión de narrativas desinformativas recogidas en la prensa española. Disponible en: https://elpais.com/ciencia/2023-02-22/terraplanismo-chemtrails-y-negacionistas-de-la-pandemia-unas-jornadas-de-la-universidad-de-cordoba-dan-voz-a-los-censurados.html https://www.newtral.es/teoria-conspiracion-chemtrails/20230509/ https://www.elconfidencial.com/espana/2023-02-03/rafapa-jefe-conspiracion-espana-clones_3569156/ (11/01/2025).

Declaración Conjunta de la UE y la OTAN, de 10 de enero de 2023, de apoyo a Ucrania. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/ (29/09/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Efectos del crimen organizado en enero de 2023 en Ecuador, con acciones de alta violencia simultáneas y perfectamente coordinadas como el asalto al canal TC Televisión, algaradas callejeras, secuestro de policías y motines con rehenes en prisiones, que llevan al Presidente Daniel Noboa a decretar un conflicto armado interno en el país. Disponible en: https://cnnespanol.cnn.com/2024/01/10/que-es-conflicto-armado-interno-noboa-ecuador-orix/
https://www.rtve.es/noticias/20240111/ecuador-crimen-organizado/2470865.shtml (11/01/2024).

Manual de Seguridad Humana. Un enfoque integrado para la consecución de los Objetivos de Desarrollo Sostenible y los ámbitos de acción prioritarios de la comunidad internacional y el sistema de las Naciones Unidas. Disponible en: https://www.un.org/humansecurity/wp-content/uploads/2023/02/HS-handbook-Spanish.pdf (22/02/2024).

Fog of war: how the Ukraine conflict transformed the cyber threat landscape. 16 de febrero de 2023. Disponible en: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/ (02/04/2024).

Propuesta del Presidente Lula da Silva, de febrero de 2023, para alcanzar salida diplomática a la guerra de Ucrania. Disponible en: https://elpais.com/internacional/2023-02-02/brasil-plantea-una-tercera-via-para-propiciar-una-solucion-dialogada-a-la-guerra-de-ucrania.html
https://cnnespanol.cnn.com/2023/04/24/analisis-presidente-brasil-lanza-coalicion-paz-ucrania-camina-delgada-linea-trax/
https://www.swissinfo.ch/spa/economia/ha-llegado-el-momento-de-hablar-de-paz-en-ucrania/48850064 (02/03/2024).

Espionaje tecnológico entre China y EE.UU. en relación con los cazabombarderos de quinta generación J-20 *Mighty Dragon*, F-22 *Raptor* y F-35 *Lightning II.* Disponible en: https://www.larazon.es/internacional/increible-historia-familia-china-que-logro-espiar-aviones-combate-f35-eeuu_20231227658c61b8a4afb00001d07822.html
https://www.diariolasamericas.com/economia/china-crea-aviones-combate-tecnologia-robada-eeuu-n5332195 (27/03/2024).

Detención del hacker Alcasec por la Policía Nacional española, en marzo de 2023. Disponible en: https://elpais.com/espana/2023-04-03/detenido-el-joven-hacker-alcasec-en-la-causa-sobre-el-ciberataque-al-poder-judicial.html
https://www.abc.es/espana/alcasec-detenido-hackeo-punto-neutro-judicial-20230403113056-nt.html
https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=15523#
https://www.larazon.es/espana/audiencia-nacional-luz-verde-procesamiento-dos-hackers-que-atacaron-punto-neutro-judicial_202401046596af29cf86730001c74a71.html (12/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Nota de prensa del Ministerio de Defensa sobre el ejercicio Locked Shields 2023. Disponible en: https://emad.defensa.gob.es/prensa/noticias/2023/04/Listado/230425-ni-mcce-locked-shield.html (01/03/2024).

Primera reunión del Schuman Security and Defence Partnership Forum, entre el 20 y 21 de marzo de 2023. Disponible en: https://www.eeas.europa.eu/eeas/schuman-security-and-defence-forum_en (07/11/2023).

Comunicado de Prensa emitido por el Consejo Europeo, el 23 de marzo de 2023. Disponible en https://www.consilium.europa.eu/es/press/press-releases/2023/03/23/readout-of-the-working-session-of-the-european-council-with-the-un-secretary-general/ (19/10/2023).

En mayo de 2023, con la llegada de Elon Musk, Twitter cambia su nombre comercial a X y se retira del compromiso con el Código Reforzado de Buenas Prácticas de la UE. Seguimiento en prensa de esta decisión. Disponible en: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation
https://www.europapress.es/portaltic/socialmedia/noticia-twitter-retira-codigo-buenas-practicas-materia-desinformacion-ue-20230529102243.html (01/09/2024)

Discurso de Putin que justifica la decisión de iniciar la *operación militar especial* rusa para defender al pueblo ucraniano que lleva años sufriendo la persecución y el genocidio por parte del régimen de Zelenski, para lo cual es necesario proceder a la desmilitarización y desnazificación de Ucrania. Disponible en: https://www.bbc.com/mundo/noticias-internacional-60524958
https://elpais.com/internacional/2023-06-16/putin-zelenski-cubre-a-los-monstruos-neonazis.html (03/04/2024).

Atentado el martes 18 de abril de 2023 en Duisburgo (Alemania). Disponible en: https://es.euronews.com/2023/04/23/alemania-policia-detiene-a-un-sospechoso-por-el-ataque-con-cuchillos-en-un-gimnasio
https://www.agenzianova.com/es/news/germania-al-via-il-processo-contro-laggressore-di-duisburg-ritenuto-un-sostenitore-dello-stato-islamico/
https://www.latimes.com/espanol/internacional/articulo/2023-04-18/alemania-4-heridos-al-ser-apunalados-en-gimnasio (25/08/2024).

Consorcios en el marco del Programa Europeo de Inversión en Defensa (EDIP). Disponible en: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/european-defence-investment-programme
https://cnv-consulting.eu/wp-content/uploads/2023/04/1-CV-Consulting-EDIP-Rebuilding-European-Defence-by-Strengthening-our-Industry.pdf (07/11/2023).

En mayo de 2024 la Agencia de Ciberseguridad y Seguridad de las Infraestructuras y otros organismos nacionales e internacionales de ciberseguridad emiten un aviso alertando de que grupos hacktivistas rusos atacan cada vez más sistemas de tecnología operativa a pequeña escala en Norteamérica y Europa. Disponible en: Russian Hackers Attacking Small-scale Infrastructure Sectors (gbhackers.com) (05/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Compra de votos por correo en Melilla. Disponible en: https://elpais.com/espana/2023-05-23/al-menos-seis-detenidos-por-la-compra-de-votos-en-melilla.html https://www.elconfidencial.com/espana/2023-05-18/melilla-duplica-record-voto-correo-acusaciones-fraude-masivo_3631502/ (14/05/2024).

Cumbre del G7 de Hiroshima (Japón), celebrada del 19 al 21 de mayo de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/05/20/g7-hiroshima-leaders-communique/ (29/09/2023).

Europol Operación Encrochat. Disponible en: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized (23/11/2023).

En junio de 2023 se inauguró en Madrid una nueva Oficina de Programas de la Oficina de Lucha contra el Terrorismo de las Naciones Unidas. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2023/060623-onu-inaugura-madrid-oficina-terrorismo.aspx (10/03/2024).

Campaña de migración irregular impulsada desde Bielorrusia hacia Lituania, Letonia y Polonia a raíz del deterioro de relaciones con la UE. Disponible en: https://www.dw.com/es/lituania-r%C3%A9cord-de-inmigrantes-por-crisis-con-bielorrusia/a-58679564 https://es.euronews.com/2023/07/13/migrantes-en-europa-muchos-cruzan-a-lituania-desde-bielorrusia-para-quedarse-o-continuar-a https://www.rtve.es/noticias/20211118/bielorrusia-polonia-nueva-frontera-desinformacion/2225622.shtml (26/10/2024).

El grupo hacktivista prorruso NoName057(16) llevó a cabo una serie de ciberataques contra diversas instituciones españolas vinculadas con la seguridad y transparencia del proceso de elecciones generales de 2023, incidiendo especialmente en la jornada del 23 de julio en la propia página web del Ministerio del Interior, responsable de la seguridad del proceso. Disponible en: https://www.elconfidencial.com/espana/2023-07-23/elecciones-23j-hackers-prorrusos-atacan-interior-votacion_3706141/ (03/05/2024).

Conflictividad en la valla fronteriza entre España y Marruecos. Disponible en: https://fr.hespress.com/323865-melilla-bruits-de-bottes-pres-de-la-frontiere-marocaine.html (13/01/2024).

Declaraciones del presidente turco Tayyip Erdogan, de julio de 2023, sobre entrada de nuevos socios en la OTAN. Disponible en: https://es.euronews.com/2023/07/10/erdogan-apoyara-el-ingreso-de-suecia-en-la-otan-si-la-ue-reanuda-negociaciones-con-turquia (20/09/2023).

Nota de prensa del DSN sobre el golpe de Estado en Níger, de 8 de agosto de 2023. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/situaci%C3%B3n-n%C3%ADger-tras-golpe-estado (27/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Nota de prensa de VIASAT en la 26ª edición de la Conferencia de Ciberseguridad Black Hat, de agosto de 2023. Disponible en: https://cyberscoop.com/viasat-ka-hack-black-hat/ (20/09/2023).

INCIBE definición de tipos de hacktivismo. Disponible en: https://www.incibe.es/ed2026/talento-hacker/blog/explicacion-de-los-distintos-tipos-de-hackers (15/04/2024).

Cumbre de Yedá, agosto 2023. Disponible en: https://europapress.es/internacional/noticia-reunion-yeda-coincide-plan-paz-respete-soberania-integridad-territorial-ucrania-20230805225247.html (22/09/2023).

Nota de prensa del ejercicio militar MILEX 23, de septiembre de 2023. Disponible en: https://emad.defensa.gob.es/prensa/noticias/2023/09/Listado/230918-ni-inicio-milex-23.html (06/11/2023).

El 26 de septiembre de 2022 se producen varias explosiones que afectan a los gasoductos Nord Stream del mar Báltico. Para la comunidad internacional la principal sospechosa es Rusia. Disponible en: https://elpais.com/internacional/2023-02-27/el-sabotaje-del-nord-stream-cinco-meses-de-sospechas-y-teorias-conspirativas.html (04/05/2024).

Crisis humanitaria de la Isla de Lampedusa, de septiembre de 2023. Disponible en: https://es.euronews.com/2023/09/17/crisis-migratoria-ursula-von-der-leyen-y-giorgia-meloni-aterrizan-en-lampedusa (27/10/2023).

Estrategia de presión por parte de Túnez -y Libia- hacia la UE para alcanzar acuerdos económicos ventajosos que se apoya, en gran medida, en la gestión de los flujos migratorios con destino a Lampedusa (Italia). Disponible en: https://elpais.com/internacional/2023-09-26/tunez-pone-en-entredicho-el-acuerdo-migratorio-con-la-ue-al-bloquear-otra-visita-europea-al-pais.html https://gaceta.es/europa/tunez-presiona-a-italia-con-mas-de-130-embarcaciones-en-un-solo-dia-que-dejan-en-lampedusa-a-mas-5-000-inmigrantes-ilegales-20230913-1559/ (04/05/2024).

Artículo de opinión del presidente Charles Michel, "El mundo mira a nuestro continente europeo", de 5 de octubre de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/10/05/the-world-is-watching-our-european-continent-op-ed-article-by-president-charles-michel/ (30/10/2023).

Rivalidad en capacidades ofensivas de las Fuerzas Armadas españolas y marroquíes. Disponible en: https://fr.hespress.com/336631-le-maroc-domine-dans-le-domaine-des-blindes-face-a-lespagne.html https://www.eldebate.com/espana/defensa/20240113/espana-mantiene-contundente-supremacia-militar-sobre-marruecos_166686.html (13/01/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Consecuencias del veto de EE.UU. sobre la resolución que, auspiciada por Brasil, pretende una condena de los ataques de Hamas a Israel y acordar el alto el fuego para permitir la entrada de ayuda humanitaria a la Franja de Gaza. 18 de octubre de 2023. Disponible en: https://elpais.com/internacional/2023-10-18/el-veto-de-ee-uu-frustra-una-resolucion-para-un-alto-el-fuego-humanitario-en-el-consjeo-de-seguridad-de-la-onu.html
https://www.latimes.com/espanol/internacional/articulo/2023-10-18/EE.UU.-veta-resolucion-de-la-onu-que-condena-ataques-de-hamas-a-israel-y-violencia-contra-civiles (30/10/2023).

Reuniones de los ministros de Defensa aliados el 11 de octubre y el 29 de noviembre en la sede de la OTAN. Disponible en: https://www.europapress.es/internacional/noticia-zelenski-viaja-sorpresa-belgica-participar-reunion-grupo-ramstein-otan-20231011083314.html
https://www.defensa.gob.es/Galerias/gabinete/red/2023/11/RED410.pdf
https://www.swissinfo.ch/spa/ucrania-guerra-otan_la-otan-contin%C3%BAa-su-apoyo-a-ucrania-y-avisa-de-que-rusia-hipoteca-su-futuro-a-china/49016748
(08/12/2023).

Hipotética ampliación de la UE para la adhesión de Turquía, Montenegro, Serbia, Macedonia del Norte, Albania, Bosnia y Herzegovina, Ucrania, Moldavia, Georgia y Kosovo. Con este motivo, el 2 de octubre de 2023 el AR/VP Josep Borrell convoca a los Ministros de Exteriores de la Unión Europea en Kiev. Disponible en: https://www.eeas.europa.eu/delegations/ukraine/ukraine-press-remarks-high-representative-josep-borrell-ahead-eu-foreign-ministers-meeting-kyiv_en?s=232
(29/10/2023).

Ataques terroristas el viernes 13 de octubre de 2023 en Arras (Francia) y en Pekín (China). Disponible en: https://elpais.com/internacional/2023-10-13/un-profesor-muere-apunalado-en-un-instituto-del-norte-de-francia-y-dos-personas-resultan-heridas-graves.html?outputType=amp
https://www.abc.es/internacional/apunalado-empleado-embajada-israeli-pekin-20231013130138-nt_amp.html (29/10/2023).

Ataques de los rebeldes hutíes en el golfo de Adén, y restauración del control del Canal de Suez como puerta de entrada y salida de mercancías entre Asia y Europa. Disponible en: https://www.europapress.es/internacional/noticia-ue-une-operacion-guardian-prosperidad-mar-rojo-traves-operacion-atalanta-20231221085757.html
https://www.abc.es/economia/ataques-mar-rojo-disparan-precios-transporte-asia-20240103185433-nt.html
https://www.bbc.com/mundo/articles/c0ky0r0k01eo (03/01/2024).

Ataque del movimiento islamista palestino Hamás contra el Estado de Israel desde la Franja de Gaza, el 7 de octubre de 2023. Disponible en: https://www.bbc.com/mundo/articles/cqlwz3yjyeeo (29/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Valoración de las repercusiones del ataque del 7 de octubre de 2023 por parte de Hamás a Israel. Disponible en: https://cnnespanol.cnn.com/2023/10/10/analisis-guerra-israel-hamas-conmociones-politicas-planeta-trax/ (29/10/2023).

Crisis humanitaria de las Islas Canarias, de octubre de 2023. Disponible en: https://www.ondacero.es/emisoras/canarias/noticias/8-dias-octubre-llegan-4300-migrantes-canarias-media-520-dia_20231009652399dbe0d76200011f5ac5.html (27/10/2023).

Operación militar terrestre de Israel en el territorio de la Franja de Gaza. Disponible en: https://www.bbc.com/mundo/articles/cv20yw3427qo https://efe.com/mundo/2023-10-28/la-asamblea-general-de-la-onu-vota-resolucion-arabe-para-frenar-la-guerra-en-gaza/ (30/10/2023).

Declaraciones del representante de Israel en NNUU considerándola una organización "rota y moralmente corrupta". Disponible en: https://efe.com/mundo/2023-10-26/israel-vuelve-a-atacar-a-la-onu-como-una-organizacion-rota-y-moralmente-corrupta/ https://www.elperiodico.com/es/internacional/20231026/israel-ataca-onu-tacha-rota-93851208 (30/10/2023).

Mensaje de la Embajada de Rusia en España del 8 de noviembre de 2023 en su perfil de X. Disponible en: https://twitter.com/EmbajadaRusaES/status/1722218306906804393 (12/11/2023).

El Secretario General de NNUU, António Guterres, apela a la responsabilidad de la comunidad internacional para poner fin a la crisis en Gaza e invoca el artículo 99 de la Carta mediante un escrito dirigido al Presidente del Consejo de Seguridad. Disponible en: https://unric.org/es/guterres-invoca-el-articulo-99-al-consejo-de-seguridad/ (10/12/2023).

EE.UU. aplica su derecho de veto para que no se apruebe alto el fuego en el conflicto de Israel con Hamás. Disponible en: https://news.un.org/es/story/2023/12/1526302 (10/12/2023).

Celebración del 75 aniversario de la Declaración Universal de los Derechos Humanos bajo el lema "dignidad, libertad y justicia para todas las personas". Disponible en: https://www.un.org/es/observances/human-rights-day (10/12/2023).

La UE examina la financiación a Palestina. Disponible en: https://es.euronews.com/my-europe/2023/10/09/la-ue-suspende-inmediatamente-todos-los-pagos-a-las-autoridades-palestinas (29/10/2023).

Von der Leyen matiza su discurso tras las críticas e insta a Israel a que respete el derecho internacional en el marco del conflicto con Hamás. Disponible en: https://elpais.com/internacional/2023-10-14/von-der-leyen-matiza-su-discurso-tras-las-criticas-e-insta-a-israel-a-que-respete-el-derecho-internacional.html (29/10/2023).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Sanciones económicas impuestas por Bruselas a Rusia en el contexto de la invasión a Ucrania. Disponible en: https://elpais.com/internacional/2023-10-17/viktor-orban-desafia-la-postura-europea-al-convertirse-en-el-primer-lider-europeo-que-se-reune-con-putin-en-los-ultimos-meses.html#?rel=lom (27/10/2023).

Bloqueo a la declaración conjunta UE sobre migración en la Cumbre informal de la UE celebrada en octubre de 2023 en Granada. Disponible en: https://es.euronews.com/my-europe/2023/10/06/hungria-y-polonia-bloquean-de-nuevo-una-declaracion-conjunta-de-la-ue-sobre-migracion (26/10/2023).

Flexibilización del reparto obligatorio de cuotas de migrantes entre Estados miembros de la UE y endurecimiento del acceso a quienes traten de acceder de manera irregular a territorio de la UE. Disponible en: https://www.consilium.europa.eu/es/policies/eu-migration-policy/eu-migration-asylum-reform-pact/
https://spanish-presidency.consilium.europa.eu/es/programa/pacto-migratorio-presidencia-espanola-consejo-ue/
https://elpais.com/internacional/2023-12-20/la-ue-cierra-el-pacto-migratorio-tras-anos-de-negociacion-y-con-un-endurecimiento-de-los-requisitos-de-acogida.html
(21/12/2023).

Europol crea un Grupo de Trabajo Operativo para ayudar en las investigaciones sobre los crímenes de guerra cometidos en Ucrania tras la invasión rusa de febrero de 2022. Nota de prensa de 21 de noviembre de 2023. Disponible en: https://www.europol.europa.eu/media-press/newsroom/news/europol-sets-osint-taskforce-to-support-investigations-war-crimes-committed-in-ukraine (25/11/2023).

Ucrania se esfuerza para que la ayuda de occidente no decaiga y Moscú pone sus ojos en el G7. 6 de diciembre de 2023. Disponible en: https://www.france24.com/es/europa/20231206-ucrania-se-esfuerza-para-que-la-ayuda-de-occidente-no-decaiga-mosc%C3%BA-pone-sus-ojos-sobre-el-g7
(27/12/2023).

En diciembre de 2023 la compañía Maersk cancela sus rutas por el Mar Rojo a consecuencia de los ataques de los Hutíes. Disponible en: https://cincodias.elpais.com/economia/2023-12-15/maersk-paraliza-todo-su-trafico-de-contenedores-a-traves-del-mar-rojo-ante-la-escalada-de-ataques.html
https://blog.hispamicro.com/la-situacion-del-mar-rojo-y-el-golfo-de-aden-y-su-impacto-en-el-comercio-maritimo/ (08/01/2024).

La UE otorga el estatus de candidato a Georgia el 14 de diciembre de 2023. Disponible en: https://es.euronews.com/my-europe/2023/12/14/la-ue-acuerda-abrir-las-negociaciones-de-adhesion-con-ucrania-y-moldavia (19/12/2023).

El ejército israelí fija como objetivo a los hospitales palestinos. Disponible en: https://news.un.org/es/story/2023/12/1526707

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://elpais.com/internacional/2023-11-21/la-onu-trata-de-evacuar-tres-hospitales-de-gaza-asediados-y-bombardeados-por-israel.html (25/01/2024).

Plan de Innovación en Defensa de la UE (EUDIS). Disponible en: https://eudis.europa.eu/index_en (07/11/2023).

En diciembre de 2023, el Gobierno español aprueba en Consejo de Ministros la adquisición por el Estado de un 10% del capital de Telefónica, como respuesta a la agresiva operación de compra de Saudi Telecom Company. Disponible en: https://elpais.com/economia/2023-12-19/el-gobierno-aprueba-que-la-sepi-compre-hasta-un-10-de-telefonica.html
https://www.rtve.es/noticias/20230907/stc-compra-acciones-telefonica-planeado-durante-meses/2455402.shtml
https://theobjective.com/economia/2023-09-05/principal-operador-arabia-saudi-telefonica/ (11/01/2024).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Defensa de la Democracia. Estrasburgo, 12.12.2023. COM(2023) 630 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52023DC0630 (26/10/2024).

Propuesta de la Comisión Europea de una Directiva del Parlamento Europeo y del Consejo por la que se establecen requisitos armonizados en el mercado interior en materia de transparencia de la representación de intereses realizada en nombre de terceros países y se modifica la Directiva (UE) 2019/1937. Estrasburgo 12.12.2023. COM(2023) 637 final. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A637%3AFIN (26/10/2024).

Recomendación (UE) 2023/2829 de la Comisión, de 12 de diciembre de 2023, sobre procesos electorales inclusivos y resilientes en la Unión y con vistas a reforzar el carácter europeo y el desarrollo eficiente de las elecciones al Parlamento Europeo. Diario Oficial de la Unión Europea 2023/2829, de fecha 20.12.2023. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H2829 (26/10/2024).

Recomendación de la Comisión Europea sobre la promoción del compromiso y la participación efectiva de los ciudadanos y las organizaciones de la sociedad civil en los procesos de elaboración de políticas públicas. Bruselas, 12.12.2023. C(2023) 8627 final. Disponible en: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=PI_COM%3AC%282023%298627 (26/10/2024).

Eurobarómetro Flash 528 – Ciudadanía y democracia. Trabajo de campo realizado entre abril y mayo de 2023, siendo publicado en diciembre de 2023. Disponible en: https://europa.eu/eurobarometer/surveys/detail/2971 (26/10/2024).

Comunicado de Prensa del Consejo de la UE, de 20 de diciembre de 2023, haciendo referencia a las declaraciones del Ministro de Transformación Digital de España, José Luis Escrivá. Disponible en: https://www.consilium.europa.eu/es/press/press-

Ediciones Universidad de Salamanca | CC BY-NC-ND

releases/2023/12/20/cyber-solidarity-act-member-states-agree-common-position-to-strengthen-cyber-security-capacities-in-the-eu/ (06/03/2024).

El 30 de diciembre de 2023 la UE acuerda por unanimidad la entrada gradual de Rumanía y Bulgaria en el espacio Schengen, siendo a partir del 31 de marzo de 2024 cuando se eliminan los controles de fronteras interiores aéreas y marítimas, manteniéndose los controles por tierra temporalmente a expensas de la negociación con Austria. Disponible en: https://es.euronews.com/2024/03/28/rumania-y-bulgaria-se-uniran-parcialmente-al-espacio-schengen-de-europa-el-domingo
https://elpais.com/internacional/2024-03-30/rumania-y-bulgaria-inician-una-entrada-parcial-en-el-espacio-schengen-por-las-reticencias-de-austria.html (1/04/2024).

Cuestión del Sáhara en la política española y marroquí. Disponible en: https://aroapress.com/2023/12/22/43166/ (13/01/2024).

Marco General de los Medios en España 2024. Disponible en: https://www.aimc.es/a1mc-c0nt3nt/uploads/2024/01/Marco_General_Medios_2024.pdf (24/10/2024).

Declaraciones de Úrsula Von der Leyen elevando el tono de la alerta frente a la desinformación. Disponible en: https://www.eldebate.com/internacional/20240117/von-der-leyen-davos-preocupacion-principal-durante-proximos-dos-anos-desinformacion_167647.html (22/10/2024).

Atentado DAESH del 4 de enero de 2024 en Irán, durante los actos conmemorativos del fallecimiento del general iraní Qasem Soleimanini. Disponible en: https://www.elconfidencial.com/mundo/2024-01-05/iskp-atentado-iran_3805653/ (23/03/2024)

Operación Doppelgänger. Disponible en: https://euvsdisinfo.eu/es/la-campana-doppelganger-de-nuevo-en-accion-destapando-actividades-de-fimi-dirigidas-en-contra-de-las-elecciones-europeas-de-2024/
https://www.dw.com/de/ausw%C3%A4rtiges-amt-prorussische-desinformationskampagne-auf-x-aufgedeckt/a-68096288 (27/10/2024).

El Estado de Alabama ejecuta a Kenneth Eugene Smith el 25 de enero de 2024, mediante el procedimiento de asfixia por nitrógeno, a pesar de la reprobación por parte de la opinión internacional y del ACNUDH. Disponible en: https://www.elmundo.es/internacional/2024/01/26/65b34be0fdddfff58e8b45db.html
https://elpais.com/internacional/2024-01-26/alabama-mata-con-el-experimental-metodo-de-asfixia-con-nitrogeno-a-un-condenado-a-muerte-al-que-ya-trato-de-ejecutar-en-2022.html (26/01/2024).

Ecosistema de desinformación del Kremlin para desprestigiar a los Estados occidentales y sus instituciones democráticas. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.rfi.fr/es/europa/20240213-portal-kombat-francia-revela-una-red-que-difunde-propaganda-rusa-en-europa-y-ee-uu
https://euvsdisinfo.eu/es/las-manipulaciones-del-kremlin-a-nivel-mundial/
(03/05/2024).

Operación Matrioska. Disponible en: https://verifica.efe.com/operacion-matrioska-prorrusa-manipular-verificadores-alertas-falsas/ (23/05/2024).

El Kremlin reconfigura el grupo paramilitar Wagner a partir de la muerte de su líder, Yevgeny Prigozhin. Disponible en: https://www.bbc.com/mundo/articles/c514zz52gwvo (03/05/2024).

Sanciones de la Unión Europea contra Rusia como consecuencia de la invasión de Ucrania. Disponible en: https://eu-solidarity-ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine_es
https://www.consilium.europa.eu/es/policies/sanctions-against-russia/
https://www.dw.com/es/la-ue-acuerda-nuevas-sanciones-a-rusia-con-motivo-de-los-dos-a%C3%B1os-de-guerra-en-ucrania/a-68314644 (04/05/2024).

En marzo de 2024 las fuerzas navales de China, Rusia e Irán inician unas maniobras en el golfo de Omán. Disponible en: https://es.euronews.com/2024/03/12/ejercicios-navales-conjuntos-de-china-iran-y-rusia-en-el-golfo-de-oman
https://cnnespanol.cnn.com/2023/10/12/como-consigue-Hamás-armas-trax/#:~:text=No%20mencion%C3%B3%20ninguna%20participaci%C3%B3n%20exterior,nos%20da%20dinero%20y%20armas%22. (04/05/2024).

Atentado de DAESH contra los asistentes a un concierto en la sala Crocus City Hall, en Krasnogorsk, en marzo de 2024. Disponible en: https://www.elmundo.es/internacional/2024/03/22/65fdc357e85ece011a8b458a.html
https://www.france24.com/es/europa/20240323-atentado-en-mosc%C3%BA-por-gu%C3%A9-el-estado-isl%C3%A1mico-ataca-rusia
https://www.bbc.com/mundo/articles/c51wqnlg519o (23/03/2024)

Palabras de la presidenta de la Comisión Europea ante el Parlamento de la Unión el 28 de febrero de 2024, en el contexto de las declaraciones de Putin amenazando con el uso de armas nucleares si la UE envía tropas a Ucrania. Disponible en: https://www.aquieuropa.com/noticia/72706-von-der-leyen-advierte-de-que-la-amenaza-de-guerra-puede-no-ser-inminente-pero-no-imposible
https://www.publico.es/internacional/von-der-leyen-llama-al-rearme-ue-amenaza-guerra-no-sea-inminente-no-imposible.html
https://www.msn.com/es-es/noticias/internacional/von-der-leyen-la-guerra-no-es-imposible/ar-BB1j33I4 (03/03/2024).

imágenes del atentado de la sala de conciertos Crocus City Hall de Krasnogorsk. Disponible en: https://www.20minutos.es/noticia/5230157/0/estado-islamico-difunde-video-masacre-moscu-grabado-por-terroristas/ (26/03/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Programa FET FLAGSHIPS. Disponible en: https://digital-strategy.ec.europa.eu/es/activities/flagships (03/03/2024).

La junta militar que gobierna Níger escenifica la ruptura con el mando militar estadounidense poco después de haber llegado a un acuerdo trilateral con Burkina Faso y Mali para conformar una fuerza conjunta. Disponible en: https://elpais.com/internacional/2024-03-22/niger-quiere-expulsar-al-ejercito-de-estados-unidos.html
https://www.france24.com/es/%C3%A1frica/20240317-n%C3%ADger-la-junta-golpista-revoca-un-acuerdo-militar-con-ee-uu-y-pide-la-salida-de-las-tropas
(25/03/2024).

Estrategia rusa de articulación de operaciones de influencia en países como Bosnia, Moldavia o Georgia, en los que la UE tiene puestas grandes expectativas de aproximación, o el Norte de África y el Sahel, donde su presencia es cada vez más relevante. Disponible en: https://www.elmundo.es/internacional/2024/03/31/66097805fc6c8340408b4570.html
https://elpais.com/internacional/2024-04-03/la-otan-alerta-de-los-intentos-de-rusia-de-desestabilizar-bosnia-moldavia-y-georgia-los-eslabones-mas-debiles-de-europa.html (03/04/2024).

Informe sobre el grupo Sandworm, principal unidad de ciberataque rusa. Disponible en: https://www.darkreading.com/ics-ot-security/-sandworm-group-is-russia-s-primary-cyber-attack-unit-in-ukraine (19/04/2024).

Operación Portal Kombat, de febrero de 2024. Disponible en: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2024/article/foreign-digital-interference-result-of-investigations-into-the-russian (27/10/2024).

Informe de abril de 2024 de la empresa de ciberseguridad WithSecure, sobre el grupo hacktivista ruso Sandworm y su estrategia de ataque a las infraestructuras ucranianas. Disponible en: https://www.infosecurity-magazine.com/news/russian-sandworm-backdoor-ukraine/ (18/04/2024).

Operación False Facade, de mayo de 2024. Disponible en: https://euvsdisinfo.eu/building-a-false-facade/ (27/10/2024).

Operación Overload de la compañía Check First. Disponible en: https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf (27/10/2024).

Investigación dentro de la Agencia de Naciones Unidas para los Refugiados Palestinos (UNRWA) por su supuesta participación en los ataques de Hamás contra Israel del 7 de octubre de 2023. Disponible en: https://www.europapress.es/internacional/noticia-

Ediciones Universidad de Salamanca | CC BY-NC-ND

principales-responsables-onu-temen-efectos-catastroficos-suspension-ayuda-unrwa-20240131105430.html
https://www.elconfidencial.com/mundo/2024-01-29/guerra-israel-hamas-gaza-directo-hoy_3819502/
https://www.france24.com/es/medio-oriente/20240126-unrwa-investiga-presunta-colaboraci%C3%B3n-de-su-personal-en-ataques-del-7-de-octubre-ee-uu-suspende-financiaci%C3%B3n
https://www.lavanguardia.com/internacional/20240126/9506787/onu-investiga-miembros-agencia-ayuda-palestina-implicados-presuntamente-ataque-hamas-israel-7-octubre.html (02/02/2024).

El Parlamento de Hungría ratifica el 26 de febrero de 2024 la entrada de Suecia como nuevo miembro de la OTAN. Disponible en: https://www.nytimes.com/es/2024/02/27/espanol/suecia-otan-hungria.html
https://elpais.com/internacional/2024-02-26/hungria-ratifica-la-adhesion-de-suecia-a-la-otan.html
https://es.euronews.com/video/2024/02/26/el-parlamento-hungaro-ratifica-el-ingreso-de-suecia-en-la-otan (27/02/2024).

Retirada ucraniana de Avdivka. Disponible en: https://elpais.com/internacional/2024-02-17/ucrania-se-retira-de-avdiivka-en-la-mayor-victoria-rusa-en-un-ano.html
https://www.france24.com/es/europa/20240217-ucrania-anuncia-su-retiro-de-avdiivka-una-ciudad-estrat%C3%A9gica-en-la-guerra-contra-rusia
https://www.elperiodico.com/es/internacional/20240217/directo-guerra-rusia-ucrania-ultimas-noticias-conflicto-97242304 (18/02/2024).

La Comisión Europea impulsa la estrategia de la Unión para reforzar la industria de defensa y propone como objetivo que, para 2030, los EEMM compren a empresas de la UE al menos la mitad del material militar. Disponible en: https://elpais.com/internacional/2024-03-05/bruselas-urge-a-impulsar-la-industria-europea-de-defensa-para-rearmarse-frente-a-la-amenaza-de-rusia.html
https://www.elconfidencial.com/mundo/2024-03-05/bruselas-urge-a-que-en-2030-el-50-de-la-compra-de-armamento-en-la-ue-sea-de-material-europeo_3842815/
https://www.lavanguardia.com/internacional/20240306/9537750/cuando.html
(08/03/2024).

Eurodiputados alemanes acusados de espiar para los servicios secretos chinos. Disponible en: https://elpais.com/internacional/2024-04-23/detenido-en-alemania-el-asistente-de-un-eurodiputado-del-partido-ultra-afd-por-espiar-para-china.html
https://es.euronews.com/my-europe/2024/04/23/tras-el-rusiagate-los-eurodiputados-se-apresuran-a-denunciar-el-emergente-chinagate (04/05/2024).

Ataque de Irán a Israel en la noche del 13 al 14 de abril de 2024, con drones, misiles balísticos y de crucero, como respuesta al ataque contra su consulado en Damasco el 1 de abril, atribuido a Tel Aviv. Disponible en: https://elpais.com/internacional/2024-04-14/cronica-de-un-ataque-anunciado.html
https://www.bbc.com/mundo/articles/cyj3nk8zv0lo

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.europapress.es/internacional/noticia-guerra-iran-israel-directo-ultimas-noticias-conflicto-iran-israel-20240414083449.html
https://www.rtve.es/noticias/20240417/netanyahu-ante-llamadas-moderacion-occidente-respuesta-iran-israel-reserva-derecho-protegerse/16065174.shtml
https://www.elcorreo.com/internacional/netanyahu-desoye-todas-llamadas-6254831380001-20210518191512-vi.html?ref=https%3A%2F%2Fwww.elcorreo.com%2Finternacional%2Fnetanyahu-desoye-todas-llamadas-6254831380001-20210518191512-vi.html
https://www.bbc.com/mundo/articles/c1ejq8lyj2lo
https://elpais.com/internacional/2024-04-19/conflicto-israel-iran-y-guerra-en-gaza-en-directo.html (19/04/2024).

Discurso del Presidente francés Emmanuel Macron en La Sorbona, el 25 de abril de 2024. Disponible en: https://legrandcontinent.eu/es/2024/04/25/construir-un-nuevo-paradigma-el-discurso-completo-de-emmanuel-macron-en-la-sorbona/ (26/04/2024).
Operación de influencia iraní para influir en la sociedad israelí y sembrar la desconfianza en su gobierno utilizando a las comunidades ortodoxa y LGBTQ+, el discurso político de la izquierda y la derecha, o la guerra de Israel contra Hamás. Disponible en: https://www.darkreading.com/threat-intelligence/three-year-iranian-influence-op-preys-divides-israeli-society (09/05/2024).

Los servicios de inteligencia belgas confirman en abril de 2024 la existencia de una red de injerencia prorrusa en varios Estados europeos, incluida Bélgica. Disponible en: https://elpais.com/internacional/elecciones-europeas/2024-04-12/belgica-investiga-un-caso-de-injerencia-rusa-en-las-elecciones-europeas.html
https://www.larazon.es/internacional/injerencia-rusa-cierne-elecciones-europeas-mes-junio_20240429662ee3d28e66020001bd6533.html (04/05/2024).

China aparece como la principal sospechosa de una gran exfiltración de información personal y confidencial de personal militar de UK. Disponible en: https://osintcorp.net/china-suspected-after-major-mod-payroll-breach/ (07/05/2024).

En mayo de 2024 las instituciones públicas polacas son objetivo de una campaña de malware a gran escala coordinada por el actor estatal APT28, vinculado a Rusia. Disponible en: https://thehackernews.com/2024/05/kremlin-backed-apt28-targets-polish.html (11/05/2024).

Operación de influencia del Kremlin para alimentar su narrativa victimista frente a Occidente. Disponible en: https://actualidad.rt.com/actualidad/422597-expertos-culpan-expansion-otan-conflicto (08/05/2024).

Atentado en Solingen (Alemania) el 24 de agosto de 2024. Disponible en: https://www.rtve.es/noticias/20240823/varios-muertos-heridos-ataque-con-cuchillo-ciudad-alemana-solingen/16226165.shtml
https://www.elmundo.es/internacional/2024/08/23/66c8fb70fdddff9e808b4590.html
https://www.eldiario.es/internacional/detenido-presunto-autor-ataque-alemania-entregarse-policia_1_11607534.html

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.rtve.es/noticias/20240825/policia-detiene-presunto-autor-apunalamiento-mato-tres-personas-solingen/16226618.shtml (25/08/2024).

Nuevo plan del gobierno alemán contra la migración irregular, de septiembre de 2024. Disponible en: https://www.dw.com/es/el-gobierno-alem%C3%A1n-presenta-plan-contra-migraci%C3%B3n-irregular-con-restricciones-a-refugiados/a-70197330 https://www.rtve.es/noticias/20240912/gobierno-aleman-plan-migracion-irregular-restricciones-refugiados/16245903.shtml https://www.swissinfo.ch/spa/el-gobierno-alem%C3%A1n-presenta-plan-contra-migraci%C3%B3n-irregular-con-restricciones-a-refugiados/87536335 https://es.euronews.com/my-europe/2024/07/23/el-gobierno-aleman-refuerza-el-tribunal-constitucional-contra-la-extrema-derecha (15/09/2024).

Zelensky presiona a Washington para que flexibilice las restricciones sobre el uso de misiles de largo alcance para atacar a Rusia. Disponible en: https://es.euronews.com/my-europe/2024/09/27/zelenski-se-reune-con-trump-en-nueva-york-para-presentarle-su-plan-de-victoria https://www.bbc.com/mundo/articles/cp952pypj37o (08/10/2024).

Zelensky presiona a la Unión Europea para que no decaiga su apoyo en la guerra contra Rusia. Disponible en: https://es.euronews.com/my-europe/2024/10/11/volodimir-zelenski-presenta-a-sus-aliados-el-plan-de-victoria-de-ucrania-en-su-gira-por-eu https://www.europapress.es/internacional/noticia-zelenski-presenta-londres-plan-victoria-medio-demandas-armas-mas-potentes-20241010145912.html https://www.elcorreo.com/internacional/europa/zelenski-presenta-plan-victoria-fugaz-viaje-europeo-20241010165338-ntrc.html (11/10/2024).

Guía de estudio 2024 de la UNAV sobre el Modelo de NNUU y la Comisión de Desarme y Seguridad Internacional. Disponible en: https://www.unav.edu/documents/5506181/0/guia-estudio-unoda-jr.pdf (22/02/2024).

OPA lanzada en marzo de 2024 por el grupo empresarial húngaro Ganz-Mavag para la compra de la empresa ferroviaria española Talgo. Disponible en: https://elpais.com/economia/2024-08-28/el-cni-alerto-de-la-conexion-rusa-del-grupo-hungaro-que-puja-por-talgo.html https://es.euronews.com/2024/08/27/el-gobierno-rechaza-la-venta-de-talgo-a-una-empresa-hungara-por-riesgos-para-la-seguridad- https://www.publico.es/economia/gobierno-rechaza-opa-hungara-talgo-razones-seguridad-nacional.html https://www.eleconomista.es/transportes-turismo/noticias/12672715/02/24/la-conexion-rusa-en-la-opa-de-talgo-la-sombra-de-putin-se-extiende-sobre-el-fabricante-espanol.html (28/08/2024).

Conflicto ruso ucraniano. Declaraciones en marzo de 2024 del portavoz del Kremlin, Dmitry Peskov. Disponible en: https://elpais.com/internacional/2024-03-22/el-kremlin-reconoce-que-su-operacion-militar-especial-contra-ucrania-es-una-guerra.html

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.elperiodico.com/es/internacional/20240323/rusia-cambiando-lenguaje-guerra-dv-99869724 (27/03/2024).

Ciberataque del grupo ucraniano Blackjack, de abril de 2024, contra el complejo TIC ruso donde se almacenaba información utilizada por industrias militares, de energía y telecomunicaciones rusas. Disponible en: https://cybernews.com/cyber-war/ukraine-blackjack-destroys-russian-data/ (09/04/2024).

Denuncia de Sudáfrica contra Israel por genocidio en Gaza. Disponible en: https://unric.org/es/denuncia-sudafricana-contra-israel-por-genocidio-en-gaza/ https://efe.com/mundo/2024-01-11/denuncia-sudafrica-israel-genocidio-corte-internacional-de-justicia/ https://www.bbc.com/mundo/articles/czrl8zv388eo (02/03/2024).

Interpretación de EE.UU. de la resolución 2728, adoptada por el mismo Consejo de Seguridad de NNUU referente al alto el fuego en el conflicto entre Israel y Hamás. Disponible en: https://elpais.com/internacional/2024-03-29/ee-uu-provoca-una-polemica-en-la-onu-por-considerar-la-resolucion-de-alto-el-fuego-en-gaza-no-vinculante.html (01/04/2024).

Bombardeos israelíes cerca de la ciudad de Isfahán. Disponible en: https://es.euronews.com/2024/04/19/el-supuesto-ataque-israeli-a-iran-impacta-cerca-de-la-central-nuclear-de-isfahan https://cnnespanol.cnn.com/2024/04/13/ataque-iran-israel-noticias-ultima-hora-orix/ (04/05/2024).

Reunión informal del Consejo de Seguridad NNUU, coorganizada por Corea del Sur y EE.UU., celebrada en abril de 2024, sobre Evolución del panorama de las ciberamenazas y sus implicaciones para el mantenimiento de la paz y la seguridad internacionales. Disponible en: https://www.oodaloop.com/archive/2024/04/23/the-un-security-council-has-a-role-in-international-cybersecurity/ (11/05/2024).

Discurso del Presidente de la República Francesa, en La Sorbona, el 25 de abril de 2024, titulado *Construir un nuevo paradigma europeo*. Disponible en: https://legrandcontinent.eu/es/2024/04/25/construir-un-nuevo-paradigma-el-discurso-completo-de-emmanuel-macron-en-la-sorbona/ (26/04/2024).

United States´International Cyberspace and Digital Policy Strategy: towards an innovative, secure and rights-respecting digital future. Disponible en: https://www.state.gov/release-of-united-states-international-cyberspace-and-digital-policy-strategy/ (22/05/2024).

Georgia se plantea un proyecto de ley sobre agentes extranjeros. Disponible en: https://es.euronews.com/2024/05/18/la-presidenta-de-georgia-veta-la-ley-de-agentes-extranjeros-o-ley-rusa https://cnnespanol.cnn.com/2024/05/19/presidenta-georgia-veta-controversia-proyecto-ley-agentes-extranjeros-rusia-trax/ (19/05/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

El 8 de mayo de 2024 la exalcaldesa de Berlín Franziska Giffey, y a un día después la política Yvonne Mosler, sufren actos de violencia en el desarrollo de la campaña electoral europea. Disponible en: https://es.euronews.com/my-europe/2024/05/08/golpean-a-una-politica-alemana-durante-un-acto-oficial-en-berlin-esta-atacando-nuestra-dem
https://elpais.com/internacional/2024-05-08/dos-nuevas-agresiones-agravan-la-preocupacion-en-alemania-por-la-violencia-contra-los-politicos.html
https://es.euronews.com/my-europe/2024/05/04/agreden-en-plena-calle-a-un-candidato-aleman-para-las-elecciones-europeas
https://elpais.com/internacional/2024-05-12/la-oleada-de-agresiones-a-politicos-desata-la-alarma-en-europa-me-atacaron-de-forma-repentina-e-inesperada.html (18/05/2024).

El 15 de mayo de 2024, el primer ministro de Eslovaquia, Robert Fico, recibió hasta cinco disparos a corta distancia, cuando salía de una reunión con su gabinete y se disponía a saludar a simpatizantes que aguardaban en la ciudad de Handlova. Disponible en: https://www.elmundo.es/internacional/2024/05/16/66459542e4d4d867308b45a6.html
https://www.bbc.com/mundo/articles/cjmkmw3g0ppo (18/05/2024).

El Ministro del Interior español activa el 6 de mayo de 2024 la Red de Coordinación para la Seguridad en Procesos Electorales, como parte del dispositivo de seguridad nacional para garantizar las elecciones europeas. Disponible en: https://www.dsn.gob.es/gl/actualidad/sala-prensa/activaci%C3%B3n-red-coordinaci%C3%B3n-para-seguridad-procesos-electorales-ante-9j (14/05/2024).

En mayo de 2024 el grupo de hackers patrocinado por el Estado iraní conocido como APT42 se hace pasar por conocidos medios de comunicación –The Washington Post, The Economist- y think tanks para atacar a periodistas, investigadores y activistas de países occidentales y Oriente Medio, redirigiéndoles a enlaces maliciosos y, posteriormente, tener acceso a las redes sociales de la víctima. Disponible en: https://news.hitb.org/content/iranian-state-backed-cyber-spies-continue-impersonate-media-brands-think-tanks (05/05/2024).

En mayo de 2024 se detecta un grupo de ciberespionaje vinculado a China, conocido como Mustang Panda, centrado en varias de las compañías navieras de transporte marítimo comercial con sede en Noruega, Grecia y Países Bajos. Disponible en: https://www.escudodigital.com/ciberseguridad/china-malware-espiar-envios-comerciales-barcos_59045_102.html (19/05/2024).

Ejercicio de la OTAN denominado “Swift Response” de mayo de 2024, en escenarios del norte y el este de Europa colindantes con Rusia, al tiempo que el secretario de Estado de EE.UU., Antony Blinken, visita Kiev para reunirse con el presidente Zelenski y su cúpula militar, para reafirmar el compromiso estadounidense con el apoyo logístico y económico a Ucrania. Disponible en:

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://www.elconfidencialdigital.com/articulo/defensa/salto-paracaidistas-espanoles-rumania-ejercicio-otan/20240426000000768528.html
https://efe.com/mundo/2024-05-14/antony-blinken-llega-a-ucrania-para-reiterar-apoyo-duradero/ (14/05/2024).

Fallo generado en los sistemas de Microsoft, en julio de 2024, a raíz de una actualización defectuosa de la plataforma de seguridad CrowdStrike. Disponible en: https://efe.com/economia/2024-07-19/actualizacion-crowdstrike-fallo-incidencias-microsoft/
https://ciberseguridadtic.es/reportajes/los-principales-detalles-del-incidente-de-crowdstrike-y-microsoft-202407226156.htm
https://www.europapress.es/portaltic/ciberseguridad/noticia-crowdstrike-avanza-error-ocasiono-apagon-global-no-puede-repetirse-hecho-evitarlo-20240807141103.html (22/09/2024).

Argelia se une al Nuevo Banco de Desarrollo (NBD) de los BRICS, para diversificar sus asociaciones económicas y tratar de fortalecer su papel en el escenario global, tras el varapalo que supuso el reconocimiento francés a las tesis marroquíes sobre el Sáhara occidental, y que se sumó a la posición mantenida por EE.UU. y España. Disponible en: https://www.barrons.com/articles/argelia-se-une-al-nuevo-banco-de-desarrollo-de-los-brics-e20f6b6b
https://www.lanacion.com.ar/agencias/argelia-se-une-al-nuevo-banco-de-desarrollo-de-los-brics-nid01092024/
https://www.swissinfo.ch/spa/aprobada-la-membres%C3%ADa-de-argelia-en-el-banco-de-los-brics-un-a%C3%B1o-despu%C3%A9s-de-su-solicitud/87472961
(12/09/2024).

Rusia no recibe con agrado el Proyecto de Convención de las NNUU contra la Ciberdelincuencia. Disponible en: https://efe.com/mundo/2024-08-09/naciones-unidas-primer-tratado-ciberdelincuencia/
https://www.rtve.es/noticias/20240809/naciones-unidas-aprueba-su-primer-tratado-contra-ciberdelincuencia/16213537.shtml (21/08/2024).

Atentado terrorista del 17 de septiembre de 2024 en Bamako, contra la Escuela de la Gendarmería y la Base Aérea militar 101. Disponible en: https://www.europapress.es/internacional/noticia-registradas-varias-explosiones-tiroteos-capital-mali-bamako-20240917103819.html
https://www.larazon.es/internacional/13-terroristas-suicidas-perpetraron-ataque-instalaciones-militares-capital-mali_2024092166eec8cbfcf7b300013c44fd.html
https://elpais.com/internacional/2024-09-21/un-ataque-terrorista-contra-unas-instalaciones-militares-en-bamako-causa-mas-de-50-muertos.html (22/09/2024).

Intentos de asalto a la valla fronteriza de Ceuta durante el mes de septiembre de 2024. Disponible en: https://elpais.com/espana/2024-09-15/un-masivo-despliegue-policial-marroqui-impide-que-cientos-de-migrantes-salten-la-valla-de-ceuta.html
https://efe.com/espana/2024-09-15/ceuta-intento-salto-valla-marruecos/

Ediciones Universidad de Salamanca | CC BY-NC-ND

https://es.euronews.com/my-europe/2024/09/16/disturbios-y-detenciones-en-castillejos-tras-el-intento-de-saltar-la-valla-de-ceuta (22/09/2024).

Incumplimiento por Mongolia de sus obligaciones internacionales respecto a las órdenes de detención emitidas por la Corte Penal Internacional sobre el presidente Putin, el exministro de Defensa ruso Serguéi Shoigú y el Jefe del Estado Mayor de las Fuerzas Armadas del Kremlin, Valeri Gerasimov. Disponible en: https://www.rtve.es/noticias/20240902/putin-llega-mongolia-riesgo-detenido-orden-corte-penal-internacional/16234199.shtml
https://www.eldiario.es/internacional/mongolia-recibe-putin-niega-detenerlo-pese-orden-corte-penal-internacional_1_11624716.html
https://es.euronews.com/2024/09/02/putin-llega-a-mongolia-estado-miembro-de-la-corte-penal-internacional-sin-ser-detenido
https://www.france24.com/es/asia-pac%C3%ADfico/20240903-putin-es-bienvenido-y-con-honores-en-mongolia-a-pesar-de-la-orden-de-detenci%C3%B3n-de-la-cpi
(05/09/2024).

Acusación de la Fiscalía sueca, en septiembre de 2024, contra el servicio de inteligencia de Irán, por piratear un operador de SMS en 2023 para lanzar una campaña de influencia con potencial afectación al orden público, a través de mensajes que incitaban a la acción contra los manifestantes que habían protagonizado la quema de libros del Corán. Disponible en: https://es.euronews.com/2024/09/24/suecia-acusa-a-iran-de-piratear-su-servicio-de-mensajeria-tras-los-incidentes-de-la-quema-
https://www.swissinfo.ch/spa/suecia-acusa-a-ir%C3%A1n-de-ciberataque-para-provocar-reacciones-a-las-quemas-del-cor%C3%A1n/87605518
https://apnews.com/world-news/general-news-3e78ea8cbd3ff27bb0edd4975c5d8dd0
(27/10/2024).

Presentación del Plan de Acción por la Democracia, el 17 de septiembre de 2024. Disponible en: https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (04/01/2025).

Exposición temática en el MUVIM de Valencia, desde octubre de 2024 hasta febrero de 2025, con el título *Tinta contra Hitler. Mario Armengol, caricaturista en la II Guerra Mundial*. Disponible en: https://elpais.com/cultura/2024-10-03/mario-armengol-el-gran-desconocido-de-la-caricatura-de-la-segunda-guerra-mundial-contra-hitler.html
https://www.rtve.es/play/videos/telediario-2/armengol-dibujante-caricaturas-contra-hitler/16279995/
https://www.dival.es/sala-prensa/sites/default/files/sala-prensa/VERSI%C3%93%20DIGITAL%20TRILING%C3%9CE%20TINTA%20CONTRA%20HITLER.pdf (11/10/2024).

XVI cumbre de los BRICS, celebrada en Kazán (Rusia) del 22 al 24 de octubre de 2024. Disponible en: https://efe.com/mundo/2024-10-23/cumbre-de-los-brics-kazan-rusia/
https://legrandcontinent.eu/es/2024/10/22/comienza-la-cumbre-anual-de-los-brics-en-kazan-en-rusia/ (17/11/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

Encuesta del Instituto Internacional de Sociología de Kiev (KI IS), de octubre de 2024 Disponible en: https://www.kiis.com.ua/?lang=eng&cat=reports&id=1438&page=1 (17/11/2024).

Ataques contra cables submarinos de fibra óptica. Disponible en: https://efe.com/economia/2024-11-19/danos-cables-submarinos-telecomunicaciones-baltico/
https://www.dw.com/es/cables-da%C3%B1ados-en-el-b%C3%A1ltico-guerra-h%C3%ADbrida-en-el-fondo-del-mar/a-70853517
https://www.swissinfo.ch/spa/investigan-una-aver%C3%ADa-en-cable-de-telecomunicaciones-submarino-entre-finlandia-y-alemania/88210823 (14/12/2024).

Relevo de Jens Stoltenberg como Secretario General de la OTAN a partir del 1 de octubre de 2024 por Mark Rutte. Disponible en: https://es.euronews.com/my-europe/2024/06/26/ya-es-oficial-la-otan-tiene-un-nuevo-lider-mark-rutte-secretario-general
https://www.rtve.es/noticias/20240626/aliados-otan-eligen-primer-ministro-neerlandes-mark-rutte-como-nuevo-secretario-general/16162944.shtml (23/08/2024).

Violentos enfrentamientos entre distintos grupos delincuencias en el sur de Francia como respuesta a una reorganización del sistema judicial y policial en lo referido a la lucha contra el crimen organizado. Disponible en: https://elpais.com/internacional/2024-11-08/francia-declara-la-guerra-al-narcotrafico-con-un-plan-especial-para-reducir-la-criminalidad.html
https://www.rfi.fr/es/francia/20241108-gobierno-franc%C3%A9s-anuncia-un-plan-de-lucha-para-combatir-el-narcotr%C3%A1fico (25/11/2024).

Presentación de Arsenio Escolar, presidente del Club Abierto de Editores (CLABE), durante la II Jornada contra la Desinformación, celebrada el 14 de octubre de 2024 bajo el título "Comprometidos con la verdad". Disponible en: https://clabe.org/2024/10/15/intervencion-arsenio-escolar-ii-jornada-contra-la-desinformacion/ (20/10/2024).

Operación de la Policía Nacional contra narcodrones. Disponible en: https://www.interior.gob.es/opencms/va/detalle/articulo/La-Policia-Nacional-desmantela-una-red-de-narcodrones-que-operaba-entre-Espana-y-Marruecos/
https://elpais.com/espana/2024-11-28/cae-una-banda-que-usaba-narcodrones-ucranios-para-transportar-hachis-por-el-estrecho.html
https://www.rtve.es/noticias/20241128/desmantelada-algeciras-red-narcodrones-fabricados-ucrania/16350551.shtml (14/12/2024).

Relación de municipios más afectados por la DANA: Algemesí, Catarroja, Xirivella, Paiporta, Alfafar, Aldaia, Benetússer, Massanassa, Sedaví o Albal, que conforman la denominada *zona 0* de la catástrofe. Disponible en: https://www.datadista.com/playa-burbuja/el-mapa-con-las-130-000-viviendas-afectadas-por-las-inundaciones-en-valencia/#:~:text=Entre%20ellos%20se%20encuentra%20la,y%20Massanassa%20(10.146%20habitantes) (01/12/2024).

Ediciones Universidad de Salamanca | CC BY-NC-ND

El diario La Vanguardia y Verificat firman en noviembre de 2024 un acuerdo para la verificación de información, la detección de bulos y de narrativas desinformadoras. Disponible en: https://www.lavanguardia.com/vida/20241110/10093363/vanguardia-verificat-alian-desenmascarar-noticias-falsas.html
https://www.verificat.cat/es/verificat-y-la-vanguardia-se-alian-para-hacer-llegar-el-fact-checking-a-nuevas-audiencias/ (17/11/2024).

Protestas y disturbios de noviembre y diciembre de 2024 en Georgia por la decisión del partido prorruso *Sueño Georgiano* de suspender hasta 2028 el proceso de adhesión a la Unión Europea. Disponible en: https://elpais.com/internacional/2024-11-29/el-gobierno-de-georgia-frena-la-adhesion-a-la-ue-y-la-oposicion-se-echa-a-la-calle-para-protestar.html
https://elpais.com/internacional/2024-12-02/cientos-de-detenidos-en-georgia-tras-cuatro-noches-de-protestas-multitudinarias-contra-el-gobierno-prorruso.html
https://www.europapress.es/internacional/noticia-cinco-detenidos-veintena-agentes-heridos-ultima-noche-protestas-georgia-20241202080010.html
https://www.elmundo.es/internacional/2024/12/02/674d747be4d4d890628b4787.html (14/12/2024).

Seguimiento de la decisión del Tribunal Constitucional de Rumanía ante la campaña híbrida rusa en plataformas sociales, principalmente TikTok. Disponible en: https://elpais.com/internacional/2024-12-06/el-constitucional-de-rumania-anula-la-primera-vuelta-de-las-presidenciales-tras-revelarse-la-campana-de-ataques-hibridos-rusos.html
https://es.euronews.com/my-europe/2024/12/08/anulan-las-elecciones-presidenciales-en-rumania-tras-las-denuncias-de-interferencia-extran
https://www.newtral.es/rumania-anula-elecciones/20241206/
https://efe.com/mundo/2024-12-06/rumania-elecciones-presidenciales-anulacion-justicia/ (14/12/2024).

Declaraciones del Secretario General de la OTAN, Mark Rutte, en la reunión de diciembre de 2024 de los ministros de Asuntos Exteriores aliados. Disponible en: zhttps://www.nato.int/cps/en/natohq/news_231006.htm (14/12/2024).

Nota de prensa sobre el acuerdo del CSN para la elaboración de la Estrategia Nacional contra las Campañas de Desinformación. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/2025/Enero/noticia-2025-01-30-Aprobado-procedimiento-elaboracion-Estrategia-Nacional-contra-Campa-as-de-Desinformaci-n.html (31/01/2025).

La Fiscalía del Supremo pide la imputación de Alvise por los desórdenes públicos de Ferraz de noviembre del 2023. Disponible en: https://www.elmundo.es/espana/2025/01/11/6782572d21efa0673a8b457c.html (11/01/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

La UE advierte a Meta que deberá cumplir con la DSA en el ámbito de soberanía digital europea. Amplia repercusión en prensa. Disponible en: https://efe.com/ciencia-y-tecnologia/2025-01-07/meta-verificacion-notas-comunidad-x/
https://www.bbc.com/mundo/articles/clyjlp66q2po
https://www.rtve.es/noticias/20250108/meta-elimina-verificacion-profesional-whatsapp-facebook-instagram-para-pasarse-a-notas-comunidad/16399446.shtml
https://www.swissinfo.ch/spa/ce-avisa-a-meta-que-tiene-que-respetar-normativa-sobre-moderaci%C3%B3n-de-contenidos-en-la-ue/88688106
https://elmon.cat/es/mundo/bruselas-advierte-a-meta-sobre-la-eliminacion-de-verificadores-de-datos-949634/ (11/01/2025).

Alto el fuego acordado por Israel y Hamás el 15 de enero de 2025, a instancia de EE.UU., Qatar y Egipto, que actúan como mediadores. Disponible en: https://www.bbc.com/mundo/articles/c0e4494vjg5o
https://efe.com/mundo/2025-01-19/alto-el-fuego-gaza-israel/
https://elpais.com/internacional/2025-01-19/el-alto-el-fuego-en-gaza-en-directo.html (19/01/2025).

Nota de prensa del DSN sobre el acuerdo del CSN para la elaboración de la Estrategia Nacional contra las Campañas de Desinformación. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-de-prensa/aprobado-procedimiento-elaboracion-estrategia-nacional-campanas-desinfo (31/01/2025).

Lanzamiento en 2025 de los satélites de nueva generación SpainSat NG I y II, para dotar de comunicaciones seguras a las Fuerzas Armadas españolas y sus aliados. Al tratarse de tecnología de doble uso, también dará servicio al ámbito civil. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/5082017/despegue-satelite-comunicaciones-spainsat-ng-i-llevara-cabo-entre-enero-febrero-2025
https://www.europapress.es/nacional/noticia-satelite-militar-spainsat-pasa-ultimas-pruebas-cara-ponerse-orbita-principios-2025-20241124110003.html (24/11/2024).

Repercusión en prensa internacional de la entrevista en la Casa Blanca entre Zelenski y Trump, el 28 de febrero de 2025. Disponible en: https://www.rtve.es/noticias/20250228/trump-zelenski-encuentro-casa-blanca/16471009.shtml
https://www.bbc.com/mundo/articles/clyd11np8p7o
https://www.elespanol.com/mundo/20250228/video-momento-tenso-trump-zelenski-discuten-gritos-casa-blanca-planeta/927657740_0.html (14/03/2025).

Reflejo en prensa de la mesa de negociación en Yeda (Arabia Saudí) del alto el fuego en Ucrania, de 11 de marzo de 2025, disponible en: https://legrandcontinent.eu/es/2025/03/11/propuesta-de-alto-el-fuego-inmediato-en-ucrania-el-texto-completo-de-la-declaracion-conjunta-con-estados-unidos/
https://www.rtve.es/noticias/20250311/eeuu-ucrania-arabia-saudi-negociaciones-paz/16485603.shtml
https://www.elperiodico.com/es/internacional/20250310/ucrania-alto-fuego-parcial-rusia-negociaciones-eeuu-arabia-saudi-115148191 (14/03/2025)

Ediciones Universidad de Salamanca | CC BY-NC-ND

Reunión en París el 11 de marzo de 2025 para definir la postura europea en la negociación de la paz para el conflicto ruso ucraniano. Disponible en: https://elpais.com/internacional/2025-03-11/macron-reune-en-paris-a-31-jefes-militares-de-paises-dispuestos-a-implicarse-en-una-paz-en-ucrania.html https://www.france24.com/es/europa/20250311-par%C3%ADs-30-naciones-de-europa-y-la-otan-debaten-sobre-la-defensa-y-la-paz-en-ucrania https://www.france24.com/es/europa/20250311-macron-urge-a-sus-aliados-a-definir-garant%C3%ADas-de-seguridad-cre%C3%ADbles-para-ucrania-en-cumbre-de-par%C3%ADs https://www.ansalatina.com/americalatina/noticia/union_europea/2025/03/11/paris-primer-paso-para-garantias-seguridad-en-kiev_e439b8ae-bec6-4e69-926f-28eaab84aab3.html (16/03/2024)

Reflejo en prensa de la reunión del presidente Trump con el Secretario General de la OTAN Mark Rutte, el 14 de marzo de 2025, sobre la negociación de la paz en Ucrania. Disponible en: https://www.infobae.com/america/mundo/2025/03/13/el-jefe-de-la-otan-se-reunio-con-trump-en-la-casa-blanca-y-se-mostro-cauto-al-hablar-de-gastos-en-defensa-y-groenlandia/ https://es.euronews.com/2025/03/14/rutte-ser-reune-con-trump-en-washington-y-este-vuelve-a-insistir-con-la-anexion-de-groenla (14/03/2025)

Cita de la presentación del Libro Blanco de la Defensa Europea y el Plan ReArm Europe – Preparación 2030, el 19 de marzo de 2025, en Bruselas, con la intervención de Úrsula von der Leyen, Presidenta de la Comisión Europea, y Kaja Kallas, Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793 (25/03/2025).

Las pretensiones territoriales de EE.UU. sobre Groenlandia en el marco de la negociación del alto el fuego en el conflicto de Urania tienen amplio seguimiento en prensa internacional. Disponible en: https://www.bbc.com/mundo/articles/cqx8xgy2yryo https://elpais.com/internacional/2025-03-23/trump-desata-la-ira-de-groenlandia-al-enviar-una-delegacion-al-pais-encabezada-por-la-segunda-dama.html https://www.bbc.com/mundo/articles/c14jm544x87o (25/03/2025).

La incorporación de las tierras raras ucranianas como parte de los factores determinantes de la negociación de la paz con Rusia, a través de la mediación de EE.UU., tiene amplio seguimiento en la prensa internacional. Disponible en: https://elpais.com/internacional/2025-02-12/trump-quiere-las-tierras-raras-de-ucrania-y-zelenski-esta-dipuesto-a-darselas.html https://es.euronews.com/my-europe/2025/02/28/esta-intentando-trump-dejar-fuera-a-la-ue-para-apoderarse-de-la-riqueza-mineral-de-ucrania https://www.youtube.com/watch?v=hW61fmf2FZM (25/03/2025).

El respaldo internacional que supone para Benjamín Netanyahu su visita a Donald Trump en febrero de 2025, y la consecuente desacreditación para la Corte Penal Internacional,

Ediciones Universidad de Salamanca | CC BY-NC-ND

queda reflejada en los medios de comunicación de todo el mundo. Puede consultarse en: https://efe.com/mundo/2025-02-04/trump-netanyahu-apoyo-visita-eeuu/ https://www.elmundo.es/internacional/2025/02/06/67a4f8ab21efa01e2d8b4570.html (03/04/2025).

El Gobierno húngaro no solo no hace efectiva la orden de detención internacional en vigor sobre Benjamín Netanyahu en su visita de abril de 2025 sino que, además, aprovecha la visita oficial del mandatario israelí para anunciar su intención de retirarse del Estatuto de Roma. Esta circunstancia tiene amplio seguimiento en la prensa nacional e internacional. Disponible en: https://www.rtve.es/noticias/20250403/hungria-anuncia-se-retira-corte-penal-internacional-tras-llegada-netanyahu/16519251.shtml https://es.euronews.com/2025/04/03/hungria-abandona-la-corte-penal-internacional-en-un-gesto-de-apoyo-a-netanyahu-y-putin https://cnnespanol.cnn.com/2025/04/03/mundo/hungria-anuncia-retirada-corte-penal-internacional-trax (03/04/2025).

Ediciones Universidad de Salamanca | CC BY-NC-ND

TESIS POLICIALES, 6



VNiVERSiDAD
D SALAMANCA