

Monografía 160

Selección de los nueve mejores trabajos de fin de curso del XXVI CEMFAS y el mejor trabajo de fin de curso del I CAEID en el año escolar 2024-2025 impartido en el CESEDEN

Escuela Superior de las Fuerzas Armadas

MINISTERIO
DE DEFENSA



Monografía 160

Selección de los nueve mejores trabajos de fin de curso del XXVI CEMFAS y el mejor trabajo de fin de curso del I CAEID en el año escolar 2024-2025 impartido en el CESEDEN

Escuela Superior de las Fuerzas Armadas

MINISTERIO
DE DEFENSA

Catálogo de Publicaciones de Defensa
publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

© Autores y editor, 2026

NIPO 083-26-189-2 (edición impresa)
ISBN 978-84-1083-175-9 (impresión bajo demanda)

NIPO 083-26-190-5 (edición en línea)

Depósito legal M 16610-2026
Fecha de edición: octubre de 2026
Maqueta e imprime: Imprenta Ministerio de Defensa

Las opiniones emitidas en esta publicación son de exclusiva responsabilidad del autor de la misma. Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del copyright ©.

En esta edición se ha utilizado papel procedente de bosques gestionados de forma sostenible y fuentes controladas.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica». No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

Página

Prólogo 15
José Antonio Fuentes de la Orden

Capítulo primero

Aplicación de la inteligencia económica en la lucha contra la delincuencia organizada y la delincuencia grave 23
Antonio Balas Dávila

1 Antecedentes 33
2 La seguridad y la inteligencia económica 37
2.1 Aproximación al concepto de inteligencia económica 39
2.2 Actores que conforman el sistema económico 44
2.2.1 Administración Pública 47
2.2.2 Organizaciones internacionales y supranacionales 48
2.2.3 Grandes empresas y pymes 49
2.2.4 Think tanks, universidades y centros tecnológicos 51
2.2.5 Actores no estatales y sociedad civil organizada 53
2.3 Generación de inteligencia económica por los distintos actores 53
2.3.1 Inteligencia económica en el marco de la UE 54
2.3.2 Generación de inteligencia económica en el marco español 56
3 La delincuencia organizada y grave y su afectación a los intereses económicos 58
3.1 Ámbitos delictivos con mayor incidencia económica 61
3.1.1 Blanqueo de capitales 62
3.1.2 Fraude fiscal 63
3.1.3 Cibercriminalidad económica 65
3.1.4 Economía derivada del tráfico de drogas 66
3.1.5 Delitos contra el mercado y la propiedad intelectual/industrial 67
3.1.6 Criminalidad medioambiental 67
3.1.7 Trata de seres humanos 68
3.1.8 Corrupción 69
3.2 Sectores con mayor penetración criminal, perspectiva económica 70

Página

4 Las investigaciones económicas ... 72
4.1 Estructura de una investigación económica ... 73
4.2 Integración de la inteligencia económica en las investigaciones ... 77
4.3 Necesidades de información no normalizada en las investigaciones económicas ... 81
5 Conclusiones ... 83
Bibliografía ... 86

Capítulo segundo

Fusión nuclear, la panacea de la geopolítica energética: viabilidad, actores e impacto global ... 93

Noel Díaz Muñoz

1 Introducción ... 95
1.1 La fusión nuclear ... 95
1.2 Geopolítica energética ... 97
1.3 Soberanía energética y seguridad ... 98
2 Estado actual de la fusión nuclear y su impacto en la geopolítica ... 99
2.1 Condicionantes de la fusión nuclear ... 99
2.1.1 Temperatura necesaria ... 100
2.1.2 Escasez del tritio ... 101
2.1.3 Eficiencia de la reacción ... 101
2.1.4 Mantenimiento de la estabilidad del plasma (confinamiento magnético) ... 102
2.2 Futuro de la energía de fusión ... 102
2.3 Actores ... 103
2.3.1 Corea del Sur y Japón ... 104
2.3.2 Rusia ... 105
2.3.3 Países del Golfo Pérsico ... 105
2.3.4 Actores no estatales ... 106
2.4 Impacto de la fusión nuclear ... 107
2.4.1 Cambios en el mercado energético ... 108
2.4.2 Redefinición de alianzas y rivalidades ... 109
2.4.3 Desigualdad y brecha tecnológica ... 110
3 Principales actores de la fusión nuclear ... 111
3.1 Unión Europea ... 111
3.1.1 Producción, consumo e importación de energía ... 111
3.1.2 Dependencia tecnológica ... 111
3.1.3 Relación con países exportadores ... 113
3.1.4 Tensiones internas debidas a la energía ... 114
3.1.5 La Unión Europea frente al cambio climático y la transición energética ... 115
3.1.6 Interés estratégico en la fusión nuclear ... 115
3.1.7 Iniciativas y cooperación internacional ... 116
3.1.8 Financiación y regulación ... 116
3.1.9 Impacto geopolítico, económico y energético de la fusión nuclear 117
3.2 Estados Unidos ... 118
3.2.1 Producción, consumo y comercio de energía ... 118
3.2.2 Innovación y liderazgo tecnológico ... 118
3.2.3 Geopolítica energética: aliados y rivales ... 119

Página

3.2.4 El pragmatismo estadounidense ante la transición energética 120
3.2.5 Interés y estrategias en fusión nuclear 121
3.2.6 Proyectos públicos y privados en fusión nuclear 122
3.2.7 Financiación y marco regulatorio de la fusión en EE. UU. 122
3.2.8 impacto geopolítico, económico y energético de la fusión nuclear 123
3.3 China 124
3.3.1 crecimiento económico y consumo energético 124
3.3.2 Seguridad energética y proyección internacional 125
3.3.3 Transición energética 125
3.3.4 Interés estratégico en la fusión nuclear 126
3.3.5 Capacidades tecnológicas y estratégicas chinas en fusión nuclear 127
3.3.6 Impacto geopolítico de la fusión nuclear 127
4 Conclusiones 128

Capítulo tercero

Impacto del «campo de batalla transparente» en la guerra de Ucrania y sus implicaciones para la doctrina militar española 141

Francisco Freire Rodríguez

1 Introducción. Concepto de «campo de batalla transparente» 146
1.1 Buscando la definición doctrinal 146
1.2 Componentes del sistema 147
1.2.1 Los drones 147
1.2.2 Otros medios de vigilancia 148
1.2.3 El procesamiento de datos 149
1.2.4 La conectividad 150
1.2.5 La letalidad 151
1.2.6 La «democratización» 152
1.3 Concepto de RSC 153
1.4 Preanálisis: primeras consecuencias 154
1.5 Ver y entender 155
1.6 La diferencia entre ver y entender: la decepción 156
2 Estudio de caso: la guerra de Ucrania (2022) 158
2.1 Introducción 158
2.2 Análisis de las funciones conjuntas 158
2.2.1 Mando y control 158
2.2.2 Maniobra 160
2.2.3 Fuegos 162
2.2.4 Información 165
2.3 Análisis de los principios operativos 166
2.3.1 Sorpresa 166
2.3.2 Concentración 168
2.3.3 Continuidad 169
2.4 Conclusiones. Síntesis del modelo teórico 170
2.4.1 Mando y control 171
2.4.2 Maniobra 171
2.4.3 Fuegos 171
2.4.4 Información 172
2.4.5 Sorpresa 175
2.4.6 Concentración 175
2.4.7 Continuidad 176

Página

3 Implicaciones doctrinales ... 178
3.1 Introducción ... 178
3.2 Implicaciones para la doctrina conjunta ... 178
3.2.1 Mando y control ... 178
3.2.2 Maniobra ... 179
3.2.3 Fuegos ... 180
3.2.4 Información ... 182
3.2.5 Sorpresa ... 182
3.2.6 Concentración ... 183
3.2.7 Continuidad ... 184
4 Conclusiones ... 184
4.1 Recopilación de ideas ... 184
4.1.1 La transparencia ... 184
4.1.2 La transparencia y la guerra de Ucrania ... 185
4.1.3 La transparencia, la guerra de Ucrania y la doctrina ... 186
4.2 Resultados ... 187
Bibliografía ... 188

Capítulo cuarto

Paradigma de seguridad en el Antropoceno: un análisis de las Estrategias de Seguridad Nacional de España y Francia ... 195

Jaime Graus Thiesen

1 Introducción ... 198
1.1 Marco teórico ... 199
1.2 Consideraciones generales ... 199
1.3 Antropoceno ... 200
1.4 Concepto clásico de seguridad y cambio de paradigma ... 202
1.5 El nuevo paradigma ... 205
1.6 El Pyroceno, la potencia de fuego civil y sus consecuancias ... 207
1.7 Simon Dalby y el nuevo enfoque de seguridad ... 209
2 Estrategia de Seguridad Nacional de España ... 213
2.1 Principales características de la Estrategia de Seguridad Nacional de España 2021 ... 213
2.2 El impacto del cambio climático en España ... 218
2.3 Alineación con las teorías contemporáneas de Simon Dalby y el paradigma del Antropoceno ... 221
3 Revisión Nacional Estrategia de Francia 2022 ... 225
3.1 Principales características de la revisión estrategica de Francia 2022 ... 225
3.2 El impacto del cambio climático en Francia ... 228
3.3 Alineación con las teorías contemporáneas de Simon Dalby el paradigma del Antropoceno ... 231
4 Convergencias y divergencias ... 233
4.1 Convergencias entre la ESN 2021 y la RNE 2022 ... 234
4.1.1 Adaptación a un contexto de inestabilidad geopolítica global ... 234
4.1.2 Amenazas híbridas y desinformación ... 234
4.1.3 Importancia de la resiliencia nacional ... 235
4.1.4 Cambio climático como multiplicador de riesgos ... 235
4.1.5 Reforzar la autonomía estratégica europea ... 235
4.2 Divergencias entre la ESN 2021 y la RNE 2022 ... 235

Página

4.2.1 Enfoque prioritario en el cambio climático ... 235
4.2.2 Énfasis en la disuasión nuclear ... 236
4.2.3 Prioridades regionales y globales ... 236
4.2.4 Modernización militar y capacidad operativa ... 236
4.2.5 Visión del desarrollo sostenible y la Agenda 2030 ... 237
4.3 Una visión contrapuesta de la seguridad nacional ... 237
5 Conclusiones ... 238
Bibliografía ... 240

Capítulo quinto

La polarización social en EE. UU. durante el siglo XXI y su repercusión geopolítica sobre el vínculo transatlántico ... 245

Miguel Requeno Soler

1 Introducción ... 247
1.1 Delimitación y justificación de la investigación ... 247
1.2 Eje del análisis y alcance de la discusión ... 249
1.3 Propuesta interpretativa: de la polarización doméstica a la incertidumbre estratégica ... 249
2 Marco teórico ... 250
2.1 Teorías de las relaciones internacionales ... 250
2.1.1 Perspectiva neorrealista ... 250
2.1.2 Enfoque constructivista en las relaciones internacionales ... 252
2.1.3 Convergencia entre neorrealismo y constructivismo ... 254
2.2 Concepto de polarización ... 255
2.2.1 Definición y tipos de polarización ... 255
2.2.2 ¿Cómo medir la polarización? ... 257
2.2.3 Evolución de la polarización en EE. UU. ... 258
2.3 Relación entre polarización y teorías de relaciones internacionales ... 260
2.3.1 Articulación entre polarización y política exterior desde el neorrealismo ... 260
2.3.2 Papel del constructivismo en el análisis de la percepción transatlántica ... 261
3 La política exterior de Estados Unidos (2001–2024) ... 262
3.1 La política exterior de EE. UU. en la administración Bush (2001-2008) ... 262
3.2 La política exterior de EE. UU. en la administración Obama (2009-2016) 263
3.3 La política exterior de EE. UU. en la primera administración Trump (2017-2020) ... 265
3.4 La política exterior de EE. UU. durante la administración Biden (2021-2024) ... 267
4 Análisis de la repercusión de la polarización en EE. UU. en el vínculo transatlántico ... 269
4.1 Evolución de la polarización en EE. UU. según V-DEM (2001-2024) ... 269
4.2 Período 2009-2011 ... 270
4.3 Despolarización: el caso de 2013 ... 272
4.4 2017: récord de polarización durante el primer año de presidencia de Trump ... 274
4.5 Polarización, unilateralismo y tensión transatlántica. El trienio 2018-2020 ... 276
4.6 Polarización en la administración Biden (2021-2024) ... 278

Página

5 Conclusiones ... 280
Bibliografía ... 282

Capítulo sexto

Del *laissez faire* a la acción decidida. ... 297

La respuesta policial vasca al terrorismo etarra (1980-1993) ... 297
Diego Abel Redondo Olmedo

1 Introducción ... 300
2 I Legislatura (1980-1984). Nacimiento de la Ertzaintza y pasividad inicial ... 301
2.1 El papel del PNV ... 301
2.2 El papel de la Ertzaintza ... 304
2.3 El papel de ETA ... 305
2.4 Integración de datos de la legislatura ... 306
3 II Legislatura (1984-1986). Primeros atentados y estrategia incipiente ... 308
3.1 El papel del PNV ... 308
3.2 El papel de la Ertzaintza ... 311
3.3 El papel de ETA ... 313
3.4 Integración de datos de la legislatura ... 314
4 III Legislatura (1987-1990). Traspasos de competencias a la Ertzaintza y primeras actuaciones ... 316
4.1 El papel del PNV ... 316
4.2 El papel de la Ertzaintza ... 317
4.3 El papel de ETA ... 319
4.4 Integración de datos de la legislatura ... 323
5 IV Legislatura (1991-1993). La Ertzaintza contra ETA y viceversa ... 325
5.1 El papel del PNV ... 325
5.2 El papel de la Ertzaintza ... 328
5.3 El papel de ETA ... 329
5.4 Integración de datos de la legislatura ... 331
6 Conclusiones ... 332
Bibliografía ... 334

Capítulo séptimo

Adaptación del mando y control (C2) de las Fuerzas Armadas (FAS) españolas a las Operaciones Multidominio (MDO) ... 343

Fernando Casado Yagüe

1 Introducción ... 348
Basil H. Liddell Hart
1.1 Factores de estudio ... 349
1.2 Variables de estudio ... 350
2 Las MDO en las FAS españolas ... 355
2.1 Plan de implantación de las MDO en las FAS ... 357
3 Implementación de medidas en el factor humano ... 359
3.1 Formación ... 359
3.2 Liderazgo ... 363

Página

4 Implementación de medidas en los procesos de mando y control 368
4.1 Conectividad 368
4.2 Gestión del dato y la información 372
4.3 Incorporación de Tecnologías Emergentes y Disruptivas 376
5 Implementación de medidas en la estructura de mando y control 378
5.1 Agilidad 379
5.2 Enfoque integral 382
5.2.1 El enfoque integral y los dominios no físicos 384
5.3 Interoperabilidad 387
6 Conclusiones 388
Bibliografía 394

Capítulo octavo

La inteligencia artificial en la toma de decisiones en el nivel operacional. Impacto en la confrontación y comparación de las líneas de acción ... 399

Jordi Francesc Rubio Carceller

1 Introducción 402
2 La inteligencia artificial en la toma de decisiones operacionales 404
2.1 Inteligencia artificial, poder militar y competencia estratégica 405
2.2 Impacto de la inteligencia artificial en el planeamiento operacional OTAN 408
3 Impacto de la IA en la confrontación 410
3.1 El rol de la IA en la confrontación 410
3.2 Confrontación optimizada con IA 413
3.2.1 Caso práctico confrontación con IA 417
3.3 Resultados comparativos modelo tradicional vs IA 422
4 Impacto de la IA en la comparación de líneas de acción 424
4.1 El rol de la IA en la comparación de líneas de acción 424
4.2 Comparación de líneas de acción optimizada con IA 426
4.2.1 Caso práctico comparación líneas de acción con IA 430
4.3 Resultados comparativos modelo tradicional vs IA 435
5 Conclusiones 437
Bibliografía 440

Capítulo noveno

Capacidades militares de Arabia Saudí para la defensa de infraestructuras críticas en su litoral marítimo 451

Patricio Adrián Alisi

1 Introducción 454
2 Dialéctica de voluntades entre Arabia Saudí, Irán y los rebeldes hutíes 456
2.1 La proyección asimétrica de la amenaza hutí y su impacto sobre la seguridad estratégica saudí 456
2.2 Intereses estratégicos y racionalidad de Arabia Saudí 458
2.3 Intereses estratégicos y racionalidad de Irán 460
2.4 Intereses estratégicos y racionalidad Hutí 462
2.5 Emotividad de los tres actores. Factores y estilos de liderazgo en la toma de decisiones 464

Página

2.6 Equilibrios y asimetrías de poder en el triángulo Arabia Saudí-Irán-hutíes ... 467
2.6.1 Relaciones de poder. Arabia Saudí frente a la disuasión nuclear y la proyección indirecta iraní ... 467
2.6.2 Relaciones de poder entre Arabia Saudí y los hutíes: presión indirecta y vulnerabilidad estratégica ... 470
2.6.3 El poder en la alianza Irán-Hutí: cooperación estratégica y guerra por delegación ... 471
2.7 Situación estratégica actual y dinámica del conflicto ... 472
3 Infraestructuras críticas y pasos marítimos del sistema energético saudí ... 473
3.1 Vulnerabilidad sistémica y valor estratégico de las infraestructuras energéticas saudíes ... 473
3.2 La arquitectura energética de las costas saudíes ... 475
3.3 La dimensión marítima de la seguridad de las infraestructuras críticas saudíes ... 478
3.4 El estrecho de Ormuz: un paso sin alternativa ... 478
3.5 Bab al Mandeb: la amenaza desde la inestabilidad ... 479
4 Defensa de infraestructuras vitales y transformación militar saudí hacia 2030 ... 481
4.1 Disuasión, diplomacia y alianzas estratégicas ... 481
4.2 Limitaciones del poder marítimo saudí: una lectura desde el pensamiento naval clásico ... 483
4.3 El fortalecimiento naval saudí ... 485
4.4 Defensa aérea y protección del espacio estratégico ... 487
4.5 Capacidades terrestres y ciberdefensa ... 488
4.6 Las Fuerzas Armadas saudíes como instrumento de la Visión 2030 ... 489
5 Conclusión ... 491
Bibliografía ... 493

Capítulo décimo

Hacia un nuevo modelo de colaboración entre Fuerzas Armadas y fuerzas y cuerpos de seguridad en la seguridad pública en España ... 503

Juan Miguel Planchuelo Castiñeira

1 Introducción ... 506
2 La seguridad pública en el contexto de la seguridad nacional ... 507
2.1 La evolución del concepto de seguridad pública ... 507
2.2 La seguridad nacional como política del Estado ... 509
2.3 Relación entre seguridad interior y defensa nacional ... 510
3 Marco jurídico de la participación de las Fuerzas Armadas en seguridad pública en España ... 511
3.1 Fundamento constitucional de la actuación de las Fuerzas Armadas ... 511
3.2 Marco normativo aplicable en seguridad pública ... 513
3.3 Principios de subsidiariedad, excepcionalidad y mando civil ... 514
3.4 Límites jurídicos y garantías democráticas ... 515
4 Capacidades de las Fuerzas Armadas aplicables a la seguridad pública en España ... 517
4.1 Capacidades de despliegue, apoyo logístico y apoyo operativo ... 517
4.2 La Unidad Militar de Emergencias como referencia operativa ... 518

Página

5 La participación reciente de las Fuerzas Armadas en la seguridad pública en España 520
5.1 Actuaciones recientes de las fuerzas armadas en el ámbito interior 520
5.2 Lecciones aprendidas en el contexto español 525
6 Modelos comparados en el entorno europeo 527
6.1 Francia: empleo de las Fuerzas Armadas en la seguridad interior 527
6.2 Italia: modelo híbrido y cooperación estructurada 529
6.3 Reino Unido: apoyo militar a las autoridades civiles 532
6.4 Enseñanzas aplicables al caso español 533
7 Riesgos asociados de una mayor participación de las Fuerzas Armadas en la seguridad pública en España 535
7.1 Percepción ciudadana de la presencia militar en la seguridad pública 535
7.2 Cambio cultural en la sociedad española en materia de defensa 537
8 Hacia un modelo de colaboración entre Fuerzas Armadas y fuerzas y cuerpos de seguridad en España 539
8.1 Principios rectores del modelo 539
8.2 Condicionantes para la implantación del modelo 541
8.2.1 Necesidad de un nuevo marco normativo 542
9 Conclusiones 544
Bibliografía 546
Composición del grupo de trabajo 553
Relación de Monografías del CESEDEN 555

Prólogo

José Antonio Fuentes de la Orden

La presente obra, titulada *Selección de los diez mejores trabajos de fin de curso del XXVI CEMFAS y I CAEID*, constituye mucho más que una recopilación académica. Es, en esencia, el reflejo del compromiso, la dedicación y la excelencia intelectual de quienes han formado parte de estas dos iniciativas formativas, y al mismo tiempo, un testimonio del esfuerzo institucional por fomentar el pensamiento crítico, la investigación rigurosa y la aplicación práctica del conocimiento.

A lo largo de los años, la edición de este libro se ha consolidado como una tradición que trasciende lo meramente académico. No se trata solo de distinguir a los alumnos cuyos trabajos han sido mejor valorados, sino de ofrecer un espacio donde el talento emergente pueda ser reconocido, compartido y proyectado hacia la comunidad profesional y académica. En este sentido, cada edición representa una instantánea del nivel alcanzado por los participantes, así como de las inquietudes, desafíos y perspectivas que caracterizan a cada promoción.

El XXVI CEMFAS y el I CAEID marcan un punto de encuentro entre la experiencia consolidada y la innovación. Por un lado, el CEMFAS, con su trayectoria ya consolidada, ha demostrado ser un referente en la formación especializada, manteniendo un estándar de calidad que se ha fortalecido con cada edición. Por otro lado, el CAEID, en su primera edición, aporta una mirada renovada, integrando nuevas metodologías, enfoques y líneas de trabajo que enriquecen el conjunto y abren nuevas posibilidades de desarrollo.

Los trabajos seleccionados en esta obra son el resultado de un proceso exigente, tanto para los alumnos como para el equipo docente y evaluador. Cada uno de ellos ha sido concebido como una pieza única, en la que confluyen la formación recibida, la experiencia previa de sus autores y su capacidad para analizar, sintetizar y proponer soluciones en contextos complejos. La calidad de estos trabajos no reside únicamente en el dominio técnico de los temas abordados, sino también en la claridad expositiva, la solidez argumentativa y la pertinencia de sus conclusiones.

Cabe destacar que el proceso de selección no ha sido sencillo. El nivel general de los trabajos presentados ha sido notablemente alto, lo que refleja no solo el esfuerzo individual de los alumnos, sino también la eficacia de los programas formativos y la implicación del profesorado. La elección de los diez mejores responde a criterios de excelencia, originalidad, aplicabilidad y rigor metodológico, entre otros aspectos. Sin embargo, es importante reconocer que cada uno de los trabajos elaborados durante el curso ha contribuido, en mayor o menor medida, al enriquecimiento colectivo del conocimiento generado.

En este libro, el lector encontrará una diversidad de temas, enfoques y perspectivas que ponen de manifiesto la amplitud y profundidad de los contenidos abordados en ambos cursos. Desde análisis estratégicos hasta estudios aplicados, pasando por propuestas innovadoras y reflexiones críticas, cada trabajo ofrece una visión particular que invita a la reflexión y al debate. Esta pluralidad no solo enriquece la obra, sino que también refleja la complejidad de los ámbitos en los que se inscriben estos programas formativos.

Asimismo, esta publicación cumple una función esencial como puente entre el ámbito académico y el profesional. Los trabajos aquí recogidos no son ejercicios teóricos aislados, sino propuestas que, en muchos casos, tienen una clara vocación de aplicación práctica. En este sentido, el libro se convierte en una herramienta de consulta y referencia para quienes buscan comprender mejor los retos actuales y explorar posibles vías de actuación.

No puede dejar de mencionarse el papel fundamental del profesorado, cuya labor ha sido clave en el desarrollo de estos trabajos. Su acompañamiento, orientación y exigencia han permitido a los alumnos alcanzar niveles de excelencia que se ven reflejados en las páginas de esta obra. Del mismo modo, la labor del equipo

evaluador ha sido determinante para garantizar un proceso de selección justo, riguroso y transparente.

Igualmente, es necesario reconocer el esfuerzo y la dedicación de los alumnos. La elaboración de un trabajo de fin de curso implica no solo la aplicación de conocimientos adquiridos, sino también una inversión significativa de tiempo, energía y compromiso. Detrás de cada uno de los trabajos seleccionados hay horas de estudio, reflexión, revisión y mejora continua. Este libro es, en definitiva, un reconocimiento a ese esfuerzo.

La continuidad de esta publicación a lo largo de los años pone de manifiesto la importancia de generar espacios donde el conocimiento pueda ser compartido y difundido. En un contexto en constante cambio, en el que los desafíos son cada vez más complejos, resulta fundamental contar con aportaciones rigurosas y bien fundamentadas que contribuyan a la toma de decisiones y al desarrollo de nuevas estrategias.

Con esta nueva edición, se reafirma el compromiso con la excelencia académica y la promoción del talento. Al mismo tiempo, se consolida una iniciativa que no solo reconoce el mérito individual, sino que también fortalece el prestigio de los programas formativos a los que pertenece.

Se invita al lector a adentrarse en estas páginas con una mirada abierta y reflexiva, dispuesto a descubrir no solo los resultados de un proceso académico, sino también las ideas, inquietudes y propuestas que configuran el presente y el futuro de este ámbito de conocimiento.

Que esta obra sirva, por tanto, como fuente de inspiración, aprendizaje y reconocimiento. Y que continúe siendo, en futuras ediciones, un reflejo fiel del esfuerzo colectivo por alcanzar la excelencia.

A continuación, se incorporan unas líneas dedicadas a cada uno de los trabajos seleccionados, con el fin de contextualizar su aportación y poner en valor su relevancia dentro del conjunto de la obra:

El trabajo titulado *Empleo de marcos de trabajo KANBAN para la identificación y gestión de cargas de trabajo en el CEMFAS* aborda la aplicación de metodologías ágiles en entornos institucionales complejos, demostrando cómo herramientas propias del ámbito empresarial pueden optimizar la planificación, la eficiencia y la transparencia en la gestión de recursos y tareas. Su valor

radica en trasladar soluciones prácticas y probadas a la administración pública, contribuyendo a una cultura organizativa más eficaz, algo esencial para instituciones vinculadas a la seguridad y defensa, donde la correcta gestión del tiempo y los recursos tiene un impacto directo en la operatividad.

En fusión nuclear, la panacea de la geopolítica energética: viabilidad, actores e impacto global, el autor explora uno de los debates más actuales en materia energética, analizando el potencial transformador de la fusión nuclear, los actores implicados y sus posibles repercusiones en el equilibrio geopolítico mundial. Este trabajo destaca por su visión estratégica y prospectiva, subrayando la importancia de la independencia energética como pilar de la seguridad nacional y del bienestar ciudadano, en un contexto donde la energía condiciona tanto la economía como la estabilidad internacional.

El estudio *Consecuencias doctrinales del nuevo «campo de batalla transparente»* profundiza en cómo las nuevas tecnologías de vigilancia, sensorización y acceso a la información están modificando la naturaleza del conflicto, obligando a una revisión de las doctrinas militares tradicionales. Su aportación es especialmente valiosa al anticipar escenarios en los que la superioridad informativa será decisiva, ofreciendo claves que pueden resultar determinantes para la adaptación de las Fuerzas Armadas españolas a los conflictos del futuro.

Por su parte, *Paradigma de seguridad en el Antropoceno: un Análisis de las Estrategias de Seguridad Nacional de España y Francia* ofrece una reflexión comparada sobre cómo dos países europeos adaptan sus estrategias a un contexto marcado por riesgos globales. Este trabajo sobresale por su capacidad de integrar variables medioambientales, sociales y políticas, poniendo de relieve que la seguridad ya no puede entenderse sin una visión amplia que afecta directamente a la vida diaria de los ciudadanos.

El trabajo *Mongolia y la geopolítica regional: relaciones internacionales y estrategias de cooperación* pone el foco en un actor frecuentemente olvidado, analizando su papel entre grandes potencias. Su mérito reside en ampliar el foco analítico hacia escenarios menos estudiados, aportando lecciones útiles sobre equilibrio estratégico y diplomacia que pueden inspirar la acción exterior española en contextos complejos.

En *La polarización social en EE. UU. durante el siglo XXI y su repercusión geopolítica sobre el vínculo transatlántico*, se exa-

mina cómo las dinámicas internas de la sociedad estadounidense influyen en sus relaciones exteriores. Este análisis resulta especialmente relevante por cuanto afecta a uno de los pilares fundamentales de la seguridad de España, como es la relación transatlántica, evidenciando cómo fenómenos sociales internos pueden tener consecuencias estratégicas globales.

El análisis *Evolución de la política pública antiterrorista contra ETA en el País Vasco. La policía autónoma vasca* constituye una aportación rigurosa al estudio de las políticas de seguridad, destacando el papel de las instituciones autonómicas. Su valor es doble: por un lado, preserva la memoria de un desafío crítico para España; por otro, ofrece enseñanzas aplicables a la lucha contra futuras amenazas, reforzando la resiliencia institucional.

El trabajo *Adaptación del Mando y Control de las FAS españolas a las operaciones multidominio* aborda uno de los desafíos clave de las Fuerzas Armadas contemporáneas. Su importancia es incuestionable, ya que incide directamente en la capacidad de respuesta de España ante crisis complejas, proponiendo mejoras que pueden traducirse en una mayor eficacia operativa y en una defensa más robusta del territorio nacional.

En la inteligencia artificial en la toma de decisiones en el nivel operacional. Impacto en la confrontación y comparación de líneas de acción, se analiza cómo la IA está transformando los procesos de decisión militar. Este trabajo destaca por su actualidad y aplicabilidad, mostrando cómo la tecnología puede reducir errores, optimizar recursos y, en última instancia, salvar vidas tanto en contextos militares como civiles.

El estudio *Capacidades militares de Arabia Saudí para la defensa de infraestructuras críticas en su litoral marítimo* examina la evolución de las capacidades defensivas de este país. Su relevancia trasciende el caso concreto, ofreciendo claves sobre la protección de infraestructuras críticas, un aspecto fundamental también para España, especialmente en lo relativo a sus propias instalaciones energéticas y portuarias.

En Influencia del pensamiento estratégico de Colin S. Gray en el pensamiento estratégico occidental, se realiza un recorrido por las aportaciones de este influyente teórico. El valor de este trabajo radica en su profundidad intelectual, proporcionando herramientas conceptuales que permiten comprender mejor los conflictos actuales y mejorar la toma de decisiones estratégicas.

El trabajo *Las migraciones desde África a España: una herramienta de política exterior* plantea una perspectiva innovadora al analizar los flujos migratorios desde un enfoque estratégico. Su aportación es, sobre todo, relevante para España, país directamente afectado por estas dinámicas, al ofrecer claves para una gestión más eficaz y humana de un fenómeno con profundas implicaciones sociales y de seguridad.

En *Análisis del impacto de una mayor participación de las Fuerzas Armadas en la seguridad pública en España*, se reflexiona sobre los límites y oportunidades de ampliar su papel en tareas civiles. Este estudio resulta de gran utilidad para el debate público, al aportar argumentos rigurosos que ayudan a definir el equilibrio entre seguridad y libertades.

El estudio *Las noticias falsas en el ámbito de la Defensa en España y la neutralidad de las agencias de verificación españolas* aborda el fenómeno de la desinformación. Su valor es especialmente significativo en una sociedad hiperconectada, donde la manipulación informativa puede afectar directamente a la estabilidad social y a la confianza en las instituciones.

Por su parte, *Estrategias de prevención y control del tráfico ilícito de drogas en el estrecho de Gibraltar: un enfoque multidisciplinar* ofrece un análisis integral de un problema complejo. Su carácter aplicado lo convierte en una herramienta de gran utilidad para las fuerzas de seguridad, contribuyendo a mejorar la eficacia en la lucha contra el crimen organizado.

El *Estudio de caso: Estados Unidos y el impacto de las exportaciones de GNL en la geopolítica de la energía (2014-2024)* examina cómo el auge del gas natural licuado ha reforzado la posición estratégica estadounidense. Este trabajo resulta clave para entender las dinámicas energéticas globales y su impacto en Europa y España, especialmente en términos de seguridad de suministro.

En *Confrontación de líneas de acción en el nivel operacional: implicaciones del nuevo paradigma multidominio*, se profundiza en la complejidad de la toma de decisiones en escenarios actuales. Su aportación es fundamental para mejorar los procesos de planificación militar, aumentando la eficacia y reduciendo la incertidumbre en contextos críticos.

El trabajo *El potencial de la IA generativa como herramienta de engaño* analiza los riesgos asociados a tecnologías emergentes.

Su relevancia es indiscutible en el ámbito de la seguridad, alertando sobre amenazas que ya comienzan a materializarse y que pueden afectar tanto a operaciones militares como a la vida cotidiana de los ciudadanos.

En *El papel de la Agencia Internacional de la Energía en la geopolítica global de la energía*, se estudia la relevancia de esta organización como actor clave. Este análisis permite comprender mejor los mecanismos de gobernanza energética y su influencia en la estabilidad internacional, con implicaciones directas para la política energética española.

El estudio *Tecnologías disruptivas. Impacto en la industria de* defensa ofrece una visión amplia sobre la innovación tecnológica. Su valor reside en identificar tendencias que definirán el futuro de la defensa, permitiendo anticipar cambios y reforzar la competitividad del sector.

Finalmente, *Aplicación de la inteligencia económica en la lucha contra la delincuencia organizada y la delincuencia grave* pone de relieve la importancia de integrar herramientas analíticas en la seguridad. Este trabajo destaca por su enfoque práctico y su capacidad para mejorar la eficacia en la lucha contra amenazas complejas, contribuyendo de manera directa a la protección de la sociedad.

Cada uno de estos trabajos no solo refleja un alto nivel académico, sino que constituye una aportación valiosa y aplicable a los grandes desafíos contemporáneos, reforzando el vínculo entre conocimiento, seguridad y servicio a la sociedad.

Capítulo primero

Aplicación de la inteligencia económica en la lucha contra la delincuencia organizada y la delincuencia grave

Antonio Balas Dávila

Sumario

El concepto de seguridad, en los últimos veinte años, se ha venido expandiendo, alcanzando la generalidad de los ámbitos y de los espacios, tanto reales como virtuales. Esta circunstancia se enmarca en el difuso y omnipresente fenómeno de la globalización, la «hiperconectividad» y el desarrollo exponencial de las tecnologías.

En este contexto, la inteligencia se erige en fundamental para cualquier estrategia de seguridad. Sin embargo, la complejidad y especificidad inherente a cada ámbito de interés, requiere de una inteligencia especializada. En este sentido, la seguridad económica es un elemento esencial de la seguridad nacional y, por tanto, requiere una inteligencia *ad hoc*.

Es precisamente en el marco de la seguridad nacional donde la inteligencia económica coadyuva en la lucha contra la delincuencia organizada y grave, detectando de manera temprana, patrones inusuales en un determinado sector productivo, transacciones sospechosas o la aparición de elementos anómalos en un concreto contexto mercantil.

Palabras clave

Seguridad económica, Inteligencia económica, Delincuencia organizada y grave, Globalización, Seguridad nacional.

Application of economic intelligence in the fight against organized crime and serious crime

Abstract

Over the past two decades, the notion of security has broadened considerably, extending across virtually all domains and spaces, both physical and virtual. This expansion is intricately linked to the pervasive dynamics of globalization, hyper-connectivity, and the exponential advance of technology.

In this environment, intelligence becomes indispensable to any security strategy. Yet the complexity and specificity of each domain call for specialized approaches. Within this framework, economic security stands as a core dimension of national security and thus demands tailored intelligence.

Economic intelligence, in turn, plays a pivotal role in the National Security system by supporting the fight against serious and organized crime. It does so through the early identification of atypical patterns in productive sectors, suspicious transactions, and the emergence of anomalous elements in commercial contexts.

Key words

Economic security, Economic intelligence, Serious and organized crime, Globalization, National security.

Lista de abreviaturas

AEAT	Agencia Estatal de Administración Tributaria
AI	Artificial Intelligence / Inteligencia Artificial
AML	Anti-Money Laundering / Lucha contra el blanqueo de capitales
AMLA	Autoridad Europea contra el Blanqueo de Capitales
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (lucha contra el blanqueo de capitales y contra la financiación del terrorismo)
ASEAN	Asociación de Naciones del Sudeste Asiático / The Association of Southeast Asian Nations
AVE	Asociación Valenciana de Empresarios
BC	Blanqueo de Capitales
BCE	Banco Central Europeo
BdE	Banco de España
BfV	Bundesamt für Verfassungsschutz / Oficina Federal para la Protección de la Constitución (Alemania)
BI	Business Intelligence / Inteligencia de negocios
BM	Banco Mundial
BRICS	Brasil, Rusia, India, China y Sudáfrica
CAEID	Curso de Altos Estudios de Inteligencia y Defensa
CCAA	Comunidades Autónomas
CCN-CERT	Centro Criptológico Nacional – Computer Emergency Response Team
CE	Constitución Española
CEOE	Confederación Española de Organizaciones Empresariales
CEPYME	Confederación Española de la Pequeña y Mediana Empresa
CI	Competitive Intelligence / Inteligencia Competitiva
CIDOB	Barcelona Centre for International Affairs (en catalán Centre d'Informació i Documentació Internacionals a Barcelona).
CIFAS	Centro de Inteligencia de las Fuerzas Armadas

CITCO	Centro de Inteligencia contra el Terrorismo y el Crimen Organizado
CMN	Corporaciones Multinacionales
CNMC	Comisión Nacional de los Mercados y la Competencia
CNMV	Comisión Nacional del Mercado de Valores
CNI	Centro Nacional de Inteligencia
CNP	Cuerpo Nacional de Policía
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas
COREPER	Comité de Representantes Permanentes (del Consejo de la UE)
CPFF	Consejo de Política Fiscal y Financiera
CPI	Corte Penal Internacional
CSN	Consejo de Seguridad Nacional
DGEIPYME	Dirección General de Estrategia Industrial y de la Pequeña y Mediana Empresa
DG TAXUD	Dirección General de Fiscalidad y Unión Aduanera (Comisión Europea)
DG TRADE	Dirección General de Comercio (Comisión Europea)
DG	Delincuencia Grave
DO	Delincuencia Organizada
DSN	Departamento de Seguridad Nacional
EARTO	Asociación Europea de Organizaciones de Investigación y Tecnología / European Association of Research and Technology Organisations
EBA	European Banking Authority / Autoridad Bancaria Europea
EE.UU.	Estados Unidos (de América)
EES	Estrategia Española de Seguridad (2011)
EFECC	European Financial and Economic Crime Centre (Centro de Europol contra la delincuencia financiera y económica)
EFIPPP	Europol Financial Intelligence Public Private Partnership / Asociación Público-Privada de Inteligencia Financiera de Europol

EIOPA	European Insurance and Occupational Pensions Authority / Autoridad Europea de Seguros y Pensiones de Jubilación
EMPACT	European Multidisciplinary Platform Against Criminal Threats (Plataforma Multidisciplinar Europea contra las Amenazas Criminales)
ENCODG	Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave
EPPO	European Public Prosecutor's Office / Fiscalía Europea
ESCB	European System of Central Banks / Sistema Europeo de Bancos Centrales
ESMA	European Securities and Markets Authority / Autoridad Europea de Valores y Mercados
ESN	Estrategia de Seguridad Nacional
ESRB	European Systemic Risk Board / Junta Europea de Riesgo Sistémico
EU INTCEN	EU Intelligence and Situation Centre (Centro de Inteligencia y Situación de la UE)
EUIPO	European Union Intellectual Property Office (Oficina de Propiedad Intelectual de la UE)
EUROJUST	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
EUMS INT	Intelligence Directorate of the EU Military Staff (Dirección de Inteligencia del Estado Mayor de la UE)
EU SOCTA	EU Serious and Organised Crime Threat Assessment (Evaluación de Amenazas de Crimen Grave y Organizado de la UE)
FDI	Foreign Direct Investment (Inversión extranjera directa – IED)
FEDEA	Fundación de Estudios de Economía Aplicada
FEDER	Fondo Europeo de Desarrollo Regional

FEDIT	Federación Española de Centros Tecnológicos
FEMP	Federación Española de Municipios y Provincias
FGE	Fiscalía General del Estado
FIU	Financial Intelligence Unit / Unidad de Inteligencia Financiera
FMI	Fondo Monetario Internacional
FSE	Fondo Social Europeo
FSR	Financial Stability Review (Informe de Estabilidad Financiera del BCE)
G8	Grupo de los Ocho
G20	Grupo de los Veinte
G77	Grupo de los Setenta y Siete (ONU)
GAFI / FATF	Grupo de Acción Financiera Internacional / Financial Action Task Force
GATT	General Agreement on Tariffs and Trade / Acuerdo general sobre Aranceles Aduaneros y Comercio
GRECO	Grupo de Estados contra la Corrupción (Consejo de Europa)
HFC	Hybrid Fusion Cell (Célula de Fusión Híbrida de la UE)
HUMINT	Human Intelligence / Inteligencia de Fuentes Humanas
I+D+i	Investigación + Desarrollo + innovación
IASN	Informe Anual de Seguridad Nacional
IBEX	Índice Bursátil Español
IE	Inteligencia Económica
IED/FDI	Inversión Extranjera Directa
IF	Inteligencia Financiera
INCIBE	Instituto Nacional de Ciberseguridad
INE	Instituto Nacional de Estadística
INTERPOL	International Criminal Police Organization / Organización Internacional de Policía Criminal

IPCR-ISAA	Integrated Political Crisis Response / Integrated Situational Awareness and Analysis
IVA	Impuesto sobre el Valor Añadido
LEAs	Law Enforcement Agencies (Fuerzas y Cuerpos de Seguridad)
LECrim	Ley de Enjuiciamiento Criminal
LOSU	Ley Orgánica del Sistema Universitario, aprobada en España en 2023 (Ley Orgánica 2/2023, de 22 de marzo)
LRBRL	Ley Reguladora de las Bases del Régimen Local
MAIC	Máster en Análisis de Inteligencia y Ciberinteligencia
MERCOSUR	Mercado Común del Sur
MITI	Ministry of International Trade and Industry / Ministerio de Industria y Comercio exterior
MRR	Mecanismo de Recuperación y Resiliencia (instrumento central de la UE para canalizar los fondos Next Generation EU)
MTIC	Missing Trader Intra-Community / Fraude intracomunitario de comercio
MUR	Mecanismo Único de Resolución
MUS	Mecanismo Único de Supervisión
OCDE	Organización para la Cooperación y el Desarrollo Económico
OCC	Oficina de Coordinación de Ciberseguridad
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OCTA	Organised Crime Threat Assessment (antiguo documento de Europol) / Evaluación de la amenza del Crimen Organizado
OEPM	Oficina Española de Patentes y Marcas
OIIE	Observatoire International de l'Intelligence Économique / Observatorio Internacional de Inteligencia Económica
OLAF	Oficina Europea de Lucha contra el Fraude

OMC	Organización Mundial del Comercio
ONG	Organización No Gubernamental
ONI	Oficina Nacional de Investigación de Aduanas e Impuestos Especiales (AEAT)
ONIF	Oficina Nacional de Investigación del Fraude (AEAT)
ONU	Organización de las Naciones Unidas
ORGA	Oficina de Recuperación y Gestión de Activos
OSCE	Organización para la Seguridad y la Cooperación en Europa
OSINT	Open Source Intelligence / Inteligencia de Fuentes Abiertas
OTAN	Organización del Tratado del Atlántico Norte
OUA	Organización para la Unidad Africana
PBC/FT	Prácticas de Blanqueo de Capitales y Financiación del Terrorismo
PENTRA	Plan Estratégico Nacional contra la Trata y la Explotación de Seres Humanos
PESC	Política Exterior y de Seguridad Común (de la UE)
PIB	Producto Interior Bruto
PIF	Informe sobre la Protección de los Intereses Financieros de la UE
PNUMA	Programa de las Naciones Unidas para el Medio Ambiente
PRTR	Plan de Recuperación, Transformación y Resiliencia
pymes	Pequeñas y medianas empresas
REF	Régimen Económico y Fiscal (de Canarias)
RECI	Red Española de Ciudades Inteligentes
RIS3	Research and Innovation Strategies for Smart Specialisation / Estrategias Regionales de Especialización Inteligente
ROI	Registro de Operadores Intracomunitarios
RSC	Responsabilidad Social Corporativa

RTO	Research and Technology Organisations / Organizaciones de Investigación y Tecnología
SATCEN	European Union Satellite Centre / Centro de Satélites de la UE
SEAE / EEAS	Servicio Europeo de Acción Exterior / European External Action Service
SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias
SEPI	Sociedad Estatal de Participaciones Industriales
SESF	Sistema Europeo de Supervisión Financiera
SGAE	Sociedad General de Autores y Editores
SIAC	Capacidad Única de Análisis e Inteligencia / Single Intelligence Analysis Capacity
SIE	Sistema de Inteligencia Económica
SIGINT	Signals Intelligence / Inteligencia de Señales
SOCTA	Serious and Organised Crime Threat Assessment (véase EU SOCTA) / Evaluación de la amenaza de la Delincuenica Grave y Organizada
STS	Sentencia del Tribunal Supremo
SVA	Servicio de Vigilancia Aduanera (AEAT)
TFM	Trabajo Fin de Máster
TFUE	Tratado de Funcionamiento de la Unión Europea
UA	Unión Africana
UCO	Unidad Central Operativa (Guardia Civil)
UDEF	Unidad de Delincuencia Económica y Fiscal (CNP)
UE	Unión Europea
UIE	Unidad de Inteligencia Económica
UIF	Unidad de Inteligencia Financiera
UK	United Kingdom / Reino Unido
UNCTAD	United Nations Conference on Trade and Development / Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

UNICRI	United Nations Interregional Crime and Justice Research Institute Institute / Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y Justicia
UNODC	United Nations Office on Drugs and Crime / Oficina de las Naciones Unidas contra la Droga y el Delito
USA	United States of America / Estados Unidos de América
USMCA/T-MEC	United States-Mexico-Canada Agreement / Tratado entre México, Estados Unidos y Canadá
VAB	Valor Añadido Bruto
VAT	Value Added Tax / Impuesto sobre el Valor Añadido
VTTL	VAT Total Tax Liability / Responsabilidad Fiscal Total de IVA
WoS	Web of Science

1 Antecedentes

Durante los últimos veinte años, el mundo ha sufrido una serie de calamidades de afectación mundial. En este sentido, cabe destacar la crisis financiera global de 2008 (Stiglitz, 2010), la pandemia de COVID-19 (Baldwin y Weder, 2020) o los efectos del cambio climático (Nordhaus, 2013). En todos estos amargos sucesos, la componente económica ha estado siempre presente, proyectándose en las diferentes fatalidades hacia los confines más alejados, a través de una suerte de onda expansiva de esa misma naturaleza.

Este extremo se explica, en gran medida, por el proceso de la globalización contemporánea y su constituyente económico a través de diferentes hitos acaecidos, ubicados en distintos momentos del siglo xx y xxi:

- Desmantelamiento del sistema de Bretton Woods y liberalización financiera, generando una expansión de las conexiones económicas globales (Osterhammel y Petersson, 2005).
- Revolución tecnológica y digital, posibilitando una economía global interconectada, donde las interacciones sociales y económicas ya no están limitadas por la geografía o una secuencia temporal acostumbrada, emergiendo una economía basada en la información, en la capacidad de las redes para procesarla y distribuirla mundialmente, en tiempo real (Castells, 2006).
- Consolidación del neoliberalismo, facilitando la desregularización y la apertura de nuevos mercados, derivando en una reconfiguración de estructuras económicas y sociales a nivel mundial (Harvey, 2007).
- Caída del muro de Berlín, como catalizador de la expansión del capitalismo, el libre mercado y la interconexión tecnológica, llegando, incluso, a ser considerada como el punto de inicio del actual fenómeno de globalización (Friedman, 1999).
- Surgimiento de China como potencia económica, operando cambios profundos en todos los órdenes, constituyéndose en un elemento polarizante al resistirse a una occidentalización (Jacques, 2012).

Todo ello moldea un orden mundial explicado a través de las teorías constructivistas, vinculadas a las relaciones internacionales, poniendo en valor las ideas, las identidades, las normas y los

procesos sociales frente a factores materiales más propios del realismo e incluso del idealismo, asociados a teorías geopolíticas. Esta concepción puede resumirse en la famosa frase «Anarchy is what states make of it» (Wendt, 1992).

En este sentido, una vez rota la bipolaridad entre Estados Unidos (EE. UU.) y la Unión Soviética, escenificada con la caída del Muro de Berlín, aparecieron nuevas amenazas y riesgos que intensificaron la relación entre la seguridad y la defensa. La globalización y la creciente interconectividad favorecieron espacios de cooperación internacional para resolver las diferentes crisis y conflictos (Valero, 2005).

Esto fue conformando una nueva disposición mundial que supuso un fortalecimiento, expansión y redefinición de organizaciones como Organización de las Naciones Unidas (ONU), la Organización del Tratado del Atlántico Norte (OTAN) o la Unión Europea (UE), así como la institucionalización del comercio global a través de la creación de la Organización Mundial del Comercio (OMC).

De este modo, la ONU ganó protagonismo en el ámbito de la seguridad y la gobernanza global, con un sensible aumento de las misiones de paz y las intervenciones humanitarias.

La OTAN se transformó en una organización de seguridad colectiva más flexible, incorporando antiguos países del bloque soviético y realizando operaciones fuera de su área tradicional.

Del mismo modo, la UE se institucionalizó a través del Tratado de Maastricht (1992), consolidando la unión económica y monetaria con el establecimiento del euro (1999) y propiciando una Política Exterior y de Seguridad Común (PESC), ampliando, igualmente, los países miembros, a partir de 2004, sumándose países que habían permanecido bajo la influencia soviética.

Asimismo, la OMC, fundada en 1995 como sucesora del *General Agreement on Tariffs and Trade* (GATT), se configuró como la base del sistema multilateral de comercio[1]. Otras instituciones, como el Fondo Monetario Internacional (FMI) o el Banco Mundial (BM), asumieron un papel activo en la reconversión económica de Europa del Este y Rusia, promoviendo reformas de mercado.

[1] Web oficial del Ministerio de Economía, Comercio y Empresa. Política comercial de la UE. Organización Mundial de Comercio. Disponible en: https://comercio.gob.es/PoliticaComercialUE/OMCOrganismosInternacionales/Paginas/omc.aspx [Consulta: 17 abril 2025].

De igual manera, cabe reseñar la creación de la Unión Africana (UA), en 2002, con una intención más ambiciosa, desde una perspectiva continental, que la anterior Organización para la Unidad Africana (OUA), el nacimiento de la Corte Penal Internacional (CPI), en 2002, o el reforzamiento, con el Acta de París, de la Organización para la Seguridad y la Cooperación en Europa (OSCE), manteniendo un rol clave en la transición poscomunista en el control de conflictos.

En Asia, también proliferaron organizaciones que procuran fortalecer, fundamentalmente en los ámbitos de seguridad y económico, a los distintos países miembros de esa región, constituyéndose, en ocasiones, en una respuesta o alternativa a la opción proveniente de occidente (Strand *et al*., 2016).

Es decir, los distintos países se integraron en organizaciones intergubernamentales y supranacionales, cediendo, en mayor o menor medida, parte de su soberanía con el fin de alcanzar superiores cotas de desarrollo y de seguridad, admitiendo que, otorgarse normas comunes y confiar en instituciones globales para la resolución de conflictos, podrían ser vías aceptables para mantener y mejorar las cotas de bienestar y desarrollo de cada país.

Todo ello, desde un dominio casi unipolar de Estados Unidos, que generó un sistema duradero y pacífico al reducir la rivalidad hegemónica e incentivar la cooperación (Wohlforth, 1999). Estas circunstancias contribuyeron al establecimiento de un sistema mundial denominado multilateralismo[2].

Ya entrado el siglo XXI, la propia Estrategia Española de Seguridad de 2011 afirmaba que

> «España aboga por una interdependencia responsable en la que se fomenten sinergias para buscar soluciones conjuntas a los retos comunes. Ni podemos ni debemos trabajar en solitario. Como país comprometido con el desarrollo, la paz y la seguridad mundiales, España trabaja a través de la UE, la ONU, la OTAN, la OSCE, el G20 y otras organizaciones para diseñar y alcanzar un orden internacional estable que promueva la justicia, la prosperidad y la seguridad global».

[2] Entendido como una configuración institucional mediante la cual se articulan las relaciones entre tres o más Estados, sustentada en principios de conducta generalizados. Dichos principios determinan comportamientos considerados apropiados para categorías amplias de acciones, sin atender a los intereses particulares de los actores implicados ni a las exigencias estratégicas que puedan derivarse de situaciones específicas (Ruggie, 1992).

En esta dinámica de interconexión mundial, el concepto de seguridad también mutó tras la superación del bipolarismo, percibiéndose una menor amenaza en cuanto a guerras interestatales directas, emergiendo una visión holística que abarcaba distintos ámbitos como la seguridad económica, el terrorismo internacional, el crimen organizado, las migraciones, la seguridad medioambiental o la seguridad sanitaria (Buzan, 1991). Asimismo, esta interdependencia deriva en una necesidad de superar el ámbito territorial nacional, preconizado por Alberto Antón González[3] en los Cuadernos de Inteligencia, número 2, *Nuevas amenazas a la Seguridad Nacional*, como referencia última, en un sentido estricto, de la seguridad nacional.

De este modo, durante finales del siglo XX e inicios del siglo XXI se va moldeando el concepto incipiente de seguridad económica, confiriendo a factores económicos, como la competitividad industrial y la innovación tecnológica, una especial relevancia para la seguridad nacional, argumentando que una economía sólida proporciona los recursos necesarios para mantener capacidades militares y responder a amenazas externas (Neu y Wolf, 1994).

Pero adquiere un protagonismo principal después de la crisis financiera de 2008, momento en el que, mundialmente, se toma conciencia de que las fuertes interconexiones globales afectan, también, a los riegos, descubriendo vulnerabilidades (World Economic Forum, Global Risks, 2010).

Consecuentemente, las decisiones económicas influyen en la seguridad. De manera inmediata, se evidencia que el establecer una estrategia en defensa y seguridad, a largo plazo, ha de sustentarse en una acumulación planificada de recursos (Murphy y Topel, 2013).

Ampliando el foco, la inversión en innovación tecnológica, en políticas industriales y en otros sectores estratégicos determinará la consecución de esa pretendida seguridad nacional (Weiss, 2014).

De esta manera, se percibe la idoneidad de enfoques que integren consideraciones económicas en las políticas de seguridad, ya que los recursos económicos y las decisiones financieras influyen en la seguridad y la estabilidad (Silwal *et al*., 2021).

[3] Vid.https://www.defensa.gob.es/documents/2073105/2223574/articulo_3_cuaderno_inteligencia_2.pdf/0dde73a3-76e8-537d-2e29-ea2af230a0f0?t=1732100696646 [Consulta: 21 abril 2025].

En este sentido, la propia Estrategia de Española de Seguridad (EES) de 2011, establecía que la seguridad económica es un interés vital de España en cuanto elemento constitutivo del Estado. Igualmente, la Estrategia de Seguridad Nacional (ESN) de 2013 indicaba que la seguridad económica «se erige cada vez de forma más clara y patente en requisito esencial y parte integral de la seguridad nacional, debido a su repercusión en la puesta en marcha de actuaciones gubernamentales y en el bienestar de los ciudadanos».

La inteligencia y la seguridad nacional están íntimamente unidas. La inteligencia es la herramienta que permite al Estado entender el mundo y los riesgos a los que se enfrenta, mientras que la seguridad nacional es el fin último al que sirve ese entendimiento (Johnson, 2017).

Como indica la publicación de la Escuela Superior de las Fuerzas Armadas, *Cuaderno de Inteligencia 2. Nuevas amenazas a la Seguridad Nacional*, en la actualidad

> «Los riesgos y las amenazas son multidimensionales, cambiantes, difíciles de evaluar y de predecir. Esto da lugar a crisis mucho más frecuentes, más complejas, más difíciles de prever y de gestionar, que requieren actuaciones en el multidominio y donde disponer de buenos análisis de inteligencia es crítico» (Sabaté Aragonés, 2023: 13).

Este panorama muestra la significativa incidencia de la economía en los estados y en su ciudadanía, influyéndoles en múltiples aspectos. Por lo que es lógico plantearse la conveniencia de consolidar una posición donde la economía coadyuve a mantener el bienestar social y el desarrollo de los estados, protegiéndolos, a su vez, de aquellas amenazas que pudieran menoscabar esta posición.

2 La seguridad y la inteligencia económica

El panorama descrito en el apartado anterior, asociado a una suerte de multilateralismo y de cooperación internacional, en concordancia con una visión geopolítica constructivista e idealista, ha empezado a virar[4] hacia un mundo multipolar, menos colaborativo, tendente al unilateralismo.

[4] En concordancia con lo dispuesto en el Informe Anual de Seguridad Nacional (IASN) 2023 y la acción continuada de Rusia descrita en el IASN 2024.

Esta deriva menoscaba la fluidez de las relaciones comerciales internacionales y, en consecuencia, afecta negativamente a la economía desde una perspectiva global.

Esta circunstancia económica afecta a la seguridad de los países de manera determinante. En este sentido, cabe mencionar las recientes tensiones entre EE. UU. y la UE, donde el incremento de los aranceles y exigencias de índole económico, en diferentes ámbitos, realizadas por el país americano incide en la política de seguridad de la UE.

En este contexto, los países han puesto en valor la importancia de mantener una seguridad económica adecuada, que les permita cierta independencia de actuación en el ámbito nacional e internacional, favoreciendo sus intereses. Así, Estados Unidos en su Estrategia de Seguridad Nacional de 2017 afirmaba que una economía fuerte protege al pueblo estadounidense y apuntala su poder.

En España, la inteligencia está íntimamente ligada a la seguridad. Esta circunstancia se observa en la lógica y evidente relación existente entre el artículo 1 de la Ley 11/2002, de 6 de mayo, en el que se define el propósito del Centro Nacional de Inteligencia (CNI), y el artículo 3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, donde se define, precisamente, la seguridad nacional.

Asimismo, de manera específica, esta ligazón se manifiesta en el artículo 9.2 de la Ley 36/2015, de 28 de septiembre, precisando que los servicios de inteligencia e información apoyarán permanentemente al Sistema de Seguridad Nacional. De tal modo, que la inteligencia se pone al servicio del mantenimiento de la seguridad nacional.

De esta manera, el Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, adquiere un papel relevante como el órgano que asiste al presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, siendo el responsable de la gestión y supervisión de este último, así como de la elaboración de las líneas estratégicas en este ámbito.

La prevalencia de esta comisión sobre otras se pone de manifiesto, también, en el propio funcionamiento de las comisiones. Pues, aunque normativamente no existe una prelación entre comisiones delegadas, es significativo que solo en la Comisión

Delegada del Gobierno para la Seguridad Nacional se prevea la asistencia del rey de España, así como el deber de ser informado anualmente. Del mismo modo, es la única comisión delegada donde por lo general se recoge que la presidencia le corresponderá al presidente del Gobierno (salvo si asiste el rey, que entonces lo preside).

2.1 Aproximación al concepto de inteligencia económica

En relación con la triple acepción realizada por Sherman Kent (1966) y Mark M. Lowenthal (2012) organización, proceso y producto, este apartado se dirigirá a delimitar el concepto de inteligencia vinculado al producto.

En este sentido, desde finales del siglo xx hasta el tiempo actual se han ido sucediendo diferentes definiciones, entre las que se podría resaltar las realizadas por Sherman Kent, en 1966, que concibe la inteligencia como el producto resultante de la recolección, procesamiento, integración, análisis, evaluación e interpretación de información disponible sobre áreas o actores de interés.

Asimismo, Jennifer E. Sims define la inteligencia como la recopilación, análisis y diseminación de información para decisores en materia de seguridad nacional (Sims y Gerber, 2005: 15), inmersos en un entorno competitivo.

Peter Gill y Mark Phythian proponen una definición funcional y relacional, que integra proceso, producto y acción para anticipar y preservar la ventaja relativa (Gill y Phythian, 2012). Mientras que Loch K. Johnson incide en el «conocimiento y preconocimiento» (Johnson, 2007: 3) como antesala de la decisión.

Rubén Arcos aporta una visión funcional orientada a la decisión y la seguridad entendiendo que la inteligencia constituye la primera línea de la defensa y la seguridad del Estado (Arcos, 2012), aportando el conocimiento especializado para que los dirigentes puedan tomar las decisiones en las mejores condiciones.

Antonio M. Díaz Fernández muestra, también, la finalidad estratégica de la anticipación y la influencia, al conferirle a la inteligencia la comprensión del entorno para anticiparse a él (Díaz Fernández, 2013) y modificarlo, en cierta medida.

En base a todo ello, y sin extenderse mucho más, se podría definir el concepto de inteligencia, en el marco de esta monografía, como un producto analítico orientado a un decisor y sobre un asunto

concreto, desarrollado mediante un ciclo (dirección/obtención/análisis/difusión) que busca reducir la incertidumbre de manera oportuna, para preservar la seguridad o la ventaja relativa del actor, así como eludir riesgos y aprovechar oportunidades.

A partir de todo lo anterior, se puede determinar que la inteligencia es un proceso que, bajo una dirección, debe ser alimentado y analizado de manera adecuada para resultar el producto inteligencia.

De este modo y en este contexto, cabe diferenciar datos, información e inteligencia, cada uno de los cuales asociado a un nivel de elaboración distinto. Los datos son unidades básicas de observación, hechos brutos o registros aislados sobre realidades específicas huérfanos de contexto. Estos datos, recopilados de distinta forma y manera conforman la materia prima inicial.

Cuando esos datos se organizan, procesan, estructuran, analizan y se interrelacionan dotándoles de un significado contextualizado, se convierten en información una vez los datos han sido interpretados. La información agrega valor al dato, pero aún no implica un juicio analítico profundo.

Finalmente, la inteligencia es el producto final resultante de someter datos e información a un riguroso proceso analítico, evaluándolos, integrándolos y proyectándolos hacia escenarios futuros, orientando todo el proceso a facilitar una decisión minorando la incertidumbre, erigiéndose por tanto la inteligencia en un conocimiento anticipativo.

Llegados a este punto, teniendo como referencia el análisis realizado por Rafael Jiménez Villalonga, en Global Strategy[5], sobre los tipos de inteligencia, esta, en virtud de su finalidad, puede ser calificada como estratégica, operativa o táctica.

Inteligencia estratégica es aquella orientada al largo plazo, vinculada con la formulación de políticas generales, planes de alto nivel y objetivos fundamentales de una organización o Estado, entre la que se incluye la seguridad nacional. En el contexto de la seguridad nacional, la inteligencia estratégica suministra a la alta dirección del Estado apreciaciones sobre el entorno global, identificando actores, tendencias, riesgos emergentes y oportunidades que puedan afectarlos. Dado su carácter anticipativo, está muy ligada a la prospectiva. En el ámbito empresarial, la inteligencia

[5] Vid. https://global-strategy.org/tipos-de-inteligencia/

estratégica apoya a la alta dirección de la empresa (en la definición de su estrategia corporativa de largo plazo)[6].

La inteligencia operativa ocupa el eslabón intermedio entre la formulación estratégica y la acción inmediata. Su cometido es traducir la orientación estratégica en planes con un horizonte de medio plazo, proporcionando a los niveles intermedios el conocimiento necesario para diseñar, sincronizar y evaluar operaciones en un ámbito determinado.

De esta forma, se asegura su alineación con los objetivos estratégicos y su producto debe integrar indicadores, riesgos y cursos de acción con métricas de desempeño[7].

Para finalizar, la inteligencia táctica se asocia al corto plazo y al día a día de las diferentes áreas, proporciona alertas y apoyos informativos muy concretos para decisiones inmediatas, normalmente a mandos de unidad y equipos operativos.

Es importante destacar que estos tres niveles forman un continuo: la inteligencia estratégica marca la dirección general, la operativa traduce esa dirección en planes y coordina los medios, y la táctica ejecuta acciones concretas informadas por inteligencia de detalle. Cada una atendiendo a diferentes escalones de decisión[8].

En definitiva, la distinción entre inteligencia estratégica, operativa y táctica resulta útil para asegurar que cada decisor recibe el tipo de inteligencia adecuado a sus necesidades, garantizando así la eficacia de un sistema global de inteligencia[9].

Por otro lado, existen muchas tipologías de inteligencia según la materia a tratar, en el caso de esta monografía, al versar sobre el entorno económico, se tratará de definir la inteligencia económica.

---

[6] Se especializa en analizar el macroentorno competitivo y económico, previendo escenarios futuros, movimientos de competidores, cambios tecnológicos o regulatorios, de modo que la empresa pueda orientar sus decisiones estratégicas informadas sobre posibles amenazas y oportunidades de negocio.

[7] La Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2025 inscribe explícitamente esta capa en el diseño de la respuesta pública, al exigir la integración de inteligencia estratégica y operativa como base de prevención, investigación y análisis frente a redes delictivas, lo que confirma la importancia estructural en la planificación de políticas y campañas.

[8] Alta dirección política, mandos intermedios ministeriales o fuerzas de seguridad, y unidades ejecutoras respectivamente.

[9] En esta monografía, la inteligencia irá vinculada a alguno de estos niveles según el contexto, siendo siempre igual de relevante.

La inteligencia económica (IE) se ha consolidado como una disciplina específica, con rasgos que la diferencian de otras modalidades afines como la inteligencia competitiva, la inteligencia empresarial, o las prácticas de *Big Data* y analítica de datos.

Una definición clásica, contenido en el Glosario de Inteligencia publicado por el Ministerio de Defensa de España, en 2007, describe la inteligencia económica como

> «el tipo de inteligencia que se ocupa de la obtención y el procesamiento de la información financiera, económica y empresarial de un Estado para permitir una eficaz salvaguarda de los intereses nacionales tanto en el interior como en el exterior».

La tradición francesa consolidó la IE en los años noventa con el Rapport Martre (1994) (Informe de Henri Martre), que la sitúa como la gestión estratégica de la información económica al servicio de la competitividad empresarial y del interés nacional, en un contexto de globalización y «guerra económica» no militar, pretendiendo coordinar la vigilancia, la protección del patrimonio informacional/tecnológico y la influencia (capacidad de proyectar normas y estándares) como función pública y de mantenimiento y desarrollo del ecosistema (Estado-empresa-territorios).

El «référentiel de formation en intelligence économique»[10], promovido por Alain Juillet[11], con el objeto de establecer los contenidos y pilares fundamentales para la formación de inteligencia económica en Francia, con un enfoque estratégico y operacional, formula una definición muy citada: la IE consiste en la gestión eficaz y la protección de la información estratégica por todo actor económico, con triple finalidad competitividad–seguridad–influencia.

Nicolas Moinet[12] enfatiza la IE como «dinámica colectiva» que busca agilidad mediante el uso estratégico de la información, reuniendo vigilancia, seguridad e influencia como campos operativos interdependientes.

[10] Referencia de formación en inteligencia económica.

[11] Fue nombrado en diciembre de 2003 «Haut responsable chargé de l'intelligence économique» (Alto Responsable para la Inteligencia Económica) por el primer ministro francés.

[12] Catedrático en la Université de Poitiers y figura destacada en la formación académica de inteligencia económica en Francia. Cofundador del Observatoire International de l'Intelligence Économique (OIIE).

Reino Unido ha tendido a integrar la IE en la noción más amplia de *national security intelligence*, centrada en la protección de intereses nacionales y financieros, en línea con las *UK National Security Strategies*. Existe un fuerte vínculo con la protección contra el espionaje económico y la seguridad corporativa.

Alemania mantiene un modelo de IE que asocia la *Wirtschaftsschutz* (protección económica) y la *Industrieschutz* (protección industrial) a la contrainteligencia empresarial y la seguridad industrial. El *Bundesamt für Verfassungsschutz* (BfV)[13] ha señalado en varios informes la relevancia de la inteligencia económica para la protección frente al espionaje industrial y tecnológico.

China ha desarrollado un modelo de inteligencia estratégica con un fuerte componente estatal, donde la IE forma parte de su expansión global y del control de sectores críticos. El concepto de «guerra económica» está explícitamente presente, con un uso instrumental del espionaje tecnológico y comercial.

En la práctica empresarial anglosajona, se distinguen dos planos, la inteligencia competitiva, (*Competitive Intelligence*, CI), definida como el proceso ético y sistemático de recogida y análisis sobre competidores, mercados y entorno para reducir el riesgo estratégico y anticipar actuaciones, apoyando las decisiones de la máxima dirección, y la inteligencia de negocios (*Business Intelligence*, BI), entendida como el conjunto de tecnologías y aplicaciones para explotar datos internos de la corporación (operativos/financieros/comerciales), así como producir cuadros de mando con informes analíticos relevantes para la toma de decisiones táctico-operativas[14].

Finalmente, es importante distinguir la IE, y sus variantes mencionadas, de conceptos como *Big Data* y la analítica de datos. *Big Data* alude al conjunto de tecnologías y metodologías capaces de extraer, almacenar y procesar volúmenes masivos de datos, a gran velocidad y con gran variedad de formatos, para extraer

[13] Oficina Federal para la protección de la Constitución.

[14] De esta forma, la inteligencia de negocios explota, principalmente, datos generados por la actividad interna (ventas, clientes, procesos, etc.), aplicando técnicas de minería de datos, análisis estadístico y visualización para obtener conocimientos accionables sobre el desempeño y las eficiencias o ineficiencias de la organización. A diferencia de la inteligencia competitiva, que mira al entorno externo, la BI mira hacia adentro, aunque ambas confluyen en proporcionar información de calidad para la estrategia empresarial. De hecho, suele englobarse a veces todo este espectro bajo el término amplio de inteligencia empresarial, entendiéndola como la inteligencia orientada a la toma de decisiones en la empresa en todos sus niveles (estratégico, táctico y operativo).

de ellos información útil. Sin embargo, el *Big Data* por sí mismo opera fundamentalmente en el plano de los datos e información, por lo que no supone de forma automática la generación de inteligencia en sentido estricto.

En relación con todo lo anterior, se infiere que la IE pública integra vigilancia, protección e influencia para salvaguardar los intereses nacionales y apoyar políticas; la IE empresarial converge con CI+BI para sostener la ventaja competitiva, mientras que el *Big Data* aporta capacidad.

Con base en ello, en este trabajo se entenderá por IE el producto dimanante de un proceso sistemático y legal de recolección, análisis, elaboración, protección y difusión de conocimiento accionable sobre factores, actores y dinámicas económicas (internas y externas) que afectan a la seguridad, a los intereses económicos legítimos (nacionales, sectoriales o corporativos), con participación público-privada, orientado a la toma de decisiones en tres niveles (estratégico, operativo y táctico).

En este sentido, la ESN-2021 incorpora un enfoque anticipatorio y de alerta temprana basado en el análisis de hechos y de datos objetivos, plenamente coherente con una IE de orientación pública que apoya la seguridad económica y la gestión de riesgos interdependientes[15].

En el ámbito de la Unión Europea, el EU SOCTA 2025 constituye la evaluación *intelligence-driven* de las amenazas de delincuencia grave y organizada con repercusión económica y sistémica. Sus conclusiones sirven de base para la definición de las prioridades del ciclo político-operativo de la Plataforma Multidisciplinar Europea contra las Amenazas Criminales (EMPACT) 2026-2029, aprobadas por el Consejo.

2.2 Actores que conforman el sistema económico

Con el fin de profundizar en la incidencia de lo económico, y, en consecuencia, la incidencia de la IE en la seguridad se considera necesario identificar los principales actores económicos y como interactúan entre ellos.

[15] En este mismo sentido, la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (ENCODG) 2025 (aprobada por el CSN y publicada por Orden PJC/846/2025), estrategia de segundo nivel, refuerza el eje de inteligencia como prevención, anticipación y neutralización de la economía del crimen, es decir, una IE pública aplicada a riesgos económico-criminales.

Este conocimiento posibilitará la detección de entidades generadoras de datos o información económico-financiera, a partir de los cuales se posibilita la elaboración de inteligencia económica y, en este marco, la identificación de nuevos ámbitos de aplicación de esa inteligencia en la lucha contra el crimen organizado y grave.

Por todo ello, se procederá a realizar una definición de los actores desde una perspectiva global, para después exponer otro listado asociado al ámbito nacional. Pues, según lo ya expuesto, lo internacional incide de manera significativa en lo local.

Desde una perspectiva global, los principales actores estarían incluidos en la siguiente categorización:

- Estados nacionales: establecen sus propias políticas económicas y de seguridad, con el fin de proteger sus intereses. Fundamentalmente, interactúan a través de acuerdos bilaterales o multilaterales, así como aplicando medidas proteccionistas de manera unilateral.
- Organizaciones supranacionales: la más representativa es la Unión Europea, aunque existen otras con un menor grado de integración supranacional o institucionalización, de este modo, se pueden incluir Mercado Común del Sur (MERCOSUR), Asociación de Naciones del Sudeste Asiático (ASEAN), UA o el tratado entre México, EE. UU. y Canadá (USMCA/T-MEC), todas ellas con un marcado carácter económico.

Estas organizaciones actúan de manera multidimensional y de forma asimétrica, llevando a cabo funciones de representación ante determinados organismos, facilitando el comercio y la inversión (tanto privada como pública), así como, posicionándose estratégicamente en los continuos reequilibrios del orden mundial. Todo ello, lo realizan de manera integrada con otros niveles de gobernanza y con los diversos tipos de actores.

- Organizaciones internacionales: estas instituciones, como el FMI, la ONU, el Banco Mundial (BM) o la OMC, facilitan la cooperación y el entendimiento en distintos ámbitos, fundamentalmente en el económico, posibilitando la resolución de conflictos en el marco de regulaciones aceptadas por los diferentes intervinientes, financiando o subvencionando, incluso, distintas iniciativas de desarrollo social y económico.
- Corporaciones multinacionales: actualmente, constituyen el motor comercial y de inversión del sistema económico global, lo que se proyecta en una gran influencia en dicho sistema.

- Foros de gobernanza informal o clubes de poder internacionales: en este nivel, se deben destacar el G-20, G-8, G-77 o los denominados BRICS: Brasil, Rusia, India, China, Sudáfrica. Aunque son estructuras no institucionalizadas, poseen una gran capacidad de influencia en el sistema económico global[16].
- *Think Tanks* y universidades: su actividad principal es la generación de conocimiento, pudiendo realizar análisis prospectivos y, consecuentemente, influir en las políticas estratégicas y, entre ellas, las económicas. Igualmente, interactúan con los estados y las corporaciones mediante informes estratégicos, asesorías o formación especializada.
- Actores no estatales: en esta categoría se sitúan las organizaciones no gubernamentales (ONG), sindicatos, los diversos grupos de interés y todos aquellos dimanantes de una sociedad civil organizada. De este modo, estos grupos ejercen su influencia sobre la gobernanza económica global mediante la presión social, incidencia en la Administración Pública y demandas de responsabilidad estatales y corporativas.

Este conjunto de actores, los intereses de estos y la actividad que desarrollan para alcanzarlos, configuran una arquitectura económica mundial extremadamente compleja, densa y, en cierta medida, estructurada. En este marco, se genera un orden económico híbrido, donde lo informal coexiste con lo formal, lo que amplía el rango de escenarios futuros posibles.

Si se centra el foco en España, los principales actores son los siguientes:

- Administración Pública.
- Organizaciones internacionales y supranacionales.
- Grandes empresas y pequeñas y medianas empresas (pymes).
- *Think Tanks*, universidades y centros tecnológicos.
- Actores no estatales y sociedad civil organizada.

[16] En este sentido, actúan como espacios de concertación política, derivando en una coordinación macroeconómica y en el establecimiento de agendas estratégicas de los distintos actores. Complementan a las organizaciones formales, maximizando su estructura no institucional e intergubernamental para conseguir un entendimiento político en escenarios complejos, adoptando decisiones rápidas y flexibles.

2.2.1 Administración Pública

Las administraciones públicas españolas se configuran, básicamente, en tres niveles: estatal (Administración General del Estado), autonómico (comunidades autónomas)[17] y local/municipal (ayuntamientos)[18].

El nivel estatal es el que aglutina las competencias más críticas, ostentando atribuciones exclusivas en fiscalidad (salvo excepciones), comercio exterior, seguridad económica, política monetaria (delegada en el BCE) y regulación financiera.

En base a ellas, articula la seguridad económica en seis ejes: la gestión de los sectores estratégicos a través de la Sociedad Estatal de Participaciones Industriales (SEPI), el control de la inversión extranjera directa (IED/FDI) en sectores sensibles, la supervisión financiera (BdE, CNMV, Tesoro) integrada en el marco europeo, la prevención de prácticas de blanqueo de capitales y financiación del terrorismo (PBC/FT) con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) como Unidad de Inteligencia Financiera (UIF) nacional, la gestión de la ciberseguridad y el aseguramiento de las infraestructuras críticas (Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), Centro Criptológico Nacional – Computer Emergency Response Team (CCN-CERT), Instituto Nacional de Ciberseguridad (INCIBE) y Oficina de Coordinación de Ciberseguridad (OCC)) y la regulación de los mercados estratégicos (CNMC y ministerios competentes).

El nivel autonómico también ejerce funciones económicas relevantes en un modelo multinivel y asimétrico [régimen común, foral y Régimen Económico y Fiscal (REF)], gestiona fondos UE y promueve el desarrollo mediante agencias y clústeres público-privados.

---

17 También, se considera un nivel intermedio, entre el autonómico y el local, constituido por las diputaciones provinciales (en los territorios de régimen común), los cabildos insulares, uno por isla en Canarias, los consells insulars, uno por isla mayor (Mallorca, Menorca e Ibiza) en Islas Baleares y las diputaciones forales del País Vasco, una por provincia. En Navarra, y en el resto de las comunidades uniprovinciales, no existen diputaciones, asumiendo sus funciones la comunidad foral o la comunidad del régimen común, respectivamente.
Las estructuras intermedias (diputaciones, cabildos, consells) coordinan y canalizan inversiones, mientras que las diputaciones forales disponen de una amplia autonomía tributaria y capacidad de política económica.

18 En las ciudades autónomas, Ceuta y Melilla, el ayuntamiento y el órgano autonómico están fusionados en una única institución: la ciudad autónoma.

Asimismo, el nivel local aporta fiscalidad propia, urbanismo y promoción económica, con un impacto significativo por número de municipios y el peso de grandes ciudades.

Todo ello refleja un panorama de la gestión económica multinivel que conjunta la complementariedad y una complejidad vinculada a una correspondencia asimétrica de competencias.

Los distintos niveles, en el marco económico, financiero y fiscal, se coordinan y cooperan a través de distintos órganos y procedimientos formales, en virtud de lo dispuesto en el artículo 103.1 de la Constitución española (CE) y los artículos 2.1.b y 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Así, el nivel estatal se relaciona con el autonómico, fundamentalmente, a través del Consejo de Política Fiscal y Financiera (CPFF)[19], conferencias sectoriales[20] y las Comisiones bilaterales Estado-CCAA[21].

2.2.2 Organizaciones internacionales y supranacionales

Las organizaciones que se podrían incluir en este apartado alcanzan un número muy elevado, precisamente por la enorme interacción mundial que ya se ha descrito entre los distintos actores intervinientes. En este sentido, se ha considerado que, para este estudio, lo adecuado es centrarse en la que mantiene una mayor influencia en el sistema económico español, la UE.

Se debe tener en cuenta que la CE prevé la cesión de competencias mediante ley orgánica en su artículo 93, así como la incorporación de tratados al derecho interno, según lo dispuesto en el artículo 96.

Según el artículo 2 del Tratado de Funcionamiento de la UE (TFUE), existen competencias exclusivas de la UE, recogidas en el artículo 3, competencias compartidas con los Estados miembros, artículo 4, y competencias de apoyo, artículo 6 del tratado.

Entre las competencias exclusivas se encuentran la unión aduanera, el establecimiento de las normas sobre competencia, la política monetaria (en los países de la zona euro) y la política

19 Órgano colegiado previsto en la Ley Orgánica 8/1980, de financiación de las CC. AA.

20 Previstas en el artículo 147 de la Ley 40/2015.

21 Dispuestas para las CC. AA. con estatutos reforzados o régimen especial (Cataluña, País Vasco, Navarra, Canarias).

comercial común. Respecto a las compartidas se pueden destacar el mercado interior, cohesión económica, redes transeuropeas, energía, medio ambiente y consumidores[22].

Resulta evidente, por tanto, que esta cesión competencial, total o parcial, condiciona la seguridad económica de España a la UE.

En el marco de la seguridad económica, la UE ejerce el cribado de inversiones extranjeras directas (FDI *screening*), Mecanismo Único de Supervisión (MUS), Mecanismo Único de Resolución (MUR) y el Sistema Europeo de Supervisión Financiera (SESF), regulado principalmente por el Reglamento (UE) n.º 1092/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010.

La UE, además, posee instrumentos para proteger el mercado europeo como medidas *antidumping*, y antisubvenciones, el Reglamento de obstáculos al comercio y las medidas de salvaguardia[23].

2.2.3 Grandes empresas[24] y pymes

Las grandes corporaciones españolas, muchas agrupadas en el IBEX-35, son actores decisivos tanto por su capacidad de inversión, como por su influencia en la política económica y su papel como tractores del ecosistema empresarial.

Según la Asociación Valenciana de Empresarios (AVE), la aportación al Producto Interior Bruto (PIB) del conjunto de las empresas españolas fue en 2024 del 86,8 % del total[25]. De igual forma, la Dirección General de Apoyo a la Pequeña y Mediana Empresa

---

22 EUR-Lex, Reparto de competencias en la Unión Europea. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/division-of-competences-within-the-european-union.html?utm_source [Consulta: 8 agosto 2025].

23 EUR-Lex, Política comercial UE. Disponible en: https://eur-lex.europa.eu/ES/legal-content/glossary/eu-trade-policy.html?utm_ [Consulta: 8 agosto 2025].

24 La Recomendación 2003/361/CE de la Comisión Europea clasifica como gran empresa a aquella que supera doscientos cincuenta empleados y presenta un volumen de negocios anual superior a cincuenta millones de euros o un balance general anual superior a 43 millones de euros.

Las corporaciones multinacionales (CMN) se definen doctrinalmente como aquellas entidades que poseen o controlan activos productivos en más de un país, operando bajo una estructura corporativa integrada, pero con filiales que actúan conforme a los marcos regulatorios propios de los territorios donde están ubicadas. UNCTAD (2023). World Investment Report 2023: Investing in Sustainable Energy for All. United Nations Conference on Trade and Development. Disponible en: https://unctad.org/wir [Consulta: 8 agosto 2025].

25 Asociación Valenciana de Empresarios (AVE), Barómetro del empresario, 2025. Disponible en: https://barometrodelempresario.es/ediciones/ [Consulta: 8 agosto 2025].

(DGEIPYME) indica que el valor añadido bruto (VAB)[26] de las grandes empresas en España era del 37,8 %, mientras que el de las pymes, incluido autónomos, es del 62,2 %, sin incluir a las financieras, según lo dispuesto en el informe emitido por la DGEIPYME «Marco Estratégico en Política de Pyme 2030», de 2019.

En el contexto español, las grandes empresas y corporaciones multinacionales (CMN) desempeñan un papel determinante en el producto interior bruto, el empleo y la balanza comercial, concentrando un volumen significativo de facturación y exportaciones[27] pese a representar un porcentaje reducido del total de sociedades registradas. En este sentido, constituyen un 55,6 % del volumen de las exportaciones[28].

A su vez, de acuerdo con la estadística de empresas según pertenencia a grupos elaborado por el Instituto Nacional de Estadística (INE), en 2022 se contabilizaron 5514 empresas residentes en España integradas en grupos multinacionales de matriz española (empresas controladoras con filiales en el extranjero) y 14 209 empresas pertenecientes a multinacionales extranjeras[29].

Las pymes representan el 99 % de las empresas existentes en España según la DGEIPYME, atendiendo a las referencias mostradas en párrafos anteriores. Paralelamente, mantienen más o menos el 66 % del empleo empresarial total.

Además, las pymes coadyuvan a la cohesión territorial, fijando población en territorios y reduciendo los desequilibrios regionales, a la diversificación productiva, favoreciendo la resiliencia económica frente a potenciales crisis, aplicando la innovación en proyectos con universidades y centros tecnológicos y aportan valor añadido al insertarse en las cadenas de suministros como proveedores especializados.

---

[26] Índice íntimamente ligado al PIB, según lo descrito por el Instituto Galego de Estadística: Definiciones. Economía. Disponible en: https://www.ige.gal/igebdt/esq.jsp?c=0307&idioma=es&ruta=definiciones/defcod.jsp?C=03070000 [Consulta: 8 agosto 2025].

[27] Subdirección General de Estudios y Prospección: El sector exterior en 2023. Disponible en: https://www.revistasice.com/index.php/SICE/article/view/7757 [Consulta: 8 agosto 2025].

[28] Ministerio de Economía, Comercio y Empresa: Informe de Evaluación a medio camino de la Estrategia de Internacionalización de la Economía Española 2017-2027. Disponible en: https://comercio.gob.es/es-es/estrategia_internacionalizacion/Documents/20231222-Evaluacion-EIEE-2017-27.pdf [Consulta: 9 agosto 2025].

[29] INE: Estadística de Empresas según Pertenencia a Grupos. Año 2022. Disponible en: https://ine.es/dyngs/Prensa/EEPG2022.htm. [Consulta: 8 agosto 2025].

Por otro lado, las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación, reguladas por la Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación, actúan como agentes institucionales clave en el fortalecimiento de las pymes, favoreciendo la internacionalización, procurando la formación y la digitalización, apoyando la financiación y el emprendimiento, y elaborando inteligencia económica local, mediante la recopilación y la difusión de información sectorial y de mercado útil para la toma de decisiones empresariales, todo ello, en base a sus propias competencias.

2.2.4 Think tanks, universidades y centros tecnológicos

En el marco del sistema económico español, los *think tanks*, universidades y centros tecnológicos constituyen nodos esenciales para la generación, transferencia y aplicación de conocimiento, tanto en el plano nacional como internacional. Su actividad incide de forma directa en la competitividad, la innovación, en la toma de decisiones y la resiliencia del tejido productivo, y, de manera indirecta, en la seguridad económica del Estado.

- Think tanks

  En el contexto español, los *think tanks* actúan como plataformas de análisis e investigación que elaboran estudios prospectivos, informes de estados de situaciones concretas y propuestas de política pública.

  Según la clasificación del *Think Tanks and Civil Societies Program* de la Universidad de Pensilvania (2020)[30], España se sitúa en el puesto 17 mundial, por número de *think tanks*, reconociendo la relevancia internacional por parte del Real Instituto Elcano del Barcelona Centre for International Affairs (CIDOB) o la Fundación de Estudios de Economía Aplicada (FEDEA), que proporcionan análisis estratégicos en ámbitos como la geoeconomía, la política exterior o la economía industrial, entre otros.

- En el ámbito económico, su valor reside en la capacidad de generar IE y transferirla a las administraciones públicas, empresas y sociedad civil, contribuyendo a la formulación de políticas y a la anticipación de riesgos. Actuando, de este modo,

[30] The Lauder Institute, University of Pennsylvania: 2020 Global Go To Think Tank Index Report. Disponible en: https://repository.upenn.edu/bitstreams/8fa7709a-310d-43b2-bee6-94c49db23e41/download [Consulta: 10 de agosto 2025].

como puente entre el ámbito académico y la toma de decisiones políticas (McGann, 2020).

– Universidades

Según el Ministerio de Ciencias, Innovación y Universidades el impacto económico de las universidades públicas españolas en la economía se cifra en el 2,2 % del PIB[31]. Pero su aportación va mucho más allá.

Las universidades, públicas y privadas, desarrollan un papel estructural en la formación de capital humano altamente cualificado, en la investigación aplicada y en la cooperación universidad-empresa[32].

En el plano económico, los programas de transferencia tecnológica y de innovación abierta permiten a las universidades conectar con pymes y grandes empresas para impulsar la I+D+i, en coordinación con el sistema estatal de ciencia, tecnología e innovación regulado por la Ley 14/2011, de 1 de julio, de la Ciencia, la Tecnología y la Innovación.

Estos centros además generan IE a través de su actividad investigadora, formando también expertos en esta temática a través de formación especializada.

– Centros tecnológicos

Los centros tecnológicos españoles, agrupados en redes como Federación Española de Centros Tecnológicos (FEDIT) o Tecnalia en el País Vasco, constituyen entidades de apoyo a la innovación empresarial, proporcionando capacidades de investigación aplicada, desarrollo experimental y validación industrial.

Según el Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2027, estos centros son instrumentos clave para cumplir los objetivos de digitalización, transición

[31] Ministerio de Ciencias, Innovación y Universidades: Estudio de impacto económico de las universidades públicas españolas. Análisis territorializado para el año 202. Disponible en: https://www.ciencia.gob.es/Noticias/2023/junio/Las-universidades-publicas-espanolas-multiplican-por-5--cada-euro-invertido-en-ellas.html#:~:text=Las%20universidades%20p%C3%BAblicas%20espa%C3%B1olas%20multiplican%20por%205,la%20actividad%20de%20las%20universidades%20p%C3%BAblicas%20espa%C3%B1olas [Consulta: 10 agosto 2025].

[32] La Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (LOSU) establece, en su artículo 3, que la misión de las universidades incluye la transferencia, difusión y valorización del conocimiento para el desarrollo social y económico.

energética y fortalecimiento de la autonomía estratégica industrial. Su financiación combina aportaciones públicas (nacionales y europeas) y servicios de I+D+I contratados por empresas.

Desde una perspectiva de IE, estos actores contribuyen a detectar y analizar tendencias globales con capacidad de impactar en la economía española, transferir conocimiento y tecnología para fortalecer los distintos sectores estratégicos, aumentando la independencia tecnológica y sirviendo de enlace eficaz entre el sector público y privado.

2.2.5 Actores no estatales y sociedad civil organizada

Sindicatos, organizaciones empresariales como la Confederación Española de Organizaciones Empresariales (CEOE) y la Confederación Española de la Pequeña y Mediana Empresa (CEPYME), ONG sectoriales y asociaciones ambientales tienen una influencia creciente en la deliberación de políticas públicas.

Interactúan con el Estado mediante el diálogo social y con las empresas a través de la negociación colectiva y programas de responsabilidad social corporativa (RSC)[33].

Un ejemplo de participación en las políticas económicas de sindicatos, organizaciones empresariales y Administración es el Consejo Económico y Social, según lo dispuesto en la Ley 21/1991, de 17 de junio, por la que se crea el Consejo Económico y Social.

2.3 Generación de inteligencia económica por los distintos actores

De todo lo expuesto en el apartado anterior, se puede observar que la realidad del sistema económico español se vincula, de manera especial, a una estructura multinivel de gobernanza asimétrica que deriva en una red compleja de competencias. Estas competencias determinan la capacidad de acción de cada nivel.

Los distintos niveles interactúan, además, con los diferentes actores privados y no estatales, dependiendo de los intereses y competencias de cada uno de ellos.

[33] Observatorio de Responsabilidad Social Corporativa. Disponible en: https://observatoriorsc.org/ [Consulta: 10 agosto 2025].

Todo este sistema se complica al enmarcarlo, y en gran medida supeditarlo, al ámbito internacional. En este sentido, la cesión de soberanía a la UE, en materia económica, influye decisivamente en el sistema económico español, más aún si se atiende a la financiación de proyectos y concesión de subvenciones provenientes de la UE.

Esta influencia europea se intensifica al incorporar el hecho de que la UE es la zona prioritaria de las exportaciones e importaciones españolas, con un 61,8 % y 48,9 %, respectivamente[34], lo que evidencia que cualquier estrategia de seguridad económica debe estar alineada con la que desarrolle la UE.

También se aprecia, de la descripción de los diferentes actores, que, aunque existe una interacción entre todos los niveles (incluyendo el internacional), la coordinación y la cooperación del conjunto se vehiculiza, de manera referencial, a través de la Administración central. Este hecho es relevante para establecer fórmulas eficientes en la aplicación práctica del conocimiento, especialmente en el ámbito de la IE.

Una vez que se han definido los distintos actores se requiere conocer si generan IE o si su actividad posibilitase la generación de esta.

En primer lugar, en el marco internacional, se analizará la UE por resultar el ente supranacional con mayor incidencia en el sistema económico español.

2.3.1 Inteligencia económica en el marco de la UE

El ecosistema UE de inteligencia, y la económica en particular, se articula en torno a varias agencias u organismos propios.

Así el Centro de Inteligencia y situación de la UE (EU INTCEN) (parte civil de la SIAC), produce evaluaciones *all-source*[35] y comparte su análisis con la Comisión, las demás agencias europeas y con los Estados miembros.

[34] Informe Mensual de Comercio Exterior junio 2025. Ministerio de Industria, Comercio y Turismo. Disponible en: https://comercio.gob.es/ImportacionExportacion/Informes_Estadisticas/Historico_Informes/Mensuales/2025/2025-06_Informe_Mensual_Comercio_Exterior.pdf [Consulta: 11 agosto 2025].

[35] Producto de inteligencia resultante de la fusión y validación de información procedente de todas las disciplinas y canales disponibles, con el fin de reducir incertidumbre y orientar decisiones.

La Oficina Europea de Lucha contra el Fraude (OLAF) investiga administrativamente el fraude y la corrupción que afectan a los intereses financieros de la UE, generando inteligencia estratégica y operativa mediante distintos informes periódicos o información concreta con la que nutre causas judiciales y de manera referencial al European Public Prosecutor's Office (EPPO).

En el marco de la lucha contra falsificación/piratería, la oficina de Propiedad Intelectual de la Unión Europea (EUIPO)-Observatorio constituye una referencia internacional con el desarrollo de estudios y buenas prácticas.

Por otro lado, EUROPOL, que cuenta con un departamento específico dedicado al ámbito económico, el Centro Europeo de Delincuencia Financiera y Económica (EFECC), brinda apoyo operativo-analítico en delincuencia financiera/económica, incluyendo la trazabilidad de bienes ilícitos y su decomiso, coordinando la Asociación Público-Privada de Inteligencia Financiera de EUROPOL EFIPPP[36].

La generación de IE que realiza la UE, a través del sistema económico y de seguridad, evidencia una estructura cohesionada en aras de preservar una de las mayores fortalezas de la UE, su poder económico (Damro, 2012). Esta fortaleza le permite una significativa influencia en la gobernanza mundial (Bradford, 2015), en concordancia con los objetivos de la IE.

Por ello, la UE considera esencial mantener una seguridad económica eficaz, en un mundo cada vez más tensionado con una afectación significativa a las relaciones económicas, como ya se ha expuesto. Muestra de este compromiso se evidencia en la adopción de la «Estrategia europea de seguridad económica», de 20 de junio de 2023.

De esta manera, la IE es fundamental para la toma de decisiones que garantice la pretendida seguridad económica, en un ámbito internacional donde los elementos económicos pueden ser utilizados como instrumentos de presión, coerción o para acumular poder (Farrell y Newman, 2019).

También se observa como estos productos de inteligencia son empleados en la lucha contra actividades ilegales, tanto desde una perspectiva administrativa como penal. Configurándose la

[36] Es una red creada en 2017 para compartir información y coordinarse entre Europol, autoridades competentes (FIU, policía/investigación) y entidades financieras frente al blanqueo y el crimen financiero/económico. Su secretaría está en el EFECC (Europol).

cooperación entre los Estados miembros, las propias instituciones de la EU, las empresas e, incluso, países terceros, como un elemento determinante para la utilización eficiente de la referida inteligencia. En tal sentido, la UE ha normalizado los mecanismos de cooperación.

2.3.2 Generación de inteligencia económica en el marco español

La producción de inteligencia no deriva de una única entidad, sino de una comunidad. Esta comunidad de inteligencia puede conceptualizarse como una federación funcional de organismos ejecutivos que, aunque cooperan y a veces integran esfuerzos, sirven a decisores distintos y operan bajo líneas de autoridad diferentes. Este entramado se va configurando a través de un proceso transformacional, no derivado de un diseño previo, y que combina especialización y coordinación para producir inteligencia al servicio de la decisión política (Lowenthal, 2012).

En el ámbito español, la comunidad de inteligencia española se correspondería con un sistema compuesto por los servicios de inteligencia e información del Estado y por los distintos órganos de coordinación, orientado a evitar la dispersión de esfuerzos y a garantizar eficiencia y eficacia en la generación e intercambio de inteligencia para la decisión política en el contexto de la seguridad nacional, entendiendo el término seguridad en una acepción amplía (Rosales Pardo, 2005).

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, recoge la existencia de una comunidad de inteligencia, mediante su artículo 6 «La Comisión Delegada del Gobierno para Asuntos de Inteligencia velará por la adecuada coordinación de todos los servicios de información e inteligencia del Estado para la formación de una comunidad de inteligencia».

Se le encomienda, por tanto, a esta comisión delegada la coordinación de los diferentes actores de inteligencia e información, integrantes de la comunidad. Así como, proponer al presidente del Gobierno los objetivos anuales para el CNI, que se materializarán en la Directiva de inteligencia, de frecuencia anual y de carácter secreto.

Sin embargo, la comunidad de inteligencia en España no está definida. En virtud de lo dispuesto en el artículo 6.1 y 6. 4c) de la Ley 11/2002, de 6 de mayo y del artículo 4 del Real Decreto 1/2024, de 9 de enero, la comunidad se constreñiría a

la Administración civil y militar, de la Administración General del Estado:

- CNI.
- Centro de Inteligencia de las FAS (CIFAS).
- Servicios de información de Interior:
    - Comisaría General de Información (Policía Nacional).
    - Jefatura de Información (Guardia Civil).
- Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO).
- Centro Criptológico Nacional (CCN).
- INCIBE.
- SEPBLAC.
- AEAT:
    - Servicio de Vigilancia Aduanera (SVA).
    - Oficina Nacional de Investigación del Fraude (ONIF).
    - Oficina Nacional de Investigación de Aduanas e Impuestos Especiales (ONI).

Sin embargo, en el presente estudio se adopta una conceptualización ampliada de la comunidad de inteligencia, sustentada en un enfoque sistémico, holístico e integrado, que incluye no solo a las administraciones con competencias tradicionales en seguridad y defensa, sino también a otras administraciones públicas, a la sociedad civil organizada y al sector empresarial (Arcos y Antón, 2010).

En sintonía con lo expuesto, la generación de IE en España comprende un ecosistema amplio de actores públicos, privados y sociales, enmarcado por estrategias nacionales y normativas específicas.

Siguiendo un enfoque similar al de la UE, España ha ido reconociendo la IE como herramienta clave para la seguridad nacional y la competitividad (Díaz Matey, 2016). De hecho, la ESN 2021 identifica la seguridad económica como un pilar esencial, destacando en los Informes Anuales de Seguridad Nacional (IASN) que los riesgos económicos (inestabilidad financiera, fraude, blanqueo, etc.) socaban el bienestar y la confianza en las instituciones.

Consecuentemente, resulta esencial impulsar iniciativas para dotar al país de estructuras y mecanismos de IE que permitan anticipar riesgos y aprovechar oportunidades en un entorno global competitivo (Davara Rodríguez, 2015).

3 La delincuencia organizada y grave y su afectación a los intereses económicos

Como se ha ido poniendo de manifiesto a lo largo de este documento, la estrecha relación económica entre la UE y España, sumado al hecho de ser un Estado miembro de este organismo supranacional, ocasiona que las políticas económicas de la UE influyan notablemente en las españolas. Esta circunstancia, determina que la seguridad económica, en concordancia con los postulados de la UE, se configure como una pieza fundamental en la seguridad nacional.

En este sentido, ambas estrategias coinciden en identificar al crimen organizado y grave como una de las amenazas que pone en riesgo al sistema económico. En este escenario, conviene determinar qué ámbitos delictivos tienen la capacidad de menoscabar en mayor medida el sistema económico descrito.

Los Informes SOCTA de Europol (2021, 2025) confirman que la delincuencia organizada en Europa se configura de forma policéntrica, generando un sistema en el que se distribuyen numerosas redes y actores que interactúan entre sí, en el marco de los distintos mercados criminales.

Por otro lado, se ha determinado que más del 80 % de las redes criminales activas en la UE utilizan estructuras empresariales legales en sus operaciones (SOCTA, 2025), lo que pone de relieve una penetración sistemática en sectores regulados e infraestructuras críticas, como puertos y plataformas logísticas.

De este modo, el Informe sobre delincuencia financiera y económica de EUROPOL (2023) subraya que los sistemas financieros europeos y los profesionales facilitadores se encuentran en el corazón de la economía criminal.

Estos facilitadores, frecuentemente, se erigen en conectores de varias redes criminales a través del denominado *crime as a service*, siendo contratados sus servicios por redes diferentes. A partir de este diagnóstico, el EFECC recomienda integrar la inteligencia financiera y criminal desde las fases iniciales de las

investigaciones, con el fin de impedir la entrada de fondos ilícitos en la economía formal y aumentar las posibilidades de recuperación de activos.

En síntesis, la UE ha institucionalizado un enfoque en el que la IE y financiera ocupa una posición central para identificar, anticipar y neutralizar las formas más lesivas de criminalidad organizada.

Con la Estrategia Española de Seguridad (EES-2011), España comenzó a integrar de forma expresa los riesgos económicos y financieros en su agenda de seguridad, incluyendo la fragilidad del sistema financiero, el fraude fiscal, la corrupción y el blanqueo de capitales, reconociendo, asimismo, la función de la inteligencia estratégica para prevenir y responder a estas amenazas.

De este modo, anunció la creación de un Sistema de Inteligencia Económica (SIE) para prevenir y detectar acciones contrarias a los intereses económicos, financieros, comerciales y tecnológicos en los distintos sectores estratégicos españoles, coadyuvando al fortalecimiento de la seguridad nacional. Igualmente, ponía en valor y reconocía la necesidad de potenciar la inteligencia relacionada con la lucha contra el crimen organizado.

Asimismo, evidencia la conexión entre la amenaza que supone la inseguridad económica y el crimen organizado, en virtud de lo cual, considera esencial una mayor intensidad en la investigación criminal económica y su enfoque en el blanqueo de capitales procedente del crimen organizado, desarrollando unidades especializadas.

En relación con el mantenimiento de la seguridad económica y el correcto funcionamiento del sistema económico, subraya la necesidad de generar inteligencia económica y de luchar contra el fraude fiscal, el blanqueo de capitales, la corrupción, los paraísos fiscales y los distintos tráficos ilícitos que ponen en peligro la estabilidad económica y la financiación de las instituciones. En este sentido, destaca la importancia de la inteligencia estratégica para luchar contra el crimen organizado.

La ESN 2021 resalta que el fin económico del crimen organizado y la delincuencia grave socaban la seguridad nacional, utilizando estructuras legales y criptomonedas para opacar sus negocios ilícitos, resultando especialmente desestabilizador el contrabando, el cibercrimen, el tráfico de drogas, de armas y de especies silvestres y la corrupción.

Concretamente, ponen en riesgo la seguridad económica «el fraude, la evasión fiscal, la corrupción, el blanqueo de capitales y el uso indebido de los fondos procedentes de subvenciones y contratos públicos», generando, además, desafección social a las instituciones gubernamentales.

De esta forma, explicita los riesgos económicos sistémicos, reseñando la necesidad de la cooperación interinstitucional para gestionarlos eficazmente.

La ENCODG 2019-2023 pone de manifiesto la amenaza que supone el crimen organizado y la delincuencia grave para la seguridad nacional, desestabilizando y perturbando la economía nacional mediante el blanqueo de capitales, la creación de mercados paralelos o distorsionando determinados sectores productivos a través del ejercicio de la competencia desleal, utilizando inyecciones de capital provenientes de actividades ilícitas o eludiendo fraudulentamente cargas fiscales[37].

Entre sus ejes se encuentran la explotación de inteligencia económico-financiera, el impulso de investigaciones patrimoniales y la recuperación de activos.

La ENCODG 2025 profundiza en este modelo mediante el concepto de «anticipación operativa», es decir, el uso de análisis prospectivo, *Big Data* e IA para detectar, en fases tempranas, fenómenos de fraude, blanqueo y ciberamenazas financieras. Asimismo, prioriza la cooperación estructurada interinstitucional y público-privada.

Este deterioro del sistema económico[38], como apuntan los diferentes documentos estratégicos, se puede llevar a cabo de múltiples formas, a través de la infiltración en mercados legales (Savona y Riccardi, 2015), de la corrupción y de la extorsión minorizando la inversión (Blackburn *et al*., 2017), de la inyección de dinero sucio horadando la competencia (UNICRI, 2016) o generando burbujas especulativas, desviando capital de sectores productivos y aumentando la vulnerabilidad financiera.

[37] Esta estrategia también pone el foco en el fraude fiscal, en los delitos contra la propiedad intelectual e industrial, así como en la ciberdelincuencia aplicada a las finanzas.

[38] El referido informe Shadow Money de Europol (2021) estima que hasta 1,5 billones de euros perteneciente a ciudadanos europeos se sitúan ocultos en jurisdicciones offshore, es decir, depositados en territorios o centros financieros ubicados fuera del país de residencia, caracterizados por una fiscalidad reducida y por elevados niveles de opacidad.

Según el informe «VAT gap in the EU: 2024 report»[39] (European Commission, CASE *et al*., 2024), en 2022, la diferencia entre los ingresos teóricos de IVA y la recaudación efectiva fue del 7 % en la UE (89,3 mil millones de euros). Mientras que, en España, se dejaron de recaudar 4443 millones de euros (4,6 %). Destacando, asimismo, que el fraude del impuesto es el motor de esta diferencia.

Por otro lado, el Consejo de la UE publicó, en 2023, que se han detectado en el sistema financiero de la UE actividades y transacciones sospechosas por una horquilla de 117 000 y 210 000 millones de euros, así como 1500 millones de euros en movimientos de criptomonedas en los mercados de la web oscura. En este marco, determina que el 70 % de las redes delictivas activas en la UE emplea alguna forma de blanqueo de capitales para financiar sus operaciones y ocultar sus activos[40].

3.1 Ámbitos delictivos con mayor incidencia económica

Poniendo en común las distintas estrategias referidas, las entidades y organismos generadores de información e IE y la descripción del sistema económico, junto con el referido impacto que la delincuencia organizada y grave realiza en los intereses económicos de la UE y de España, se desprende una serie de ámbitos delictivos asociados a una mayor incidencia negativa en la seguridad económica.

La convergencia de las estrategias española y europea identifica, con notable consistencia temporal, un núcleo de criminalidad de alto impacto económico compuesto por:

1. Blanqueo de capitales.
2. Fraude Fiscal.
3. Cibercriminalidad económica.
4. Economía derivada del tráfico de drogas.

---

[39] El *VAT compliance gap* es la diferencia entre la *VAT Total Tax Liability* (VTTL) (la obligación teórica de IVA calculada con el método «top-down») y los ingresos efectivos de IVA registrados en contabilidad nacional (base devengo). Es decir, mide lo que no se recauda por incumplimiento, fraude, etc.

[40] Consejo de la UE. Análisis. ¿Qué es el blanqueo de capitales? Disponible en: https://www.consilium.europa.eu/es/infographics/anti-money-laundering/#:~:text=El%20blanqueo%20de%20capitales%20en,la%20econom%C3%ADa%20de%20la%20UE . [Consulta: 26 agosto 2025].

5 Delitos contra el mercado y la propiedad intelectual/ industrial.

6 Criminalidad medioambiental.

7 Trata de seres humanos.

Esta priorización emerge de la serie EU-SOCTA de EUROPOL (2013, 2017, 2021 y 2025) estando alineadas con las ESN (2011, 2013, 2017 y 2021) y con las ENCO (2019 y 2025).

Este núcleo representa la perspectiva económica de las prioridades[41] definidas en el EMPACT 2026-2029[42].

En la determinación de estas prioridades por el Consejo de la UE, se ha tenido en cuenta la creciente desestabilización que provoca en la sociedad la delincuencia organizada y grave, haciendo uso, en numerosos casos, de la violencia o la corrupción, así como su rápida adaptación al empleo de la AI y a las nuevas tecnologías.

3.1.1 Blanqueo de capitales

Es el soporte de la delincuencia organizada y grave actual, a través de esta práctica delictiva oculta, recoloca, invierte y disfruta de los bienes ilícitos conseguidos. Por ello, se erige en el objetivo principal para erradicar la criminalidad organizada y grave (EUROJUST, 2022), afectando a sus reservas y a su financiación (Balas Dávila, 2023).

Como ya se ha referido, el blanqueo de capitales desestabiliza y perturba la economía, creando un mercado paralelo que reduce la productividad, destruye la competencia e inhibe la actividad empresarial.

---

41 Identificar y desarticular las redes delictivas y las personas que representan una mayor amenaza.

Abordar los delitos que aumentan con mayor rapidez en el ámbito digital: ciberataques, explotación sexual de menores en línea y sistemas de fraude en línea;

Luchar contra el tráfico de drogas.

Luchar contra el tráfico ilícito de migrantes y la trata de seres humanos.

Luchar contra la delincuencia relacionada con armas de fuego y explosivos.

Desarticular redes implicadas en delitos contra el medio ambiente.

Luchar contra los delitos económicos y financieros, como el fraude del IVA y los delitos en materia de propiedad intelectual e industrial.

42 Conclusiones del Consejo sobre la mejora de la EMPACT y las prioridades de la UE en materia de lucha contra delincuencia para el próximo ciclo de la EMPACT 2026-2029, 13.6.2025. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9397-2025-INIT/en/pdf [Consulta: 26 agosto 2025].

En base a ello, la ENCODG 2019-2023 ya marcaba siete líneas de acción entre las que se encontraba la de potenciar la inteligencia económica-financiera, mejorando su producción y la colaboración interagencias[43]. Así como fomentar la colaboración público-privada y la elaboración de un plan estratégico de lucha contra el enriquecimiento ilícito de las organizaciones criminales y los delincuentes.

La UE, consciente del daño económico de esta modalidad delictiva[44] y con el fin de proteger su mayor fortaleza como potencia económica, ha sido muy prolija en iniciativas y generación de normativa que sirva, de manera eficiente, en la lucha contra el BC. En este sentido y como hito destacado de los últimos años, la UE aprobó en 2024 el paquete contra el blanqueo de capitales[45], en el que se incluye la creación de la Autoridad Europea contra el Blanqueo de Capitales (AMLA).

EUROPOL insiste en que convertir la inteligencia financiera en impacto operativo (embargos, decomisos, cierres de canales de blanqueo) es clave para vaciar de recursos a las redes criminales y proteger la economía legal.

El SEPBLAC, entre 2022 y 2023, ha recibido 13 800 comunicaciones, ha atendido 2.300 solicitudes de información, ha analizado 22 000 millones de euros asociadas a distintas operativas sospechosas y ha realizado más de 10 000 informes de inteligencia, los cuales han sido remitidos a los organismos pertinentes (SEPBLAC, 2024).

3.1.2 Fraude fiscal

El fraude fiscal y, en particular, el fraude al Impuesto sobre el IVA mediante el esquema de *Missing Trader Intra-Community*

[43] AEAT, Seguridad Social, Oficina de recuperación y gestión de activos (ORGA), entidades financieras, SEPBLAC, Registro de la propiedad, Registro Mercantil, Registro de bienes muebles e inmuebles, ayuntamientos, compañías de suministro, autoridades policiales, etc.

[44] Se debe tener en cuenta que el número de casos vinculados únicamente al blanqueo de capitales monitorizados por EUROJUST solo es superado por los que representan los delitos económicos (excluyendo el blanqueo de capitales) y el tráfico de drogas (EUROJUST, 2025).

[45] Consta de tres normas: Reglamento (UE) 2024/1620 (AMLA), Reglamento (UE) 2024/1624 (reglamento de libro único) y Directiva (UE) 2024/1640 (mecanismos nacionales).

(MTIC)[46] o procedimientos defraudatorios similares, representan, desde hace varias décadas, una de las amenazas económicas más graves para la UE y España, al constituir una fuente recurrente de pérdida de ingresos públicos y representar un mecanismo asociado a redes delictivas organizadas, lo cual multiplica su capacidad de daño[47].

Evaluaciones recientes (Europol, 2025) reafirman que la amenaza persiste y que las redes usan estructuras societarias complejas y cadenas logísticas para ocultar el flujo de bienes y facturación, cuantificando el impacto del fraude de IVA en varias decenas de miles de millones de euros anuales.

En este sentido, prácticas como el MTIC abaratan artificialmente el producto que ofrecen los operadores fraudulentos frente a los ofertados por las empresas cumplidoras, expulsando a estas del mercado, en un efecto cascada, propiciando ciclos de inversión de baja productividad al canalizar beneficios ilícitos hacia actividades pantalla (UNICRI, 2016).

El SEPBLAC destaca la importancia de las tramas de defraudación de IVA, asociadas a organizaciones criminales, exponiendo, como caso paradigmático, el sector de la distribución de hidrocarburos por su altos importes, su impacto recaudatorio y su capacidad de blanqueo (SEPBLAC, 2024), lo que suponen, igualmente, una afectación grave al mercado.

La EPPO reportó en su Informe Anual 2024 que mantenían 2666 investigaciones activas, principalmente vinculadas a la delincuencia organizada. El perjuicio a los intereses financieros de estas investigaciones se ha estimado en más de 24 800 millones de euros. En este marco, el fraude de IVA representaba el 53 %, unos 13 150 millones de euros, indicador de la relevancia de este fraude en la criminalidad económica que afecta al presupuesto de la UE y a los LEA (European Public Prosecutor's Office, 2025).

[46] El fraude asociado al MTIC consiste en que una empresa adquiere bienes intracomunitarios libres de IVA y los vende aplicando el impuesto al comprador, sin embargo, dicha sociedad desaparece sin ingresarlo en Hacienda, generando pérdidas millonarias. Todo ello se suele realizar a través de un esquema complejo de empresas y testaferros coordinados para evadir el impuesto y posicionar el producto en el mercado sin competencia al reducir costes.

[47] En este sentido, ya hace diez años se estimó que el fraude MTIC generaba pérdidas del orden de 29,3 mil millones de euros/año en la UE, subrayando su carácter sistémico y su capacidad para explotar asimetrías regulatorias y operativas entre Estados miembros (Savona y Riccardi, 2015).

En España, la ENCODG 2019-2023 determinaba que el fraude asociado al IVA suponía hasta un 18 % de la recaudación prevista, un dato sensiblemente diferente al que se ha expuesto anteriormente del 4,6 % estimado por UE. El contraste ilustra la diferencia entre estimaciones estratégicas y mediciones estadísticas armonizadas más recientes, pero coincide en el diagnóstico: el fraude del IVA supone un menoscabo sustancial y sostenido de ingresos públicos.

España participa activamente en EMPACT en el ámbito MTIC y ha reforzado su cooperación con EPPO/OLAF/EUROPOL, según el informe IASN 2023[48].

3.1.3 Cibercriminalidad económica

El SEPBLAC señala que una de las consecuencias del desarrollo de la digitalización en las relaciones financieras, propiciada por la pandemia del COVID-19, ha sido un notabilísimo aumento del ciberfraude, generando una industrialización de esta actividad ilícita.

Por otro lado, esta entidad subraya el interés de las organizaciones criminales en operar con criptoactivos por favorecer el anonimato (SEPBLAC, 2024).

Pero no solo la cibercriminalidad económica se constriñe al ciberfraude, pues otra operativa sumamente dañina es la denominada como *ransomware*. Además, la modalidad *crime as a service* es una constante en este ámbito delincuencial.

Uno de los medios más eficaces seguidos por esta cibercriminalidad para alcanzar sus objetivos (*ransomware*, fraudes *online* y blanqueo) es la utilización de plataformas de servicios digitales legítimos (redes sociales, *apps*, *marketplaces*, pagos, nube). Estas se configuran como una de las principales «superficies de ataque» que la ciberdelincuencia económica explota y están en el centro de la respuesta estratégica UE-España. A escala UE, millones de ciudadanos son objetivo cada año y se sustraen miles de millones de euros[49].

[48] En este marco, ha introducido medidas regulatorias como el Real Decreto 1007/2023 (requisitos de software de facturación y trazabilidad/verificabilidad para combatir el *sales suppression*), o el establecimiento del uso del Registro de Operadores Intracomunitarios (ROI) y el impulso a equipos conjuntos de investigación en fraudes intracomunitarios.

[49] IOCTA 2024–2025, ENCODG 2025 y Estrategia Nacional de Ciberseguridad.

Por otro lado, la UE[50] y España (ESN 2021, Estrategia Nacional de Ciberseguridad 2019 y Ley 36/2015, de Seguridad Nacional) asumen la ciberseguridad como infraestructura de la seguridad económica.

La inteligencia y la colaboración público-privada es esencial en este ámbito, extremo potenciado por todas las estrategias europeas, nacionales y sectoriales.

3.1.4 Economía derivada del tráfico de drogas

La Estrategia de la UE en materia de lucha contra las drogas 2021-2025, aprobada por el Consejo el 18 de diciembre de 2020, marca como primera prioridad para luchar contra el narcotráfico la asfixia económica de las organizaciones criminales, no permitiendo que los beneficios ilícitos puedan ser introducidos en el sistema legal[51].

Los estudios que EUROPOL ha realizado sobre el tráfico de droga en la UE remarcan el impacto severo que provoca al sistema económico europeo, estimando que el mercado de drogas en la UE asciende a un valor mínimo de al menos 31 000 millones de euros al año, constituyendo una de las fuentes principales de ingresos para la delincuencia organizada (EMCDDA y EUROPOL, 2024).

La ENCO 2025 señala al narcotráfico como el mercado ilícito con mayor capacidad de generación de beneficios ilícitos en España. Detallando que los beneficios derivados del tráfico de drogas se canalizan hacia sectores como la hostelería, inmobiliario, transporte y ocio nocturno, afectando a la competencia y facilitando el blanqueo.

Estudios referidos por el Grupo de Acción Financiera Internacional (GAFI/FATF) indican que las redes dedicadas al narcotráfico suelen utilizar criptoactivos como medio de pago y capa de anonimato, así como empresas pantalla para enmascarar los flujos ilícitos y ocultar su origen (FATF, 2022) y testaferros (Savona y Riccardi, 2015).

---

[50] Communication from the Commission to the European Parliament and the Council: Advancing European economic security: an introduction to five new initiatives. Disponible en: https://commission.europa.eu/system/files/2024-01/Communication%20on%20European%20economic%20security.pdf?utm_ [Consulta: 28 agosto 2025].

[51] Consejo de la UE. Estrategia de la UE sobre drogas 2021-2025. Disponible en: https://www.consilium.europa.eu/media/54074/qc0521073esn_002.pdf [Consulta: 26 agosto 2025].

3.1.5 Delitos contra el mercado y la propiedad intelectual/industrial

Desde una perspectiva global, el comercio de falsificaciones constituye un fenómeno estructural con graves repercusiones económicas y de seguridad. Según el informe conjunto de la Organización para la Cooperación y el Desarrollo (OCDE/OECD) y la EUIPO (2021), el valor del comercio mundial de productos falsificados se estimó en 467 000 millones de dólares, lo que equivale aproximadamente al 2,3 % del comercio mundial. En el caso específico de la UE, las importaciones de falsificaciones ascendieron a 99 000 millones de euros en 2021, representando el 4,7 % del total de importaciones procedentes de terceros países (OECD/EUIPO, 2025).

En España, y únicamente en los sectores de juguetes, cosmética y textil, las pérdidas ascienden a 1511 millones de euros anuales y suponen la destrucción de más de quince mil empleos cada año[52].

Respecto a las actividades fraudulentas de afectación a los mercados, la EU mantiene una regulación básica[53], que establece los términos de manipulación de mercado y los de información privilegiada (incluidas sanciones penales mínimas armonizadas), en virtud del riesgo que suponen para la integridad de los mercados y la confianza pública.

En España, existen dos organismos reguladores para estas cuestiones la CNMV y la CNMC. En 2018, la CNMC creó, en el ámbito de su Dirección de Competencia, la Unidad de Inteligencia Económica (UIE), a la que se ha ido dotando paulatinamente de personal especializado y recursos específicos. Su cometido es la detección de oficio de conductas anticompetitivas, con especial atención a la lucha contra los cárteles (CNMC, 2023).

3.1.6 Criminalidad medioambiental

En el ámbito medioambiental, la ENCO 2025 señala que los delitos asociados a la gestión y tráfico ilegal de residuos, el comer-

[52] Oficina española de patentes y marcas (OEPM). Boletín 162. EUIPO Observatory new study. Enero 2024. Disponible en: https://www.oepm.es/cs/OEPMSite/contenidos/Revista_InfoPYM/2024/Enero/en/noticia3.html?utm_ [Consulta: 29 agosto 2025].

[53] El Reglamento (UE) N.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre abuso de mercado) y la Directiva 2014/57/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre las sanciones penales aplicables al abuso de mercado (Directiva sobre abuso de mercado).

cio ilícito de especies protegidas y la explotación irregular de recursos naturales constituyen un desafío creciente para España. Estas prácticas, con frecuencia vinculadas al crimen organizado, no solo provocan graves daños a los ecosistemas, sino que también afectan a la economía formal. Frente a ello, se subraya la importancia de potenciar las redes de inteligencia medioambiental y la cooperación interinstitucional, con el fin de mitigar los impactos más nocivos de esta modalidad criminal[54].

EUROPOL, en su European Financial and Economic Crime Threat Assessment (2023), añade un relativamente nuevo vector en este ámbito, la transición verde, que crea nuevos nichos para el fraude vinculados a la contratación pública mediante la corrupción, extremo que puede lastrar inversiones y objetivos de sostenibilidad si no se acompaña de adecuados controles de integridad.

3.1.7 Trata de seres humanos

La lucha contra la trata de seres humanos es una prioridad para la UE[55]. Es una de las prácticas delictivas más rentables para las organizaciones criminales, con unos costes sociales y económicos muy significativos para la UE. La Estrategia de la Comisión Europea 2021-2025 contra la trata cifra en 2700 millones de euros al año el coste económico de la trata en la UE.

El Plan Estratégico Nacional contra la Trata y la Explotación de Seres Humanos 2021-2023 (PENTRA)[56] ya establecía, en concordancia con la ENCODG 2019 y posteriormente con la ENCODG 2025, la necesidad de intensificar las investigaciones financieras para neutralizar la capacidad económica de las redes criminales

[54] Las estimaciones conjuntas de la OCDE, la UNODC, el PNUMA y la INTERPOL sitúan el valor monetario de toda la criminalidad medioambiental transnacional organizada entre 70 000 y 213 000 millones de dólares estadounidenses anuales (UNICRI, 2016).

[55] Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime, 3043rd JUSTICE and HOME AFFAIRS, Council meeting Bruselas, 8 y 9 de noviembre de 2010. Disponible en: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf [Consulta: 28 agosto 2025].

[56] El plan se evaluó en 2024, con la intención de elaborar una nueva estrategia para erradicar esta actividad delictiva. https://www.interior.gob.es/opencms/es/detalle/articulo/Las-Fuerzas-y-Cuerpos-de-Seguridad-del-Estado-liberaron-a-1.466-victimas-de-trata-y-explotacion-en-2023-un-24-por-ciento-mas-que-en-2022/#:~:text=BALANCE%20DEL%20PLAN%20ESTRAT%C3%89GICO%20NACIONAL,trata%20y%20explotaci%C3%B3n%20de%20personas [Consulta: 28 agosto 2025].

dedica a esta actividad delictiva, así como generar inteligencia que pueda ser empleada en la lucha contra esta lacra social[57].

3.1.8 Corrupción

La corrupción constituye un fenómeno transversal que afecta a la totalidad de los ámbitos delictivos analizados y que se erige como un facilitador crítico (junto con el blanqueo de capitales y el uso de estructuras empresariales legales) de la delincuencia organizada y grave. Su capacidad para erosionar la integridad institucional, distorsionar la competencia económica y debilitar la confianza en el Estado de Derecho (Blackburn *et al*., 2017) la convierte en una amenaza prioritaria tanto para la UE como para España.

A escala europea, el SOCTA 2025 de EUROPOL identifica la corrupción como un instrumento recurrente de las redes criminales, empleado para infiltrarse en la economía legal, manipular contrataciones públicas, asegurar impunidad y neutralizar controles regulatorios.

En España, la ENCODG 2025, en concordancia otra vez con la estrategia europea, considera a la corrupción como un fenómeno trasversal en la criminalidad organizada y grave[58], con incidencias múltiples en la seguridad nacional, debilitando los pilares del buen Gobierno, generando desconfianza y deterioro institucional, infiltrándose en infraestructuras y obstruyendo la acción de la justicia.

En este marco, cabe señalar que el Gobierno español aprobó, el 26 de agosto del 2025, el Plan de Lucha contra la Corrupción[59] y creó una Comisión Interministerial para su puesta en marcha y seguimiento[60], recogiendo las recomendaciones del Grupo de

[57] CITCO. PENTRA. Disponible en: https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/220112_Plan_nacional_TSH_PENTRA_FINAL_2021_2023.pdf [Consulta: 28 agosto 2025].

[58] Entre sus líneas de acción, prevé potenciar la detección y neutralización de los delitos de corrupción, mejorar procedimientos en áreas vulnerables a la infiltración criminal y reforzar las investigaciones financieras y la recuperación de activos.

[59] Vicepresidencia Primera del Gobierno. Ministerio de Hacienda. Nota de prensa. Disponible en: https://www.hacienda.gob.es/es-ES/Prensa/Noticias/Paginas/2025/20250826-NP-CM-LUCHA-CONTRA-CORRUPCION.aspx [Consulta: 28 agosto 2025].

[60] Real Decreto 711/2025, de 26 de agosto, por el que sea crea la Comisión Interministerial para el impulso del Plan Estatal de Lucha contra la Corrupción, y se establece

Estados contra la Corrupción del Consejo de Europa (GRECO)[61], de la OCDE, la Comisión Europea y de la sociedad civil. Destacando la potenciación del *Big Data* y la AI en el marco de la contratación pública, así como una especial atención al fraude asociado a fondos europeos.

3.2 Sectores con mayor penetración criminal, perspectiva económica

Como se ha expuesto, la evidencia europea y española muestra que la delincuencia organizada y grave penetra preferentemente en sectores intensivos en efectivo, con barreras de entrada bajas o donde puede utilizar estructuras legales (sociedades, fundaciones, testaferros, contratos, licitaciones públicas, etc.) para dar cobertura y legitimidad a actividades ilícitas, así como blanquear los bienes ilícitos.

Además, se debe apuntar que España resulta mucho más atractiva que otros países de su entorno para la DO y la DG por distintos factores geográficos, logísticos, estructurales y económicos (Balas Dávila, 2023).

En virtud de todo lo anterior, los sectores que soportan el mayor impacto de injerencia de esta criminalidad organizada y grave son:

- Sector energético e infraestructuras críticas

El sector energético, en su doble dimensión de actividad económica esencial y de infraestructura crítica, constituye un ámbito de particular vulnerabilidad frente a la delincuencia organizada y grave.

El caso del fraude en los hidrocarburos es paradigmático, según el SOCTA 2025, se lleva a cabo a través de estructuras criminales complejas que gestionan toda la cadena de suministro y la distribución minorista[62].

---

su composición y funcionamiento. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-17185 [Consulta: 28 agosto 2025].

61 El Grupo de Estados contra la Corrupción (GRECO) es un órgano del Consejo de Europa creado en 1999 para supervisar las políticas anticorrupción y ayudar a sus Estados miembros a mejorar su capacidad de prevención y lucha contra la corrupción a través de la evaluación de sus sistemas. El GRECO incluye a los 46 miembros del Consejo de Europa, Estados Unidos y Kazajistán.

62 De este modo, los delincuentes implicados en el fraude de combustibles dependen de la experiencia de profesionales, como químicos y trabajadores del sector petrolero.

– Servicios financieros, pagos y criptoactivos

Este sector es uno de los de mayor riesgo por estar expuesto, constantemente, a dinámicas de blanqueo de capitales llevadas a cabo por la generalidad de la delincuencia grave y organizada.

Por ello, su monitorización es exhaustiva y constante por las diferentes unidades de inteligencia financiera de los distintos países, siendo esta función desarrollada por el SEPBLAC en España.

– Construcción e inmobiliario

La inversión en inmuebles y construcción es una de las vías más frecuentes para colocar y estratificar fondos ilícitos, al constituir un sector intensivo en capital, con una elevada capacidad de enmascaramiento y valorización, donde el uso criminal de profesionales (abogados, agentes, notarios) y estructuras societarias está muy expandido (Europol, 2023).

– Hostelería, restauración, ocio y turismo

Bares, restaurantes, hoteles y locales de ocio, en general, son también negocios intensivos en efectivo idóneos para mezclar flujos ilícitos con ventas legítimas y para encajar empleo irregular (Savona y Riccardi, 2015). Es decir, constituyen otro instrumento para blanquear los bienes ilícitos obtenidos.

– Comercio mayorista/minorista, *e-commerce* y fraude de impuestos

El comercio, en general, se ve afectado por la competencia desleal que llevan a cabo la delincuencia organizada y grave a través de la ventaja competitiva que le proporciona la falsificación, la denominada piratería, y por la omisión en la satisfacción de las cargas fiscales[63].

En este ámbito también se incluye las distintas formas de contrabando, siendo un valor refugio para las organizaciones criminales, el contrabando y la falsificación de tabaco.

– Transporte, logística y puertos

El fraude documental, como la declaración falsa de mercancías transportadas, está plenamente implantado en estas prácticas fraudulentas.

[63] Los sectores donde sufren con insistencia este desgaste son: industria cultural y creativa (música, cine, software, videojuegos, literatura), moda y textil, industria farmacéutica y cosmética, automoción y repuestos, agroalimentario y pesticidas, así como componentes tecnológicos.

Las organizaciones criminales emplean empresas de transporte y logística (incluidos agentes transitarios, depósitos fiscales y almacenes) para mover mercancías ilícitas y legitimar flujos comerciales. Estas acciones, frecuentemente, se encuentran vinculadas con prácticas corruptoras, llegando a constituirse nodos de corrupción.

– Gestión de residuos, reciclaje y medio ambiente

La gestión de residuos, energías renovables y actividades conexas presentan barreras regulatorias aprovechables y márgenes elevados. En este contexto, la concurrencia de manipulación de licencias y vertidos y el abuso de la subcontratación proyecta efectos de dumping ambiental[64] y de competencia desleal (EUROPOL, 2023; UNICRI, 2016).

– Contratación pública

La contratación pública constituye uno de los sectores más vulnerables a la penetración de la delincuencia organizada y la corrupción, debido al elevado volumen de recursos que gestiona y a la posibilidad de influir en la asignación de contratos y licitaciones. Tanto EUROPOL como EUROJUST han señalado que este ámbito es un objetivo prioritario de las redes criminales y corruptas, ya que facilita la creación de estructuras cuasimonopólicas mediante prácticas como la manipulación de concursos, el soborno o la colusión entre empresas y funcionarios, distorsionando la competencia y erosionando la confianza institucional.

4 Las investigaciones económicas

Tanto las estrategias nacionales españolas como las europeas destacan que investigar la dimensión económica de la amenaza que supone la delincuencia organizada y grave es crucial para neutralizarla. Por ello, el desarrollo de investigaciones de naturaleza económica se ha convertido en un pilar esencial para salvaguardar la integridad del sistema financiero (que pone en riesgo la DO y la DG) y, por ende, la seguridad nacional.

Las investigaciones económicas aglutinan las tres tipologías básicas que concurren en la indagatoria criminal: investigación de actividad, investigación de hechos e investigación documental.

[64] Práctica competitiva por la que una empresa o un país obtiene ventaja de costes al producir o vender aprovechando exigencias ambientales más laxas.

Esta concurrencia es requerida por la complejidad de perfeccionar los tipos penales asociados a los diferentes delitos de índole económico. Sirva de referencia de esta dificultad el hecho de que el blanqueo de capitales se configura como una de las tipologías delictivas que habitualmente se corrobora por prueba indiciaria[65].

La redundancia de indicios, a través de las tres tipologías expuestas, facilita la comprensión de la correspondencia de los hechos con los elementos del tipo.

En este marco de complejidad, es perentorio la IE, mediante la cual se facilita el enfoque inicial de la investigación, pudiendo también reforzarla de manera directa con la aportación de información muy especializada y que, en determinados casos, únicamente puede ser aportada por los propios sectores afectados, debido a su especificidad.

En este sentido, la estructura de una investigación económica suele involucrar múltiples fases y actores, combinando las técnicas clásicas de investigación criminal con herramientas propias del análisis financiero. En términos generales, un caso típico se desarrolla en cuatro fases fundamentales: policial, preprocesal, judicial y posexplotación.

La aportación de IE en cada una de estas fases aporta calidad a la investigación y contribuye a su eficacia (EUROPOL, 2017) (FATF, 2012).

4.1 Estructura de una investigación económica

– Fase policial

Es aquella que desarrolla la unidad policial investigadora de manera autónoma y suele ser el inicio de la investigación criminal.

El origen de esta actividad se vincula, en muchas ocasiones, a la recepción de IE, la cual puede provenir de actores que tienen normalizada la elaboración de inteligencia y su difusión como OLAF, AEAT o SEPBLAC, o por otros actores como asociaciones sectoriales que ven afectados sus intereses [por ejemplo, Sociedad

[65] En concordancia con lo dictado por la STS 801/2010, de 23 de septiembre de 2010 y, también, la STS 645/2023, 25 de julio de 2023. En concomitancia con ello, la «comunicación por indicio» es obligatoria para sujetos obligados (Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo), información esencial para elaborar los informes de inteligencia elaborados por el SEPBLAC. Esto no es «prueba indiciaria» penal, pero explica por qué, en la práctica, los casos de blanqueo llegan a sede penal con indicios concatenados

General de Autores y Editores (SGAE)] que generan informes *ad hoc* sobre alguna supuesta práctica fraudulenta del sector, o por diferente información de trabajadores y directivos de empresas que observan malas praxis que la entidad encubre de manera deliberada, etc.

En esta etapa, la información es fragmentaria y debe valorarse su fiabilidad y relevancia. Si se aprecia verosimilitud, se define un plan de obtención y se activa la correspondiente coordinación interagencial. De igual modo, cuando se detecta una proyección internacional, se conforma, ya en estos estadios iniciales, el apoyo de organismos internacionales como EUROPOL/EFECC u OLAF.

De esta forma, la IE recibida se intenta corroborar a través de diferentes comprobaciones de distinta naturaleza, para a continuación conectarla con hechos y entidades concretas compatibles con una tipología delictiva.

– Fase preprocesal

Esta se desarrolla en el marco de las diligencias de investigación desarrolladas por el Ministerio Fiscal[66] o por el procedimiento de investigación que incoe la EPPO[67]. Identificado el posible delito económico se consolida la estrategia.

En este sentido, se integran, bajo la tutela de las diferentes fiscalías, los primeros grupos interdisciplinares de investigación, este extremo se facilita cuando existen unidades de apoyo o adscritas a las distintas fiscalías.

Igualmente, se requiere, a través de las distintas fiscalías, la remisión de más inteligencia e información económica concreta, fundamentalmente, financiera, fiscal, aduanera, auditoría pública y de sectores afectados, a los actores que de manera normalizada generan dicha inteligencia[68].

[66] Artículo 773 de la LECrim, artículo 5 de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal y Circular 4/2013 de la Fiscalía General del Estado (FGE).

[67] Artículo 17 de la Ley Orgánica 9/2021, de 1 de julio, de aplicación del 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.

[68] Según la Memoria 2022-2023 del SEPBLAC, este organismo remitió 97 informes de inteligencia financiera. Del mismo modo, el Informe OLAF 2024 detallaba que 74 casos fueron remitidos por OLAF a la EPPO. Mientras que el Tribunal de Cuentas remitió un caso a Fiscalía apreciando responsabilidad penal, según la Memoria 2024 de la Fiscalía General del Estado.

Debido a la dilatación de las respuestas de los distintos organismos a los requerimientos de índole económico, esta fase es muy utilizada por dos cuestiones, la primera, porque alarga el tiempo de la indagatoria sin estar constreñida a lo marcado en las causas judicializadas, y la segunda, porque posibilita una base fáctica y documental más sólida[69], para la apertura de las diligencias judiciales pertinentes.

Si las distintas fiscalías entienden que concurren en los hechos investigados algún ilícito penal, procederá a conformar una denuncia ante la autoridad judicial solicitando la instrucción de las oportunas diligencias judiciales.

– Fase judicial

Esta es la fase nuclear de cualquier investigación criminal y la dirección corresponde a la autoridad judicial competente. Aquí se desarrollan, de manera mucho más concreta, las líneas de investigación que mantengan una mayor carga probatoria. En este sentido, se seguirá recabando información e inteligencia de las distintas fuentes[70], normalizadas o no normalizadas mediante las diligencias necesarias que estime el órgano instructor[71].

Es en esta fase donde, se pueden acordar medidas de investigación limitativas de derechos fundamentales, como la interceptación de comunicaciones telefónicas y telemáticas y la captación y grabación de comunicaciones orales mediante dispositivos electrónicos, así como el uso de dispositivos técnicos de seguimiento y localización[72], al objeto de convertir la inteligencia financiera que se obtenga de estas actuaciones en impacto operativo (EUROPOL, 2017).

Una vez se tienen indicios suficientes sobre las entidades que participan en los supuestos hechos delictivos investigados, la autoridad judicial determinará la práctica de nuevas diligencias con el fin de alcanzar determinada información que de otro modo no sería posible obtener, alguna de ellas pueden consistir en entradas y registros o detenciones. La práctica del conjunto de

[69] Circular 4/2013 de la FGE, sobre las diligencias de investigación.

[70] La Memoria de actividades de la IGAE 2024 identifica actuaciones en 87 procedimientos bajo la fórmula de auxilio judicial. El Informe anual de la CNMV 2024 muestra que se actuó en sesenta ocasiones en el ámbito penal por requerimientos de la autoridad judicial o Fiscalía. La Memoria de la CNMC 2023 refleja 1051 actuaciones ante solicitudes de Juzgados y Tribunales, así como otras administraciones públicas.

[71] Artículo 774.1 de la LECrim.

[72] Artículos 588 ter, 588 quater y 588 quinquies de la LECrim.

estas diligencias se denomina, en el desarrollo de la investigación criminal policial, explotación de la investigación.

– Fase posexplotación

  Realmente, esta etapa sigue bajo la tutela de la instrucción judicial, pero se diferencia de la anterior porque la perspectiva investigativa cambia. Aunque sigue bajo la dirección del órgano judicial de la instrucción, en esta fase el énfasis de la investigación transita desde la obtención de evidencias a su tratamiento y análisis intensivo.

  El corpus documental que llega a esta fase suele ser voluminoso y no normalizado: entradas y registros, interceptaciones de comunicaciones, seguimientos/localizaciones, y, muy especialmente, registros y volcados forenses de dispositivos electrónicos y acceso remoto a sistemas, todo ello obtenido bajo autorización judicial.

  Dado el volumen y heterogeneidad de la información (documental, financiera, digital), esta etapa es eminentemente analítica, en la cual se depuran, correlacionan y visualizan los patrones y los flujos, para determinar la trazabilidad y posibles conversiones de los bienes ilícitamente obtenidos, priorizando objetivos y articulando medidas de recuperación de activos.

En este sentido, los organismos internacionales recomiendan el uso de analítica avanzada como *Big Data* y aprendizaje automático para generar inteligencia financiera que pueda ser utilizada de manera efectiva en el procedimiento judicial.

Tras el análisis de todo lo intervenido en la explotación, la Policía Judicial y los peritos elevan informes complementarios al Juzgado. Tras lo cual, y siguiendo los trámites oportunos, el instructor judicial remite la causa al órgano de enjuiciamiento, con lo que culmina la fase instructora y se inicia la de juicio oral.

En suma, las investigaciones económicas, en sentido amplio, abarcan todas aquellas pesquisas orientadas a desentrañar las estructuras financieras, patrimoniales y comerciales detrás de actividades ilícitas complejas.

Su finalidad va más allá de la mera persecución penal individual, buscando neutralizar las redes criminales atacando su capacidad económica, privándolas de ganancias ilícitas y desarticulando sus entramados empresariales.

Así, el enfoque económico complementa las investigaciones tradicionales, añadiendo una capa de análisis que permite identificar a los beneficiarios finales, detectar vínculos ocultos entre delincuentes y aparentes negocios legales, y descubrir flujos financieros opacos que alimentan actividades delictivas. Todo ello requiere de metodologías rigurosas, personal especializado (analistas financieros, peritos contables, etc.) y, sobre todo, de una adecuada integración de la IE en el proceso investigador.

4.2 Integración de la inteligencia económica en las investigaciones

Para que un proceso de inteligencia sea operativo y útil en investigación, no puede desarrollarse de forma aislada, es decir, debe conectarse estrechamente con la investigación judicial y fiscal, a través de los organismos policiales competentes encargados de materializar las pesquisas.

En otras palabras, la inteligencia (como conocimiento analítico) solo adquiere pleno valor cuando fluye hacia la acción investigadora, guiando a quienes tienen la potestad legal de obtener pruebas y perseguir delitos. Este principio de integración ha sido destacado tanto por expertos como por las propias instituciones.

En términos sustantivos, la coordinación y cooperación tempranas entre analistas de inteligencia e investigadores permite orientar desde el inicio las líneas de indagación hacia indicios de difícil detección (como cuentas en jurisdicciones de baja tributación y alta opacidad o la utilización de testaferros internacionales) antes de que se disipen o desaparezcan, lo que incrementa de forma significativa la eficacia de la investigación.

En España, la integración de la IE en las investigaciones se enfrenta al desafío de la ausencia de un SIE formal, pero cuenta con mecanismos parciales de coordinación que se han ido desarrollando en distintos ámbitos.

Uno de ellos es el Departamento de Seguridad Nacional (DSN), órgano de la Presidencia del Gobierno que integra análisis interministeriales sobre riesgos estratégicos, incluyendo los económicos.

No obstante, los intercambios en el máximo nivel estratégico no se traducen automáticamente en mecanismos operativos estables. Diversos análisis recomiendan institucionalizar dichos intercambios (objetivo que perseguía el no implementado SIE) para

que la cooperación no dependa de la mera buena voluntad personal ni de iniciativas *ad hoc*.

En consecuencia, se aprecia la necesidad de reforzar los órganos nacionales de coordinación en inteligencia económica y dotarlos de procedimientos normalizados de trabajo, canales permanentes de intercambio de información y circuitos de retroalimentación que conecten de forma estructurada y continua la inteligencia estratégica (orientada a riesgos económicos sistémicos) con las unidades investigadoras de investigación criminal.

Un caso práctico de unidad de fusión operativa es el mencionado CITCO, adscrito al Ministerio del Interior. Con rango de subdirección general, el CITCO recibe, integra y analiza la información estratégica que le proporcionan todas las fuerzas y cuerpos de seguridad sobre delincuencia organizada, criminalidad grave, terrorismo y radicalización, elaborando inteligencia criminal de carácter estratégico, prospectivo, pero también operativo.

En este sentido, actúa como punto de contacto nacional para el intercambio de inteligencia con organismos internacionales, manteniendo relaciones con centros homólogos de la UE (EUROPOL) y de terceros países. En la práctica, el CITCO coordina la elaboración de valoraciones nacionales de amenaza y la respuesta unificada a fenómenos que trascienden el ámbito de una sola agencia.

Su rol ilustra cómo integrar inteligencia en investigaciones: por un lado, gestiona información de múltiples fuentes policiales (y de otras agencias) para producir análisis integrados. Por otro, retroalimenta a las unidades investigadoras con dichas valoraciones, señalando prioridades, conexiones entre casos y tendencias emergentes.

En suma, el CITCO funciona como un modelo sectorial de integración: es un *hub* donde converge la inteligencia criminal y desde el que se articula la cooperación tanto interinstitucional (entre cuerpos de seguridad y ministerios) como internacional.

La Estrategia Nacional contra el Crimen Organizado 2019-2023 apunta que debe potenciarse el papel del CITCO para mejorar la coordinación efectiva de investigaciones[73].

[73] También recalca la importancia de que CITCO elabore inteligencia estratégica útil y facilite investigaciones conjuntas cuando las tramas criminales operan en múltiples ámbitos delictivos.

El enfoque colaborativo público-privado es esencial, pues muchas informaciones críticas residen en empresas (entidades bancarias, compañías energéticas, telecomunicaciones o grandes corporaciones tecnológicas) que deben cooperar estrechamente con el Estado para detectar distintos riesgos económicos.

Algunos pasos ya se han dado en esa dirección bajo el paraguas del CNPIC, existiendo convenios con empresas estratégicas para intercambiar información de inteligencia sobre amenazas, muchas de ellas económicas.

En el plano operativo, la integración de la inteligencia económica implica también mejorar el tránsito de la información entre agencias con competencias distintas. Un punto crítico es asegurar que la inteligencia financiera (procedente de UIF, AEAT, órganos supervisores, entidades reguladoras, etc.) pueda ser compartida en tiempo y forma con las unidades investigadoras policiales y judiciales, superando barreras legales o burocráticas en los momentos iniciales de una investigación.

A este respecto, la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que facilitan el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales en España, que transpone directivas europeas, establece cauces suficientemente ágiles para que la inteligencia accionable gestionada por el SEPBLAC pueda ser distribuida oportunamente a las fuerzas de seguridad y al Ministerio Fiscal.

A nivel europeo, la integración de la IE en las investigaciones es ya una realidad institucionalizada en varios frentes. EUROPOL cuenta con centros especializados, como el mencionado EFECC, dedicados a apoyar a los Estados miembros en casos de delincuencia financiera compleja.

EUROPOL recopila y analiza datos de inteligencia aportados por las diferentes policías nacionales siguiendo protocolos estandarizados, enriqueciendo esta información con fuentes complementarias (informes de *open sources*, investigación académica y casos de estudio). El resultado son productos de inteligencia que transfiere a los distintos cuerpos policiales de los diferentes países, posibilitando, también, la articulación de equipos conjuntos.

Tales análisis conjuntos trabajan en la prevención, permitiendo a las fuerzas de seguridad anticiparse a las tendencias delictivas y orientar mejor sus recursos.

Como ya se ha detallado, existen otros organismos como OLAF y la EPPO, que también juegan un papel integrador. OLAF investiga el fraude que afecta al presupuesto de la UE, generando inteligencia que luego se transfiere a EPPO para su judicialización cuando procede, así como a los países miembros.

En síntesis, la integración de la IE en las investigaciones es un requisito indispensable para afrontar con éxito las amenazas actuales. La UE ha ido institucionalizando un enfoque integrado, situando la inteligencia financiera en el centro de la identificación, anticipación y neutralización de las formas más lesivas de criminalidad organizada.

Para España, avanzar en esta misma línea supone reforzar los mecanismos de coordinación (DSN, CITCO, comités especializados, etc.) y asegurar que todos los procesos de IE tengan un cauce directo hacia la investigación criminal a través de las fuerzas y cuerpos de seguridad competentes y el Ministerio Fiscal.

Dados los hallazgos expuestos (inexistencia de un SIE formalmente definido, mecanismos solo parciales de coordinación y necesidad de cauces estables entre la inteligencia estratégica y las unidades investigadoras), resulta pertinente, en este punto, valorar la creación de un órgano colector con capacidad para absorber la inteligencia de interés para la seguridad nacional, filtrándola y clasificándola conforme al listado de riesgos y amenazas de la ESN, que incluye la DO y la DG.

En el ámbito de la DO y la DG, la inteligencia criminal, incluida la IE procedente de distintos generadores, debería compartirse sistemáticamente con el CITCO, como nodo de fusión y coordinación operativa entre las FCS, con proyección internacional. A efectos de diseño institucional, el DSN se perfila como candidato idóneo para ejercer ese rol de colector que aglutine, gestione y transfiera al CITCO la inteligencia, por su vinculación con el Consejo de Seguridad Nacional y su ubicación en el Gabinete de la Presidencia (Dirección Adjunta), donde se integra la Oficina de Asuntos Económicos y G-20.

No obstante, su puesta en marcha exigiría, en su caso, adecuaciones normativas y dotaciones específicas (procedimientos normalizados, capacidades técnicas y humanas, así como circuitos de retroalimentación con las unidades investigadoras).

Solo así la inteligencia dejará de ser un mero producto teórico para convertirse en palanca efectiva que impulse investigaciones,

desarticule tramas criminales y contribuya a la preservación de la seguridad económica y con ello a la seguridad nacional.

4.3 Necesidades de información no normalizada en las investigaciones económicas

Una de las lecciones derivadas de la experiencia en investigaciones financieras complejas es que, con frecuencia, la información convencional no basta. Las organizaciones criminales aprenden a explotar vacíos y a mimetizarse con la economía legal, de modo que muchas de sus actividades ilícitas no quedan registradas de forma directa, de manera evidente, en ningún registro oficial.

Por ello, las investigaciones económicas requieren acceder a información no normalizada, es decir, a fuentes y a tipos de datos que no siguen los esquemas tradicionales o que no están integrados en los canales formales de intercambio entre agencias. Este tipo de información puede incluir desde documentación informal hasta inteligencia prospectiva o fuentes abiertas, y suele ser imprescindible para llenar los vacíos de conocimiento sobre una trama delictiva.

Por información no normalizada se puede entender, en primer lugar, aquella que no está estandarizada ni estructurada en registros oficiales. Un ejemplo típico son los datos procedentes de fuentes abiertas (OSINT): noticias de prensa, publicaciones en redes sociales, *blogs* financieros, foros de Internet e incluso filtraciones como los denominados periodísticamente «papeles de Panamá". Este tipo de información, aunque inicialmente no verificada, puede aportar indicios valiosos.

La inteligencia de fuentes abiertas se ha convertido en una disciplina en sí misma dentro del análisis económico: proporciona contexto sobre tendencias de mercado, perfiles reputacionales de individuos y empresas, conexiones globales, etc., que, difícilmente, se obtienen de bases de datos estructuradas.

Integrar OSINT en las investigaciones económicas implica dotarse de herramientas para cribar grandes volúmenes de información en Internet, usar algoritmos de búsqueda avanzada y contar con analistas capaces de separar rumor del dato comprobable.

Otro ámbito de información no normalizada son los datos comerciales y registros extranjeros. Seguir la pista a estas empresas requiere obtener información societaria de múltiples jurisdiccio-

nes, la cual no está unificada ni viene en formatos homogéneos, y donde la cooperación judicial internacional es esencial.

Todo esto constituye información «no normalizada» en tanto que no existe una base de datos única ni un estándar global para acceder a ella. Para salvar este escollo, las investigaciones económicas cuentan, cada vez más, con redes de colaboración internacional.

Estas diligencias generan un flujo de información heterogénea, desde extractos bancarios hasta testimonios de testigos, que debe integrarse cuidadosamente en la respectiva investigación nacional.

Asimismo, bajo la categoría de información no normalizada entran las técnicas especiales de obtención de información propias de los servicios de inteligencia o de las investigaciones encubiertas.

Por ejemplo, puede recabarse información a través de colaboradores o informantes en el mundo empresarial (HUMINT), cuyos aportes no siguen un formato predefinido y cuyo valor depende de la evaluación cualitativa que haga el analista.

Del mismo modo, operaciones de vigilancia electrónica (intervenciones de comunicaciones, rastreo de correos electrónicos, etc.) generan un volumen masivo de datos (grabaciones de voz, *logs*, mensajes, etc.) que no están ordenados para su uso inmediato y requieren un procesamiento intensivo para extraer la inteligencia accionable.

Por ejemplo, interceptar miles de correos de una empresa investigada produce un *dataset* no estructurado donde solo técnicas de análisis semántico o búsqueda por palabras clave podrán identificar menciones a pagos ilícitos o códigos que oculten transacciones.

La inteligencia de señales o SIGINT, que incluye escuchas telefónicas, análisis de tráfico de comunicaciones, etc., es otra fuente de datos primarios que puede resultar decisiva para entender la mecánica de ciertos fraudes (por ejemplo, la identificación de responsabilidades y roles dentro de una organización criminal compleja), pero que inicialmente se presenta como información dispersa que ha de ser organizada y correlacionada con la información financiera obrante.

En el contexto de las investigaciones económicas, gestionar información no normalizada implica dotarse de capacidades analíticas y tecnológicas avanzadas. Herramientas de *data mining*, IA

y análisis de redes pueden convertir datos caóticos en patrones inteligibles. De igual forma, técnicas de *machine learning* permiten identificar anomalías en series temporales de transacciones bancarias que no serían evidentes a simple vista.

Estas tecnologías son indispensables para explotar la información no estructurada, pero a su vez requieren analistas capacitados para entrenar los modelos, interpretar los resultados y contextualizarlos correctamente, lo que supone la participación e integración en el equipo investigador de especialistas de diferentes ámbitos, más allá de los analistas económicos.

Finalmente, es importante resaltar que la información no normalizada debe ser tratada con rigor metodológico. Su naturaleza heterogénea puede abrir la puerta a errores si no se somete a un escrutinio adecuado. La calidad de la inteligencia producida dependerá de la capacidad para evaluar la fiabilidad de cada dato y fuente, para verificar la información por vías independientes y para documentar su cadena de custodia cuando vaya a incorporarse a un procedimiento judicial.

En este sentido, las investigaciones económicas exitosas suelen caracterizarse por un escrupuloso trabajo de validación: cada informe externo se contrasta con evidencias propias, cada dato crítico se apoya en al menos una fuente adicional. Así se evitan sesgos cognitivos y se garantiza que la imagen final reconstruida de la actividad económica investigada sea lo más fidedigna posible.

La meta última es que la autoridad judicial competente tenga a su disposición toda la información que necesite para su valoración jurisdiccional, en unas condiciones adecuadas de uso e integridad.

Por ello, la incorporación de información no normalizada, por muy atípica que sea su origen o formato, se erige en indispensable para perfeccionar ese objetivo: proveer a los decisores (jueces, fiscales y altos responsables de seguridad) del conocimiento completo y oportuno para tomar decisiones informadas y efectivas en la lucha contra las amenazas económico-financieras.

5 Conclusiones

Este documento constata la inexistencia en España de un SIE formalmente definido e institucionalizado, de modo que, la función

de IE se dispersa entre múltiples entidades sin una coordinación centralizada, lo que, inevitablemente, genera lagunas, enfoques dispares y dificultades para articular una respuesta unificada, adecuada y oportuna frente a las amenazas económico-financieras de la DO y la DG, respecto a la seguridad nacional.

Esta carencia estructural, provoca la incapacidad de generar una inteligencia integrada y global que aporte el valor añadido derivado de la recolección de información y de las diferentes perspectivas de los distintos actores que conforman el sistema económico descrito. Por lo que se evidencia la imposibilidad de generar una IE adecuada y oportuna, más allá de la actuación en determinados ámbitos vinculados a tipologías delictivas concretas.

Por otro lado, la complejidad competencial y la asimetría entre administraciones (incluso dentro del mismo nivel), así como la cesión de soberanía económica a la UE, dificulta la difusión de IE accionable que pudieran emanar de las entidades integradas en los distintos niveles, no existiendo un dispositivo operativo estable que garantice una integración homogénea de la IE y, menos aún, que permita alcanzar una deseable retroalimentación.

Asimismo, aunque el estudio reconoce mecanismos parciales de coordinación, subraya que los intercambios en el nivel estratégico no se traducen de forma automática en mecanismos estables y operables. Observando, igualmente, que la participación de diferentes órganos generadores de inteligencia, cuando cooperan en la lucha contra la DO y la DG, lo hacen de manera reactiva, sobre cuestiones concretas y ante revelaciones determinadas, es decir, por requerimiento de los responsables de la investigación criminal. Este extremo lastra definitivamente el factor oportunidad.

En el plano operativo-probatorio, se evidencia la necesidad de una formalización metodológica para tratar la información no normalizada. Aunque la normativa reciente facilita el uso de información financiera y su circulación hacia fuerzas de seguridad y Ministerio Fiscal, el estudio muestra que la explotación transversal de la IE presenta gradientes de madurez y barreras legales o burocráticas en momentos iniciales de la investigación, lo que afecta a la oportunidad del empleo de la inteligencia.

En coherencia con este diagnóstico, se propone valorar la habilitación normativa y material de un órgano colector de IE en el DSN, con canalización sistemática hacia el CITCO en materia de DO y DG, como mecanismo para convertir la IE en inteligencia oportuna y accionable en investigación.

Sin embargo, resulta evidente, en relación con todo lo anterior, que la IE financiera se ha institucionalizado como capacidad crítica para detectar, documentar y perseguir la DO y la DG, revelándose que su integración temprana mejora la focalización, la oportunidad y la calidad probatoria a lo largo del caso.

En este marco, la inteligencia tributaria (AEAT/ONIF) y aduanera (ONI/SVA) son palancas operativas con impacto directo en la protección de la seguridad económica (recaudación, competencia leal, integridad de mercados y flujos).

Del mismo modo, la UE ha interiorizado la IE como eje vertebrador de sus políticas de seguridad, institucionalizando un enfoque integrado que sitúa la dimensión financiera y económica en el centro de la identificación, anticipación y neutralización de las amenazas delictivas más graves, y que sirve de fundamento para iniciativas y planes estratégicos conjuntos a escala comunitaria.

En coherencia con ello, España ha avanzado en un alineamiento progresivo con estos marcos, manteniendo sus estrategias y planes nacionales de seguridad económica congruentes con las prioridades europeas e incorporando, entre las amenazas prioritarias, el crimen organizado de carácter financiero.

Existe colaboración efectiva de la CNMC y la Comisión Nacional del Mercado de Valores (CNMV) con autoridades judiciales, esencialmente, a requerimiento de estas. El reto consiste en sistematizar la explotación operativa de su inteligencia sectorial en casos penales complejos y mejorar su interoperabilidad con los canales financieros-fiscales-aduaneros, así como una aportación a las investigaciones criminales de manera proactiva y temprana.

En España existe, al menos conceptualmente, una comunidad de inteligencia ampliada que abarca el ámbito económico y que se integra con la UE. Más allá de los servicios clásicos de inteligencia y seguridad, este estudio constata la participación de un ecosistema más amplio de actores en la generación de inteligencia económica (ministerios económicos, reguladores, sector privado, academia, etc.), en línea con la visión holística promovida a nivel europeo.

En el ámbito de la indagatoria criminal, se propone consolidar equipos conjuntos y circuitos de retroalimentación operativa entre, al menos, SEPBLAC, FCS, AEAT y Ministerio Fiscal desde fases tempranas (policial y preprocesal), articulando cauces similares a los recogidos en la LO 9/2022 y utilizando canales estan-

darizados de intercambio de información como los existentes entre CITCO, EFECC, OLAF y EPPO.

Por tanto, para maximizar la explotación judicial, resulta necesario reforzar recursos humanos especializados (finanzas, datos/IA, cripto y forense digital) y clarificar el uso procesal de la IE mediante metodologías de documentación, verificabilidad y cadena de custodia, apoyadas por una unidad legal con guías y plantillas probatorias, formación a operadores y, en su caso, ajustes normativos acotados.

Con este conjunto coherente de medidas, las propuestas operativizan los hallazgos y permiten transitar de un modelo reactivo a uno anticipatorio, elevando la oportunidad (tiempo de llegada de la IE accionable) y la adecuación (relevancia y utilidad probatoria) en investigaciones económico-penales complejas.

Bibliografía

Arcos, R. (2012). Hacia un Sistema Español de Inteligencia para la seguridad económica y la competitividad [en línea]. Inteligencia y Seguridad. N.º 11, pp. 103-128. [Consulta: 2026]. Disponible en: https://rubenarcos.com/wp-content/uploads/2017/04/11.pdf

Balas Dávila, A. (2023). La financiación de la delincuencia organizada. *Cuadernos de la Guardia Civil*. N.º 69, pp. 49-70.

Buzan, B. (1991). People, States and Fear. An Agenda for International Security Studies in the post-Cold War Era. Hemel Hempstead, Harvester Wheatsheaf.

Castells, M. (2006). La era de la información: economía, sociedad y cultura. Madrid, Alianza Editorial.

Comisión Nacional de los Mercados y la Competencia (CNMC). (2023). *Memoria 2023* [en línea]. Madrid, CNMC. [Consulta: 10 agosto 2025]. Disponible en: https://www.cnmc.es/sites/default/files/editor_contenidos/CNMC/Memorias/Memoria%20CNMC_2023.pdf

—. (2025). Unidad de Inteligencia Económica (UIE) [en línea]. [Consulta: 27 julio 2025]. Disponible en: https://www.cnmc.es/vigilamos-la-competencia/unidad-de-inteligencia-economica

Consejo de la Unión Europea. (2010). Estrategia de seguridad interior de la Unión Europea. Hacia un modelo europeo de

seguridad [en línea]. Luxemburgo, Consejo de la Unión Europea, Secretaría General, Oficina de Publicaciones. [Consulta: 12 agosto 2025]. Disponible en: https://data.europa.eu/doi/10.2860/881

—. (2020). Estrategia de la UE sobre drogas 2021–2025 [en línea]. Bruselas, Consejo de la Unión Europea, Secretaría General. [Consulta: 8 agosto 2025]. Disponible en: https://www.consilium.europa.eu/media/54074/qc0521073esn_002.pdf

Damro, C. (2012). Market power Europe [en línea]. Journal of European Public Policy. 19(5), pp. 682-699. [Consulta: 2026]. Disponible en: https://doi.org/10.1080/13501763.2011.646779

Davara Rodríguez, F. (2015). Planificación estratégica e inteligencia económica. *Cuadernos de estrategia*. N.º 174, pp. 189-229.

Departamento de Seguridad Nacional (DSN). (2013). Estrategia de Seguridad Marítima Nacional 2013 [en línea]. Departamento de Seguridad Nacional, Presidencia del Gobierno. [Consulta: 18 julio 2025]. Disponible en: https://www.lamoncloa.gob.es/documents/20131333estrategiadeseguridadmartima_u.pdf

—. (2017). Estrategia de Seguridad Nacional 2017 [en línea]. [Consulta: 7 julio 2025]. Disponible en: https://www.dsn.gob.es/es/buscador?key=Estrategia+de+Seguridad+Nacional+2017

—. (2021). Estrategia de Seguridad Nacional 2021 [en línea]. Departamento de Seguridad Nacional, Presidencia del Gobierno. [Consulta: 29 julio 2025]. Disponible en: https://www.dsn.gob.es/es/publicaciones/estrategia-de-seguridad-nacional-2021

—. (2024). Estrategia Nacional de Seguridad Marítima 2024 [en línea]. Departamento de Seguridad Nacional, Presidencia del Gobierno. [Consulta: 2026]. Disponible en: https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENSM2024

Díaz Fernández, A. M. (2013). El papel de la inteligencia estratégica. *Cuadernos de estrategia*. N.º 162, pp. 35-66.

EMCDDA y Europol. (2024). EU Drug Markets Analysis: Key insights for policy and practice [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 25 agosto 2025]. Disponible

en: https://www.euda.europa.eu/publications/eu-drug-markets/analysis-key-insights-policy-and-practice_en

España. (1986). Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad [en línea]. Boletín Oficial del Estado. 3 de abril, núm. 63. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859

—. (2002). Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia [en línea]. Boletín Oficial del Estado. 7 de mayo, núm. 109. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

—. (2010). Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [en línea]. Boletín Oficial del Estado. 23 de junio, núm. 152, pp. 54811-54883. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/lo/2010/06/22/5

—. (2015). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. [en línea]. Boletín Oficial del Estado. 29 de septiembgre, núm. 233, pp. 87106-87117. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10389

—. (2017). Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017 [en línea]. Boletín Oficial del Estado. 22 de diciembre, núm. 309. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2017-15181

—. (2019a). 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 [en línea]. Boletín Oficial del Estado. 22 de febrero, núm. 46, pp. 17048-17074. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/o/2019/02/21/pci161

—. (2019b). 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 [en línea]. Boletín Oficial del Estado. 30 de abril, núm. 103, pp. 43437-43455. [Consulta: 6 julio 2025]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-6347

—. (2021a). Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 [en línea]. Boletín Oficial del Estado. 31 de diciembre, núm. 314,

pp. 167795-167830. [Consulta: 2026]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884

—. (2021b). Resolución de 13 de enero de 2021, de la Presidencia de la AEAT, sobre organización y atribuciones de funciones en el Área de Aduanas e Impuestos Especiales [en línea]. Boletín Oficial del Estado. 15 de enero, núm. 13, pp. 3826-3850. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/res/2021/01/13/(5)

—. (2024). Real Decreto 207/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. [en línea]. Boletín Oficial del Estado. 28 de febrero, núm. 52, pp. 23452-23487. [Consulta: 2026]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-3793

Esteban Navarro, M. Á. (2007). *Glosario de inteligencia*. Madrid, Ministerio de Defensa.

Eurojust. (2022). Eurojust Report on Money Laundering [en línea]. La Haya, Eurojust. [Consulta: 26 agosto 2025]. Disponible en: https://www.eurojust.europa.eu/publication/eurojust-report-money-laundering

—. (2025). Informe anual 2024 (ES) [en línea]. La Haya, Eurojust. [Consulta: 26 agosto 2025]. Disponible en: https://www.eurojust.europa.eu/about-us/planning-and-reporting/annual-report

European Commission et al. (2024). VAT gap in the EU: 2024 report [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 26 agosto 2025]. Disponible en: https://doi.org/10.2778/2476549

European Commission. (2024). Advancing European economic security: an introduction to five new initiatives [en línea]. [Consulta: 11 agosto 2025]. Disponible en: https://place-based-innovation.ec.europa.eu/publications/advancing-european-economic-security-introduction-five-new-initiatives_en

European Public Prosecutor's Office (EPPO). (2025). Annual Report 2024 [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 26 agosto 2025]. Disponible en: https://doi.org/10.2927/9973133

European Union Drugs Agency (EUDA). (2025). European Drug Report 2025: Trends and Developments [en línea]. Lisboa, European Union Drugs Agency (EUDA). [Consulta: 25 agosto

2025]. Disponible en: https://www.euda.europa.eu/publications/european-drug-report/2025_en

Europol. (2011). EU Organised Crime Threat Assessment (OCTA) 2011 [en línea]. [Consulta: 8 julio 2025]. Disponible en: https://www.Europol.europa.eu/publications-events/main-reports/octa-2011-eu-organised-crime-threat-assessment

—. (2013). European Union Serious and Organised Crime Threat Assessment (SOCTA) 2013 [en línea]. [Consulta: 23 agosto 2025]. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/aecc0329-38b1-4a8c-9d92-a5c19044c420

—. (2017a). European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017 [en línea]. [Consulta: 9 julio 2025]. Disponible en: https://data.europa.eu/data/datasets/serious-and-organised-crime-threat-assessment-2017

—. (2017b). From suspicion to action: converting financial intelligence into greater operational impact [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 20 julio 2025]. Disponible en: https://doi.org/10.2813/568228

—. (2021a). European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021 [en línea]. [Consulta: 31 julio 2025]. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/6e5575ce-c34b-11eb-a925-01aa75ed71a1

—. (2021b). Shadow money – the international networks of illicit finance. Europol Spotlight Series.

—. (2023). The other side of the coin: an analysis of financial and economic crime [en línea]. Luxemburgo, Publications Office. [Consulta: 14 agosto 2025]. Disponible en: https://data.europa.eu/doi/10.2813/105613

—. (2025). European Union Serious and Organised Crime Threat Assessment (EU SOCTA) 2025: The changing DNA of serious and organised-crime [en línea]. [Consulta: 12 julio 2025]. Disponible en: https://www.Europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

FATF. (2012). Operational Issues: Financial Investigations Guidance. París, FATF.

—. (2022). Money Laundering from Fentanyl and Synthetic Opioids. París, FATF.

Friedman, T. L. (1999). *The Lexus and the Olive Tree: Understanding Globalization*. Nueva York, Farrar, Straus and Giroux.

HM Government. (2023). Serious and Organised Crime Strategy 2023-2028.

Jacques, M. (2012). *When China Rules the World*. 2.ª ed. Londres, Penguin.

Johnson, L. K. (2007a). *Handbook of Intelligence Studies*. Londres, Routledge.

—. (2017b). *National Security Intelligence*. Cambridge, Polity Press.

Kent, S. (1966). Strategic Intelligence for American World Policy [en línea]. Princeton, Princeton University Press. [Consulta: 31 agosto 2025]. Disponible en: https://www.jstor.org/stable/j.ctt183q0qt

LLYC. (2015). Inteligencia económica; una política pública para España [en línea]. Revista UNO. [Consulta: 11 julio 2025]. Disponible en: https://www.revista-uno.com/numero-19/inteligencia-economica-una-politica-publica-para-espana/

Lowenthal, M. M. (2012). *Intelligence: From Secrets to Policy*. Washington, DC, CQ Press.

McGann, J. G. (2020). *2019 Global Go To Think Tank Index Report*. Filadelfia, University of Pennsylvania.

Ministerio de Defensa. (2023). *Nuevas amenazas a la Seguridad Nacional*. Madrid, CESEDEN/ESFAS.

Nordhaus, W. D. (2013). The Climate Casino: Risk, Uncertainty, and Economics for a Warming World. New Haven, Yale University Press.

OECD y EUIPO. (2025). *Mapping Global Trade in Fakes 2025*. París/Alicante, OECD/European Union Intellectual Property Office (EUIPO).

Ruggie, J. G. (1992). Multilateralism: the Anatomy of an Institution. *International Organization*. 46(3), pp. 561-598.

SEPBLAC. (2024). *Memoria de actividades 2022–2023*. Madrid, SEPBLAC.

UNICRI. (2016). Organized Crime and the Legal Economy. Turín, UNICRI.

Weiss, L. (2014). America Inc.? Innovation and Enterprise in the National Security State. Ithaca, Cornell University Press.

Wendt, A. (1992). Anarchy is What States Make of It [en línea]. International Organization. 46(2), pp. 391-425. [Consulta: 2026]. Disponible en: https://www.jstor.org/stable/2706858

Wohlforth, W. C. (1999). The Stability of a Unipolar World. *International Security*. 24(1), pp. 5-41.

Capítulo segundo

Fusión nuclear, la panacea de la geopolítica energética: viabilidad, actores e impacto global

Noel Díaz Muñoz

Sumario

La fusión nuclear, tradicionalmente considerada una promesa científica a largo plazo, ha adquirido una relevancia creciente en el debate energético global. Este trabajo aborda la fusión no solo como una fuente potencial de energía limpia, sino como un elemento disruptivo con capacidad para reconfigurar las dinámicas geopolíticas. Desde un enfoque interdisciplinar que combina análisis tecnológico, económico y estratégico, el estudio evalúa su viabilidad comercial en las próximas décadas y su posible impacto sobre el orden energético internacional.

El análisis se centra en el papel de tres actores clave —la Unión Europea, Estados Unidos y China—, sin descuidar la posición de actores secundarios y no estatales. Para ello, se incorporan entrevistas con expertos del sector y datos actualizados de organismos internacionales.

Las conclusiones muestran que, pese a los avances recientes, la fusión no será competitiva a corto plazo debido a los importantes retos técnicos aún no resueltos. No obstante, su implantación a medio o largo plazo podría reducir la dependencia de combustibles fósiles, alterar los equilibrios de poder geopolítico y abrir nuevas formas de cooperación y rivalidad entre Estados.

En este sentido, la fusión nuclear, si logra consolidarse, no representará únicamente una revolución tecnológica, sino también una herramienta estratégica capaz de modificar el balance de poder global.

Palabras clave

Transición energética, Soberanía tecnológica, Seguridad energética, Diplomacia científica.

Nuclear Fusion, the Panacea of Energy Geopolitics: Feasibility, Actors, and Global Impact

Abstract

Nuclear fusion, traditionally regarded as a long-term scientific promise, has gained increasing relevance in the global energy debate. This work addresses fusion not only as a potential source of clean energy, but also as a disruptive element capable of reshaping geopolitical dynamics. From an interdisciplinary perspective combining technological, economic, and strategic analysis, it evaluates its commercial viability in the coming decades and its potential impact on the international energy order.

The analysis focuses on the role of three key actors—the European Union, the United States, and China—without neglecting the position of secondary and non-state actors. To this end, it incorporates interviews with sector experts and up-to-date data from international organizations.

The conclusions show that, despite recent advances, fusion will not be competitive in the short term due to significant unresolved technical challenges. Nevertheless, its deployment in the medium or long term could reduce dependence on fossil fuels, alter geopolitical power balances, and open new forms of cooperation and rivalry among states.

In this regard, nuclear fusion, if it succeeds in consolidating itself, will not represent merely a technological revolution, but also a strategic tool capable of modifying the global balance of power.

Key words

Energy transition, Technological sovereignty, Energy security, Scientific diplomacy.

1 Introducción

La energía constituye uno de los pilares de la configuración geopolítica y del equilibrio de poder entre las distintas potencias. Para algunos países representa su principal fuente de riqueza, mientras para otros se convierte en un factor de vulnerabilidad estructural que condiciona su soberanía y capacidad de autodeterminación.

En este contexto, la posibilidad de disponer de una fuente de energía barata, limpia, inagotable e independiente de materias primas en manos de unos pocos países se presenta como una potencial panacea para aquellos Estados dependientes de recursos energéticos externos, al permitirles reforzar su soberanía energética y modificar sustancialmente su posición estratégica en el escenario internacional.

Este trabajo combina el análisis de fuentes académicas e informes de organismos internacionales con entrevistas a expertos directamente implicados en el desarrollo de la energía de fusión. En particular, se han incorporado las contribuciones de Joaquín Sánchez, director del Laboratorio Nacional de Fusión, y de Milena Roveda, directora general de *Gauss Fusion* y presidenta de la Asociación Europea de Fusión. Sus aportaciones se utilizan a lo largo del trabajo para contextualizar los avances, las limitaciones actuales y las distintas estrategias en torno a la fusión nuclear.

1.1 La fusión nuclear

La energía de fusión se basa en la emisión de energía al unir los núcleos de dos átomos ligeros para formar uno más pesado. Se trata del proceso opuesto a la fisión nuclear, en la que el núcleo de un átomo pesado se divide en otros más ligeros.

La energía de fusión es la misma que se genera en las estrellas como el Sol, donde continuamente se fusionan átomos de hidrógeno, generando átomos de helio y una inmensa cantidad de energía en el proceso.

Sin embargo, a diferencia de la reacción de fisión, la fusión nuclear no es espontánea y requiere condiciones extremas de temperatura y presión. En el núcleo del Sol, estas condiciones se alcanzan de manera natural, con temperaturas de aproximadamente quince millones de Kelvin y presiones del orden de doscientos cincuenta mil millones de veces superiores a la Tierra. Dada la imposibilidad de alcanzar dicha presión en nuestro planeta, se

considera que la temperatura necesaria para replicar la reacción de fusión es de, al menos, cien millones de Kelvin (Barbarino, 2023).

La reacción de fusión nuclear que menos energía requiere es la del hidrógeno. Los núcleos de este elemento están compuestos por un protón y, dependiendo del isótopo, un número variable de neutrones. En concreto, en la naturaleza existen tres isótopos del hidrógeno: el protio (^{1}H), compuesto únicamente por un protón y ampliamente mayoritario; el deuterio (^{2}H), con un protón y un neutrón, presente en pequeñas cantidades, y el tritio (^{3}H), con dos neutrones, que es radiactivo e inestable y del que solo existen trazas en la naturaleza. Este último solo está disponible de forma artificial, y se produce en cantidades muy limitadas en reactores nucleares de fisión convencionales, insuficientes para sostener la demanda de tritio de una central de fusión (Krishnamurthy, 1998).

Para generar artificialmente la fusión nuclear, la reacción más adecuada es la que combina un núcleo de deuterio y otro de tritio. Esta reacción produce un núcleo de ^{4}He (helio, con dos protones y dos neutrones), libera un neutrón y genera 17,6 MeV (megaelectronvoltios) de energía.

Debido a que, como se ha visto con anterioridad, el tritio es extremadamente escaso, en principio se necesitaría alguna forma de generarlo de forma artificial. El deuterio, por su parte, es lo suficientemente abundante en la naturaleza como para poder extraerse directamente del agua común; por tanto, el agua de la Tierra sería una fuente inagotable de deuterio (Arnoux, 2011).

Preguntando al doctor Joaquín Sánchez sobre la posibilidad de producir tritio en un reactor con el propósito de utilizarlo posteriormente para producir energía en una central de fusión nuclear, este lo descartó por completo. La producción mundial de tritio, de unos 20 kg anuales, sería insuficiente para una sola central de fusión, que requeriría entre 100 y 200 kg anuales (Pearson, Antoniazzi y Nuttall, 2018). Por ello, es necesario recuperar el tritio utilizado en las centrales de fusión nuclear.

Este proceso se conoce como «cría de tritio» (*tritium breeding*) y es fundamental para el funcionamiento de una central de fusión. Dado que el tritio no se encuentra disponible de forma natural en cantidades suficientes, los propios reactores deben producirlo a medida que generan energía.

Para ello, se aprovechan los neutrones liberados durante la reacción de fusión, que al interactuar con una capa externa de litio

situada alrededor del reactor permiten obtener nuevos átomos de tritio. De este modo, el combustible utilizado puede regenerarse de forma continua dentro de la propia instalación, haciendo posible el funcionamiento prolongado de una central de fusión sin depender de suministros externos de tritio (Rubel, 2018).

1.2 Geopolítica energética

Actualmente, la producción energética constituye uno de los desafíos más importantes para la mayoría de los países, ya que no solo es imprescindible para satisfacer las necesidades cotidianas de la población, sino que, además, resulta fundamental para sectores como la industria, especialmente aquella de alta intensidad energética y para el transporte. En este sentido, la energía ha dejado de ser un mero factor económico para convertirse en un elemento central de la planificación estratégica y de la política exterior de los Estados.

A nivel global, las distintas fuentes de energía pueden agruparse en tres grandes categorías, que a menudo se representan como los vértices de un triángulo según su impacto en las emisiones de dióxido de carbono. En uno de los vértices se sitúan los combustibles fósiles de mayor intensidad emisora, como el carbón. En otro vértice, se ubican el petróleo y el gas natural, que, aunque también son fuentes fósiles, generan menores emisiones específicas que el carbón. Finalmente, el tercer vértice lo ocupan las fuentes no fósiles —la energía nuclear y las energías renovables—, que son las que presentan menores o nulas emisiones directas de CO_2 y constituyen el eje principal de la transición energética (Nakićenović y Swart, 2000).

La combinación de los tres tipos de energía en un país conforma lo que se conoce como su mix energético. La proporción relativa de uso de cada uno de los tipos de energía no responde únicamente a criterios de eficiencia o coste, sino que está condicionada por factores de carácter estructural, como el nivel de desarrollo tecnológico, la disponibilidad de recursos naturales, la capacidad industrial, las alianzas comerciales y el marco regulatorio vigente.

Asimismo, el mix energético refleja decisiones políticas de largo alcance, ya que determina el grado de dependencia exterior, la exposición a la volatilidad de los mercados internacionales y la capacidad de los Estados para adaptar su sistema energético a escenarios de crisis o disrupción. En este sentido, la composición

del mix energético no es estática, sino que evoluciona en función de cambios tecnológicos, presiones medioambientales y transformaciones geopolíticas, convirtiéndose en un indicador clave de la resiliencia energética de cada país.

La producción y el consumo de energía adquieren, por tanto, una dimensión claramente estratégica para las naciones, hasta el punto de convertirse en un elemento central de su política exterior y de seguridad. El control de recursos energéticos, de las infraestructuras asociadas y de las rutas de suministro ha sido históricamente una fuente tanto de cooperación como de conflicto, influyendo en la configuración de alianzas y tratados comerciales, así como en el estallido de conflictos internacionales.

En el contexto mundial actual, el comercio internacional de energía se concentra principalmente en los combustibles fósiles, ya que tanto las energías renovables como la energía nuclear suelen destinarse mayoritariamente al consumo interno, si bien en algunos casos se produce un intercambio limitado de electricidad entre países vecinos (Foster y Elzinga, 2015).

A pesar de la creciente importancia que tienen las energías renovables en el mix energético mundial, sus principales inconvenientes son su disponibilidad variable, su falta de adaptabilidad a la demanda y la tecnología necesaria para su almacenamiento; todo ello hace necesario contar con otras fuentes energéticas de respaldo. Por ello, los Estados mantienen un interés estratégico en fuentes de energía estables, entre las que se inscriben la energía nuclear convencional y, a largo plazo, la fusión nuclear como posible elemento transformador del sistema energético global.

1.3 Soberanía energética y seguridad

La soberanía energética es un elemento central en las políticas de las naciones, especialmente en un contexto marcado por la crisis climática, la creciente competencia geopolítica y la volatilidad de los mercados energéticos internacionales. Su objetivo fundamental es garantizar un suministro estable, seguro y asequible de energía, al tiempo que permite a los Estados definir y aplicar sus propias políticas económicas, industriales y medioambientales sin depender de forma excesiva de la voluntad de actores externos. En este sentido, la soberanía energética se ha convertido en una dimensión clave de la soberanía nacional y de la autonomía estratégica de los Estados.

La soberanía energética está estrechamente ligada a la seguridad, ya que una elevada dependencia de fuentes externas puede generar vulnerabilidades estructurales. Conflictos internacionales, sanciones comerciales, interrupciones en las cadenas de suministros o crisis de abastecimiento pueden afectar la estabilidad política, económica y social de los países dependientes de la importación de combustibles fósiles. Diversificar la matriz energética y desarrollar fuentes endógenas de energía son, por tanto, estrategias clave para mitigar estos riesgos. Además, el desarrollo de energías renovables contribuye a disminuir la exposición a las fluctuaciones de precios del petróleo y gas, y permite a los países que lideren la transición energética obtener ventajas competitivas en la economía global (Timmermann y Noboa, 2022).

En el marco de la soberanía energética, la innovación tecnológica desempeña un papel crucial. La fusión nuclear, aunque aún se encuentra en fase experimental, representa una posibilidad a largo plazo para generar energía limpia, abundante y prácticamente inagotable. Su potencial para ofrecer una fuente segura y sostenible podría redefinir los paradigmas energéticos y reducir la dependencia de combustibles fósiles y minerales críticos.

En conjunto, la soberanía energética y la seguridad persiguen garantizar la estabilidad y la autonomía de los sistemas energéticos nacionales frente a un entorno internacional cada vez más incierto. La transición a energías renovables, la descentralización de la producción y la apuesta por la innovación tecnológica constituyen pilares fundamentales para reducir vulnerabilidades y aumentar la resiliencia frente a crisis globales. En este contexto, la fusión nuclear podría representar una solución a futuro, complementando la diversificación energética y fortaleciendo la independencia de los sistemas energéticos de los Estados que consigan dominar esta tecnología.

2 Estado actual de la fusión nuclear y su impacto en la geopolítica

2.1 Condicionantes de la fusión nuclear

La viabilidad comercial de la energía de fusión depende de la superación de una serie de desafíos técnicos y materiales que aún no han sido plenamente resueltos. Aunque los principios científicos que sustentan la fusión nuclear son bien conocidos,

su traslación a un sistema energético funcional y viable continúa siendo un reto.

Este apartado expone los principales condicionantes que limitan actualmente el desarrollo de la fusión nuclear, desde las exigencias físicas de la reacción hasta la disponibilidad de combustibles, la eficiencia energética de los sistemas y la estabilidad del plasma. Estos factores condicionan su viabilidad económica y su potencial impacto geopolítico.

2.1.1 Temperatura necesaria

El principal escollo para la producción de energía de fusión, como se ha señalado previamente, es la necesidad de alcanzar las temperaturas extremas necesarias para mantener la reacción. A estas temperaturas, el hidrógeno deja de comportarse como un gas y pasa a un estado de la materia conocido como plasma. Contener dicho plasma supone un desafío, ya que no existe ningún contenedor capaz de soportar temperaturas de más de cien millones de Kelvin (Chatzis y Barbarino, 2021).

Para hacer frente a esta limitación, se han desarrollado dos aproximaciones principales para contener el plasma durante el proceso de fusión. La primera consiste en el confinamiento magnético, a través de potentes campos de este tipo que mantienen el plasma retenido sin tocar las paredes del contenedor.

La segunda aproximación es el confinamiento inercial, en el que pequeñas cantidades de combustible se comprimen a altísima velocidad, generando durante unos pocos nanosegundos las condiciones extremas necesarias para que se produzca la reacción nuclear. En este caso, la propia compresión del plasma genera simultáneamente la temperatura necesaria para la reacción de fusión. Además, al aumentar la presión del plasma, se reduce la temperatura necesaria para alcanzar la reacción (Zhou, Sadler y Hurricane, 2025).

Ambas aproximaciones presentan numerosos desafíos técnicos. En el confinamiento magnético, destacan la necesidad de mantener la estabilidad del plasma durante periodos prolongados y el control de turbulencias internas. En el caso del confinamiento inercial, los principales retos se centran en lograr una implosión perfectamente simétrica del combustible y en el control de las inestabilidades que pueden impedir una fusión eficiente.

2.1.2 Escasez del tritio

Como se ha señalado con anterioridad, el tritio es un isótopo extremadamente escaso en la naturaleza, y casi todo el que se utiliza es obtenido en pequeñas cantidades en reactores nucleares. La cría de tritio es considerada la solución más prometedora para garantizar el suministro de combustible en una futura central de fusión. Sin embargo, no está exenta de dificultades. Su principal inconveniente es la necesidad de recuperar el tritio una vez obtenido, para poder extraerlo del reactor y utilizarlo de nuevo como combustible.

Si se lograse superar este escollo tecnológico, el tritio dejaría de ser una limitación estructural. Los combustibles de la central de fusión pasarían a ser el deuterio, abundante en los océanos en unas cantidades que se podrían considerar inagotables, y el litio. En palabras del doctor Joaquín Sánchez, el litio contenido en la batería de un teléfono móvil sería suficiente para generar la energía que consume una persona durante treinta años.

2.1.3 Eficiencia de la reacción

Una de las claves para que la fusión nuclear comercial sea viable es alcanzar la mayor eficiencia posible. A diferencia de la fisión nuclear, que se produce de forma espontánea, la fusión requiere un aporte de energía y, hasta el momento, ningún experimento relacionado con la fusión ha obtenido una ganancia neta de energía. Actualmente, el reactor que ha logrado una mayor eficiencia es el *Joint European Torus* (JET), con una eficiencia del 67 % (Picot, 2021).

El reactor del *National Ignition Facility*, del que se hablará más adelante, logró en 2022, por primera vez, que una cápsula de deuterio-tritio emitiese más energía de la que absorbió. Sin embargo, este resultado omite que la energía consumida por los láseres fue muy superior, debido tanto a la poca eficiencia de funcionamiento de estos, como a las pérdidas de transmisión de energía a la cápsula de combustible, de manera que la eficiencia total se aproxima al 1 % (Clery, 2022).

Por su parte, el objetivo del ITER sí es lograr una reacción con eficiencia positiva. En concreto, su objetivo es alcanzar una eficiencia de 10:1, es decir, producir al menos diez veces la energía aportada al sistema (Picot, 2021).

2.1.4 Mantenimiento de la estabilidad del plasma (confinamiento magnético)

A diferencia de los reactores de confinamiento inercial, que buscan liberar energía en un solo instante mediante la compresión del combustible, los reactores de confinamiento magnético intentan mantener una reacción de fusión estable y continua. Para lograrlo, es necesario que el plasma, que alcanza temperaturas de decenas de millones de grados, permanezca estable y bien confinado, evitando pérdidas de energía que interrumpan el proceso (Picot, 2021).

El problema es que el plasma es una sustancia muy inestable y difícil de controlar. Tiende a moverse y deformarse dentro del reactor, pudiendo tocar las paredes y enfriarse rápidamente. Para evitarlo, se utilizan potentes campos magnéticos que mantienen el plasma flotando dentro de la cámara de vacío sin contacto con ninguna superficie.

En los *tokamaks*, los campos magnéticos se generan combinando bobinas externas y una corriente eléctrica dentro del propio plasma. Esta corriente interna es útil, pero también puede provocar inestabilidades que alteran la forma del plasma y pueden detener la reacción (Picot, 2021).

Por otro lado, los *stellarators* usan únicamente bobinas externas con una forma más compleja para generar los campos magnéticos. Esto hace que el plasma sea más estable y permita un funcionamiento continuo, aunque estos reactores son más difíciles de construir y menos eficientes en la retención del calor (Pedersen *et al*., 2016).

2.2 Futuro de la energía de fusión

Hoy en día, no existe una solución tecnológica capaz de superar de forma simultánea todas las dificultades que plantea la construcción de una central nuclear de fusión económicamente rentable.

Desde el punto de vista técnico, una central de fusión debe ser capaz de elevar la temperatura y la presión del combustible hasta valores extremos, mantener dichas condiciones durante el tiempo necesario y, al mismo tiempo, extraer una ganancia neta de energía. Todo ello debe realizarse mientras se recicla y recupera el tritio para poder seguir operando de forma indefinida,

y dentro de estructuras fabricadas con materiales capaces de soportar temperaturas de millones de grados Kelvin (Waldrop, 2024).

En las entrevistas realizadas al doctor Joaquín Sánchez y a Milena Roveda, se ha encontrado un punto de acuerdo sobre el tiempo necesario: la fusión nuclear, como fuente de energía, no será factible desde el punto de vista técnico hasta la década de 2040, como mínimo, ampliándose los plazos si se hace referencia a la construcción de reactores económicamente rentables. Roveda subraya que la primera generación de centrales de fusión deberá afrontar pérdidas económicas. Por lo tanto, es necesario conjugar inversión pública y privada. De forma irónica, Parisi y Ball (2019) afirman que «La fusión está a 20 años vista… y siempre lo estará», apuntando, además, que lograr la fusión nuclear no es una cuestión de tiempo, sino de dinero, requiriendo un importante volumen de inversión sostenido.

El principal programa mundial de fusión nuclear, el ITER, se ha visto lastrado por los sucesivos retrasos que, a su vez, han provocado importantes sobrecostes al proyecto. La continuación natural del ITER, el DEMO (*Demonstration Power Plant*), carece de fecha de construcción, financiación, y una lista cerrada de países participantes. Esta situación contrasta con la situación en Asia oriental, donde China, Japón y Corea del Sur desarrollan sus propios programas nacionales de fusión. Por su lado, Estados Unidos se vuelca en iniciativas privadas, con una mínima inversión estatal, más allá del proyecto NIF, cuyo objetivo principal no es la producción comercial de energía.

2.3 Actores

El desarrollo de la fusión nuclear implica a una amplia variedad de actores con distintos niveles de influencia, capacidades técnicas y estrategias nacionales. Este apartado se centra en aquellos actores que, sin formar parte del núcleo dominante del sistema internacional —Unión Europea, Estados Unidos y China, que serán tratados en detalle en el capítulo siguiente—, desempeñan un papel relevante en el avance de esta tecnología.

Asimismo, se aborda la creciente implicación de actores no estatales, como empresas privadas, universidades y consorcios científicos, que están contribuyendo de forma decisiva a dinamizar la carrera por la energía de fusión.

2.3.1 Corea del Sur y Japón

Japón y Corea del Sur destacan como líderes en la investigación y desarrollo de la energía de fusión nuclear, contribuyendo significativamente a proyectos internacionales y avanzando en iniciativas nacionales propias. Ambos forman parte del programa ITER, con una participación del 9,1 % cada uno (ITER, 2024).

Japón ha sido a lo largo de la historia un actor clave en la investigación en fusión. Su proyecto más emblemático es el JT-60SA, un *tokamak* superconductivo desarrollado en colaboración con la Unión Europea bajo el acuerdo «Broader Approach» (European Commission, 2023a). Este dispositivo, ubicado en Naka, alcanzó su primer plasma en octubre de 2023, convirtiéndose en el *tokamak* operativo más grande del mundo, con un volumen de plasma de ciento sesenta metros cúbicos (JT-60SA, 2024).

Corea del Sur, por su parte, ha consolidado su posición mediante el desarrollo de su dispositivo KSTAR (*Korea Superconducting Tokamak Advanced Research*), uno de los primeros *tokamaks* en incorporar imanes superconductores. Esto convierte a KSTAR en un banco de pruebas crucial para tecnologías de fusión avanzadas. Corea del Sur pretende ser capaz de construir su primera planta de fusión nuclear en la década de 2040 (Korea Institute of Fusion Energy, 2020).

Ambos países presentan una gran dependencia de las importaciones energéticas. Además, ambos países son considerados «islas eléctricas», al carecer de conexiones eléctricas internacionales, lo que les obliga a ser autosuficientes en todo momento. Esta situación es especialmente crítica para Japón, que ha reducido su producción eléctrica proveniente de centrales nucleares a la tercera parte, a raíz del accidente producido en Fukushima tras el terremoto de 2011 (IEA, 2024).

La implementación exitosa de la energía de fusión podría reducir significativamente la vulnerabilidad energética de Corea del Sur y Japón, proporcionando una fuente de energía limpia y sostenible. Además, el liderazgo en tecnologías

de fusión podría ofrecer ventajas económicas y geopolíticas, posicionando a ambos países como exportadores de tecnología y conocimientos en un campo emergente.

2.3.2 Rusia

Rusia ha sido históricamente uno de los actores más influyentes en el desarrollo de la energía nuclear, tanto en su vertiente civil como militar, y este legado se extiende al ámbito de la fusión nuclear. Durante la Guerra Fría, la Unión Soviética fue pionera en el diseño del *tokamak*, una arquitectura que aún hoy constituye la base de la mayoría de experimentos de fusión a nivel mundial (Smirnov, 2009). Esta herencia científica y tecnológica ha situado a Rusia como uno de los socios fundadores del proyecto ITER, en el que participa con una contribución del 9,1 % del total (ITER, 2024).

La experiencia rusa en materiales resistentes a la radiación y en la física de neutrones de alta energía le otorga una posición competitiva en el desarrollo de componentes críticos para ITER y para otros proyectos de fusión. No obstante, la guerra en Ucrania y las sanciones internacionales han puesto en entredicho la continuidad de esta cooperación. Aunque Rusia sigue siendo miembro formal de ITER, algunos socios han comenzado a reducir o limitar su colaboración tecnológica con entidades rusas, y las sanciones han dificultado la participación del país en el proyecto (Jack, 2022).

Desde el punto de vista energético, Rusia no comparte la urgencia de transición energética de otros países altamente dependientes de las importaciones. Posee enormes reservas de petróleo, gas y uranio, y se ha consolidado como uno de los mayores exportadores energéticos del mundo. En este contexto, la fusión nuclear no se presenta como una necesidad estratégica inmediata para garantizar su seguridad energética, sino más bien como una herramienta geopolítica y científica para mantener su estatus como potencia tecnológica.

2.3.3 Países del Golfo Pérsico

Los países del golfo Pérsico, como Arabia Saudita, Emiratos Árabes Unidos (EAU), Kuwait, Catar, Baréin y Omán, obtienen la práctica totalidad de su energía, con pequeñas excepciones, de los combustibles fósiles, principalmente petróleo y gas natural.

Entre estas excepciones se encuentra EAU, que ha iniciado en los últimos años un proyecto para construir centrales nucleares en el país, suponiendo en 2022 el 13,5 % de su producción de energía eléctrica y haciendo que los tres últimos años con registros hayan sido los primeros en su historia en que ha menguado el consumo de combustibles fósiles para electricidad (IEA, 2023a).

La exportación de combustibles fósiles es la fuente principal de financiación para estos países, representando entre el 60 % y el 84 % de sus ingresos públicos (Sanfilippo, Vermeersch y Benito, 2024). Los subsidios a los combustibles fósiles y a la electricidad desincentivan el desarrollo de fuentes de energía alternativas, sobre todo a escala comercial y doméstica.

Aunque los países del golfo Pérsico no participan directamente en proyectos internacionales de fusión nuclear como el ITER, sus fondos soberanos han invertido en tecnologías relacionadas con la fusión. Por ejemplo, EAU ha identificado la energía de fusión como un componente crítico de su estrategia de inversión, considerándola tan importante como la inteligencia artificial (IA), el espacio y las energías renovables (Alotaiba, 2024).

La transición global hacia fuentes de energía más limpias y el eventual despliegue comercial de la fusión nuclear representan una amenaza estructural para la estabilidad económica de los países del Golfo, cuya prosperidad depende en gran medida de las exportaciones de petróleo y gas. Una reducción sostenida de la demanda global de combustibles fósiles, acompañada de una caída en sus precios, podría generar desequilibrios fiscales, recortes del gasto público y tensiones sociales en Estados cuya legitimidad política se apoya, en parte, en la redistribución de rentas energéticas. Aunque algunas de estas naciones han comenzado a implementar estrategias de diversificación económica e inversión en sectores emergentes, el alcance y la profundidad de estas transformaciones siguen siendo inciertos ante un escenario de cambio acelerado en los mercados energéticos globales.

2.3.4 Actores no estatales

El desarrollo de la fusión nuclear, considerada una fuente potencialmente inagotable y limpia de energía, ha sido tradicionalmente liderado por iniciativas estatales y consorcios internacionales. Sin embargo, en las últimas décadas, actores no estatales, como empresas privadas y universidades, han emergido como prota-

gonistas clave en este ámbito, aportando dinamismo y recursos significativos al avance de esta tecnología (Brans, 2024).

La inversión privada en la fusión nuclear ha experimentado un crecimiento notable, según Milena Roveda, que la cifra en más de siete mil millones de dólares desde 2008. Este incremento refleja la confianza de inversores en el potencial de la fusión como solución energética sostenible. Empresas emergentes, como *Commonwealth Fusion Systems* (CFS), en colaboración con el Instituto Tecnológico de Massachusetts (MIT), están desarrollando reactores compactos de fusión con el objetivo de tener un prototipo operativo en 2025 (*Massachusetts Institute of Technology*, 2022). Además, *Tokamak Energy* ha recaudado ciento veinticinco millones de dólares para avanzar en su tecnología de superconductores de alta temperatura y en el desarrollo de una planta piloto de fusión (De Chant, 2024).

Una de las claves sobre la participación de la industria privada es la propiedad de las patentes. Como afirma Milena Roveda para *Science Business*, «si tienes la intención de obtener financiación privada, realmente necesitas resolver el problema de la propiedad intelectual, porque la primera pregunta de un inversor privado es: ¿quién es el dueño de la propiedad intelectual?» (Matthews, 2024). Esto contrasta con el modelo de investigación pública, en el que la propiedad intelectual suele pertenecer a los Estados participantes en los proyectos, y no a entidades privadas individuales.

Este auge de la inversión privada se ve impulsado por la creciente demanda energética, especialmente en sectores tecnológicos avanzados. La IA, por ejemplo, requiere cantidades significativas de energía, lo que ha llevado a gigantes tecnológicos a explorar la energía nuclear como una solución sostenible. La capacidad de las empresas privadas para movilizar recursos y acelerar procesos de innovación las posiciona como actores esenciales en la carrera hacia la comercialización de la fusión nuclear (Regal, 2024).

2.4 Impacto de la fusión nuclear

El desarrollo de la fusión nuclear como fuente energética no solo plantea transformaciones de carácter técnico, sino también implicaciones estructurales de gran alcance para el mercado energético, las relaciones internacionales y la distribución global del

conocimiento. Este apartado examina los principales efectos potenciales de la fusión en términos de reorganización económica, redefinición de alianzas geopolíticas y posible alteración de las desigualdades entre países.

2.4.1 Cambios en el mercado energético

La posible incorporación de la fusión nuclear como fuente energética podría transformar significativamente el mercado energético global, afectando tanto a la demanda como al precio de otras fuentes de energía. Sin embargo, como indica el doctor Joaquín Sánchez en su entrevista, el impacto que tenga la fusión nuclear en el mercado depende principalmente de su coste, tanto en la implantación (desarrollo y construcción de reactores) como en su operación. Asimismo, Milena Roveda señala que es de esperar que los costes iniciales sean elevados, pero que, con el tiempo, una vez amortizada la implantación, este precio vaya disminuyendo.

La fusión nuclear ofrece la posibilidad de generar energía limpia y prácticamente ilimitada, lo que podría disminuir la necesidad de recurrir a combustibles fósiles como el carbón, el petróleo y el gas natural. Esta transición contribuiría a la reducción de emisiones de gases de efecto invernadero y al combate del cambio climático. Sin embargo, esta disminución en la demanda de combustibles fósiles podría afectar de forma negativa a las economías de países productores que dependen en gran medida de la exportación de estos recursos (Sala, 2022).

Aunque la fusión nuclear promete ser una fuente de energía limpia y abundante, deberá competir con otras tecnologías renovables ya consolidadas, como la solar y la eólica. La viabilidad económica y la aceptación pública serán factores determinantes en la adopción de la fusión en comparación con estas alternativas.

En resumen, la implementación de la fusión nuclear tiene el potencial de provocar cambios sustanciales en el mercado energético global, desde la reducción de la dependencia de combustibles fósiles hasta la reconfiguración de las dinámicas geopolíticas y económicas. No obstante, su integración exitosa dependerá de la superación de desafíos técnicos, económicos y regulatorios, así como de su capacidad para coexistir y complementarse con otras fuentes de energía limpia.

2.4.2 Redefinición de alianzas y rivalidades

La energía de fusión nuclear tiene el potencial de transformar el panorama geopolítico mundial, reconfigurando alianzas estratégicas y rivalidades entre naciones. A medida que esta tecnología avance, resulta esencial analizar cómo podría influir en las relaciones internacionales y en la estructura del poder global.

Históricamente, la dependencia de los combustibles fósiles ha definido muchas de las alianzas internacionales. Países ricos en petróleo y gas han mantenido relaciones estratégicas con naciones consumidoras, basadas en la necesidad mutua de suministro y demanda (Ibekwe *et al*., 2024). La adopción progresiva de la fusión nuclear como fuente principal de energía podría disminuir esta dependencia, reduciendo la influencia geopolítica de los países exportadores de hidrocarburos y fomentando nuevas asociaciones basadas en la cooperación tecnológica y científica.

La implementación exitosa de la fusión nuclear podría favorecer la aparición de nuevos bloques económicos y políticos. Los países que logren avances significativos en esta tecnología podrían atraer a otras naciones interesadas en acceder a energía limpia y estable, consolidando nuevas esferas de influencia y colaboración. Este proceso podría alterar el equilibrio de poder existente, beneficiando a aquellos actores que consigan situarse en una posición de liderazgo en el ámbito de la fusión nuclear.

El descenso de la demanda de combustibles fósiles podría suponer un riesgo de pérdida de relevancia geopolítica para los países productores de hidrocarburos, obligándoles a realinear sus intereses estratégicos. Esta situación es especialmente crítica para los países de Oriente Medio, cuya influencia internacional ha estado a lo largo de la historia ligada al control de los flujos globales de petróleo y gas. La aparición de tecnologías energéticas alternativas, como la fusión nuclear, podría erosionar esta posición privilegiada y forzar a estos Estados a buscar nuevas formas de relevancia estratégica (Ibekwe *et al*., 2024).

Aunque la fusión nuclear es inherentemente más segura que la fisión en términos de residuos radiactivos y riesgos de accidentes, su desarrollo plantea preocupaciones en materia de seguridad y no proliferación. La naturaleza dual de la tecnología y ciertos materiales asociados subraya la necesidad de establecer marcos regulatorios internacionales que garanticen su uso pacífico y pre-

vengan posibles desviaciones hacia fines militares (Parisi y Ball, 2019).

En conjunto, la fusión nuclear presenta un notable potencial para redefinir alianzas y rivalidades en el escenario internacional. Si bien abre oportunidades para la cooperación y el desarrollo sostenible, también introduce desafíos relacionados con la competencia tecnológica, la seguridad y la equidad global.

2.4.3 Desigualdad y brecha tecnológica

La energía de fusión nuclear se perfila como una solución prometedora para satisfacer las crecientes demandas energéticas globales de manera sostenible y limpia. Sin embargo, el desarrollo y la eventual implementación de esta tecnología plantean desafíos significativos que podrían exacerbar las desigualdades tecnológicas y económicas entre países desarrollados y en desarrollo.

El desarrollo de reactores de fusión requiere inversiones multimillonarias, una infraestructura científica avanzada y capacidades industriales ampliamente especializadas. Los países con economías emergentes a menudo carecen de los recursos financieros, tecnológicos y humanos necesarios para participar activamente en proyectos de esta envergadura. Aunque un número creciente de países en desarrollo ha expresado interés en acceder a tecnologías nucleares avanzadas, solo una minoría dispone de la capacidad económica y de la infraestructura eléctrica necesaria para integrarlas en sus sistemas energéticos (Gondemberg, 2009). Esta situación podría dar lugar a la formación de un reducido grupo de naciones con acceso efectivo a la energía de fusión, ampliando la brecha tecnológica y limitando las oportunidades de desarrollo de aquellos países que queden al margen.

El Organismo Internacional de Energía Atómica (OIEA) desempeña un papel crucial al facilitar programas de cooperación técnica que promueven la transferencia de conocimientos y tecnología entre países desarrollados y en desarrollo. Sin embargo, la efectividad de estas iniciativas depende de la capacidad de los países en desarrollo para absorber y aplicar las tecnologías transferidas, lo que a menudo se ve obstaculizado por limitaciones estructurales y falta de infraestructura adecuada.

La energía de fusión nuclear tiene el potencial de transformar el panorama energético global, pero su desarrollo y despliegue deben gestionarse cuidadosamente para evitar la ampliación de

las brechas tecnológicas y económicas entre naciones. Es esencial fortalecer las iniciativas de cooperación internacional, garantizar una transferencia efectiva de tecnología y desarrollar capacidades locales en los países en desarrollo. Solo a través de un enfoque inclusivo y equitativo se podrá asegurar que los beneficios de la fusión nuclear contribuyan al desarrollo sostenible y a la reducción de las desigualdades a nivel mundial.

3 Principales actores de la fusión nuclear

3.1 Unión Europea

3.1.1 Producción, consumo e importación de energía

La Unión Europea es una de las zonas más industrializadas del planeta. Sin embargo, esta industrialización es, en muchas ocasiones, desigual, no solo por países, sino también con profundas desigualdades internas de los propios Estados, lo que se traduce en una gran heterogeneidad de consumos energéticos.

El sector industrial es uno de los mayores consumidores de energía, representando alrededor del 26 % del consumo final, seguido muy de cerca por el transporte, que consume aproximadamente un 25 % del total (European Environment Agency, 2024). Esta estructura contribuye a la vulnerabilidad europea ante fluctuaciones internacionales en precios energéticos y crisis geopolíticas, como la provocada por la guerra en Ucrania.

Además, a pesar de su elevado nivel de industrialización, la Unión Europea no ha logrado aumentar su producción energética interna, incrementando su dependencia del exterior. Desde 2002 hasta 2022, el porcentaje de energía proveniente del exterior ha pasado del 56,3 % al 62,5 % (Eurostat, 2024).

3.1.2 Dependencia tecnológica

La Unión Europea enfrenta un significativo desafío de dependencia tecnológica en el sector energético. Esta situación se refleja claramente en sectores clave como las energías renovables, la industria automotriz y la fabricación de componentes electrónicos críticos, entre otros. De acuerdo con Milena Roveda en su entrevista, Europa se ha quedado rezagada tecnológicamente frente

a competidores globales como China y Estados Unidos, especialmente en áreas críticas para la transición energética y digital.

Un sector especialmente relevante es el de las energías renovables, donde China ha consolidado una posición dominante en tecnologías solares y eólicas. De acuerdo con la Agencia Internacional de la Energía (IEA, 2023b), China controla más del 80 % de la producción mundial de paneles solares y casi el 70 % de componentes esenciales para turbinas eólicas. Esta dependencia genera vulnerabilidades estratégicas para la Unión Europea, dificultando su objetivo de independencia energética y tecnológica.

La situación es similar en la industria automotriz, donde Europa ha perdido protagonismo tecnológico frente a otros actores internacionales. Roveda señala que la industria automotriz europea tradicional, históricamente sólida, está siendo desplazada por la creciente penetración de vehículos eléctricos fabricados en China.

Otra área crítica es la fabricación de semiconductores, esenciales para múltiples aplicaciones tecnológicas, desde la automoción hasta infraestructuras energéticas inteligentes. Europa en la actualidad produce menos del 10 % de los semiconductores que consume, dependiendo en gran medida de proveedores en Estados Unidos y Asia, principalmente Taiwán y Corea del Sur (*European Commission*, 2025a).

La dependencia tecnológica también se manifiesta en el sector energético nuclear, donde Europa depende significativamente de la importación de uranio enriquecido y tecnologías relacionadas desde terceros países. Roveda destaca en concreto que la fusión nuclear podría reducir esta dependencia tecnológica y energética, dado que no requiere materiales críticos provenientes de regiones políticamente inestables o de competidores geopolíticos.

Por último, el retraso europeo en el desarrollo de tecnologías emergentes como la IA también incrementa su vulnerabilidad tecnológica. En su extenso reporte de 2023, Mario Draghi advierte de que Europa se enfrenta a una brecha tecnológica creciente en IA comparado con Estados Unidos y China, lo que podría repercutir negativamente en múltiples sectores económicos, incluida la gestión inteligente de redes energéticas, fundamentales para el aprovechamiento eficiente de recursos energéticos futuros como la fusión nuclear (Draghi, 2023). Precisamente, una de las claves del desarrollo de la IA es la ingente cantidad de energía que requieren sus servidores (Ritchie, 2024) por lo que la disponibilidad de una fuente de energía estable, segura y abundante, como

sería la fusión nuclear, resultaría determinante para mantener la competitividad europea en este ámbito estratégico.

3.1.3 Relación con países exportadores

Las relaciones energéticas entre la UE y los países exportadores de energía son fundamentales para entender la dinámica económica y geopolítica del continente. La elevada dependencia europea de las importaciones energéticas, que en 2022 alcanzó el 62,5 % (Eurostat, 2024), limita su autonomía estratégica y tiene profundas implicaciones políticas y económicas.

Rusia ha sido a lo largo de la historia uno de los principales proveedores energéticos de la UE, especialmente en cuanto al gas natural. Antes de la invasión rusa a Ucrania en 2022, más o menos el 40 % del gas importado por la UE provenía de Rusia (European Council, 2025). Esta fuerte dependencia generó vulnerabilidades críticas, limitando la capacidad de maniobra de la UE y condicionando sus políticas exteriores y domésticas.

Noruega, que suministra alrededor del 30 % del gas natural consumido en Europa, es otro socio clave para la UE (European Council, 2025). Las relaciones energéticas entre ambas partes se caracterizan por una cooperación estable y duradera, basada en acuerdos claros y transparentes que contribuyen significativamente a la seguridad energética europea.

Estados Unidos se ha consolidado recientemente como un proveedor estratégico de gas natural licuado (GNL), llegando a cubrir el 20 % de las importaciones europeas de este recurso en 2023 (European Council, 2025). El incremento de las importaciones desde EE. UU. refleja una clara estrategia europea orientada a diversificar sus fuentes energéticas, reducir la dependencia de proveedores como Rusia y reforzar la alianza transatlántica. Esta cooperación energética no solo mejora la seguridad del suministro, sino que también tiene implicaciones positivas para las relaciones diplomáticas generales entre la UE y EE. UU., facilitando una coordinación más amplia en ámbitos políticos y económicos (European Commission, 2024a).

Por otro lado, los países del golfo Pérsico y Oriente Medio continúan desempeñando un papel esencial en el suministro de petróleo a Europa, proporcionando flexibilidad y estabilidad relativa en el mercado global debido a su capacidad para ajustar la producción rápidamente ante fluctuaciones económicas. Estas rela-

ciones implican un delicado equilibrio diplomático, donde la UE busca mantener acuerdos comerciales favorables mientras gestiona consideraciones geopolíticas complejas asociadas a cuestiones de estabilidad regional, derechos humanos y conflictos locales (European Commission, 2023b).

En definitiva, la fuerte dependencia energética europea tiene importantes consecuencias económicas y geopolíticas. Las crisis derivadas de interrupciones en el suministro han evidenciado la necesidad urgente de diversificar fuentes de energía y fortalecer la autonomía estratégica. La apuesta por el desarrollo de energías renovables y potencialmente la fusión nuclear se presentan como opciones esenciales para reducir la vulnerabilidad energética europea y fortalecer su posición internacional.

3.1.4 Tensiones internas debidas a la energía

La energía representa uno de los principales factores de tensión interna dentro de la Unión Europea, especialmente debido a las diferencias sustanciales entre Estados miembros respecto a sus matrices energéticas, dependencia de importaciones y objetivos en materia de transición energética. Estas tensiones surgen de múltiples causas, entre ellas la disparidad en infraestructuras, la desigualdad económica y las diferentes prioridades políticas de cada Estado miembro, lo que dificulta el consenso en políticas energéticas comunes.

Una fuente importante de tensiones internas es la disparidad en la dependencia energética entre países europeos. Algunos países, como Alemania o Italia, tienen altos niveles de dependencia de importaciones energéticas, especialmente en hidrocarburos, mientras otros, como Francia, tienen una mayor autonomía gracias a una significativa producción nuclear interna (Eurostat, 2024). Estas diferencias han dificultado tradicionalmente una posición europea unificada frente a crisis energéticas internacionales, evidenciado por las dificultades para responder colectivamente durante la reciente crisis derivada de la invasión rusa de Ucrania (European Council, 2024).

El aumento de precios de la energía también ha contribuido significativamente a estas tensiones. La crisis energética reciente ha generado protestas sociales y conflictos políticos internos en países como España, Francia e Italia, reflejando descontento ciudadano ante el creciente coste de vida provocado por los altos precios energéticos. Estas situaciones han empujado a varios

gobiernos a adoptar medidas de intervención en los mercados energéticos, a veces contradiciendo el marco regulatorio comunitario, lo que genera fricciones adicionales entre Bruselas y las capitales nacionales.

3.1.5 La Unión Europea frente al cambio climático y la transición energética

La Unión Europea (UE) se ha consolidado como líder global en la acción climática, adoptando un enfoque único frente a otras grandes economías. Cuenta con una estrategia conjunta —el Pacto Verde Europeo— que guía a sus veintisiete países hacia la neutralidad climática en 2050. Esta meta (ser el primer continente climáticamente neutro) está consagrada por ley mediante la Ley Europea del Clima, que fija objetivos vinculantes de reducción de emisiones de al menos 55 % para 2030 y neto cero para 2050 (Ministerio para la Transición Ecológica y el Reto Demográfico, 2021). No obstante, alcanzar estos objetivos exige transformar profundamente un sistema energético todavía marcado por dependencias externas y limitaciones estructurales.

La Comisión Europea señala que el ITER ejemplifica el compromiso a largo plazo de la UE con la neutralidad climática de 2050. Si la fusión alcanza sus promesas, podría incorporarse al mix energético europeo en la segunda mitad de siglo como una fuente segura, sin carbono y prácticamente inagotable, complementando a las energías renovables en la consecución de los objetivos climáticos (European Commission, 2021).

3.1.6 Interés estratégico en la fusión nuclear

La UE considera la energía de fusión nuclear un pilar estratégico a largo plazo dentro de sus políticas energética, climática y tecnológica. A diferencia de la fisión, la fusión promete ser segura, sostenible y prácticamente libre de emisiones de carbono, sin riesgo de reacción descontrolada ni residuos radiactivos de alta actividad a muy largo plazo.

La capacidad de la fusión de generar enormes cantidades de energía con cantidades diminutas de combustible, y el uso de isótopos abundantes (deuterio extraído del agua de mar y litio para producir tritio) en lugar de combustibles fósiles importados, reducirían drásticamente la dependencia de Europa de proveedores externos. La participación europea en proyectos de fusión

se concibe como una apuesta por una tecnología disruptiva que podría integrar el mix energético europeo en la segunda mitad del siglo (European Commission, 2025b), complementando a las energías renovables para formar un sistema eléctrico libre de carbono.

3.1.7 Iniciativas y cooperación internacional

El liderazgo europeo en fusión nuclear se materializa a través de grandes iniciativas de investigación y acuerdos de cooperación internacional. Bajo el paraguas del Tratado Euratom (1957), la UE ha coordinado durante décadas los esfuerzos de sus Estados miembros en materia nuclear, impulsando la investigación en fusión desde sus primeras etapas (European Commission, 2021). La UE desempeña un papel protagonista en ITER, al aportar aproximadamente el 45 % de la financiación total del proyecto (ITER, 2024).

La UE considera a ITER pieza clave de su hoja de ruta hacia la energía de fusión comercial, y, por ello, las instituciones europeas y los Estados miembros han mantenido su compromiso pese a los desafíos. En 2018, el Consejo de la UE reafirmó el apoyo europeo unánime a la «exitosa finalización de ITER», subrayando su carácter esencial para la realización de la fusión en el largo plazo, e instó a garantizar los fondos necesarios en los presupuestos plurianuales sucesivos, que alcanzan los 4500 millones de euros en total para el ciclo 2021-2027 (Fusion for Energy, 2018).

3.1.8 Financiación y regulación

El compromiso de la UE con la fusión nuclear se refleja en un sostenido apoyo financiero y en la adaptación progresiva de sus marcos regulatorios para viabilizar esta tecnología. En términos de financiación, la UE mantiene un flujo constante de inversión multimillonaria para la investigación en fusión y la construcción de grandes instalaciones. El capítulo más oneroso de la financiación recae en ITER, dada su escala sin precedentes. En el Marco Financiero Plurianual 2021-2027, la UE asignó 5610 millones de euros para cubrir su contribución a ITER durante dicho periodo (European Commission, 2024b).

Por otro lado, a medida que la fusión avanza hacia la fase de demostración, surge la necesidad de un marco regulatorio y normativo adecuado. Actualmente, las instalaciones de fusión en

Europa (como JET o futuras plantas experimentales) operan bajo reglamentaciones nucleares nacionales e internacionales diseñadas principalmente para la fisión, ya que no existe aún un marco legal específico de la UE para regular la energía de fusión. Sin embargo, la naturaleza distinta de la fusión —sin riesgo de accidente en cadena catastrófico y con residuos radiactivos de vida corta y media— ha llevado a plantear la conveniencia de diferenciar su regulación de la de la energía nuclear convencional.

3.1.9 Impacto geopolítico, económico y energético de la fusión nuclear

Si la energía de fusión cumple sus promesas, las repercusiones para la UE serían profundas en los ámbitos geopolítico, económico y del sistema energético. En el plano energético y climático, la disponibilidad de reactores de fusión comercial en la segunda mitad del siglo XXI brindaría a Europa una fuente prácticamente inagotable de energía limpia. Esto complementaría y consolidaría la transición hacia un sistema descarbonizado (European Commission, 2024b): la fusión podría suplir los periodos de indisponibilidad de las renovables, actuando como respaldo libre de carbono en inviernos largos o noches prolongadas.

Desde la perspectiva geopolítica y de seguridad energética, la implantación de la fusión tendría un impacto transformador para Europa. Lograr la independencia de recursos energéticos extranjeros cambiaría las relaciones exteriores de la UE: países tradicionalmente proveedores de hidrocarburos podrían perder peso estratégico si la demanda europea de gas y petróleo disminuye drásticamente en favor de la fusión y otras fuentes limpias. Europa fortalecería su posición al no estar supeditada a importaciones de energía con precios volátiles, ganando margen de maniobra en su política exterior.

En el aspecto económico-industrial, las oportunidades son igualmente notables. El desarrollo de la energía de fusión configura un sector industrial de altísimo valor tecnológico, que abarca desde ingeniería avanzada hasta nuevas industrias de suministro de componentes. La UE ya está experimentando beneficios económicos tempranos gracias a ITER: miles de empleos especializados han sido creados y empresas europeas han ganado contratos de ingeniería civil, fabricación de imanes superconductores, sistemas criogénicos, entre otros (Rademaekers *et al*., 2018).

3.2 Estados Unidos

3.2.1 Producción, consumo y comercio de energía

Estados Unidos es una de las economías más grandes e industrializadas del planeta, y también uno de los mayores consumidores de energía a nivel mundial. Esta demanda energética es resultado tanto de su fuerte base industrial como de su elevado nivel de vida, su modelo urbano extensivo y su sistema de transporte muy dependiente del vehículo privado.

En contraste con la Unión Europea, Estados Unidos mantiene un alto grado de autosuficiencia energética. Gracias al desarrollo de fuentes no convencionales como el *shale oil* y el *shale gas*, ha pasado de ser un importador neto a convertirse en uno de los principales exportadores de energía del mundo. Esta situación le otorga una posición geopolítica más ventajosa y una menor vulnerabilidad frente a crisis energéticas internacionales (EIA, 2024).

Estados Unidos combina un elevado consumo total y per cápita con una capacidad interna de producción que le permite reducir su exposición externa. Sin embargo, esta situación de fortaleza global no elimina las disparidades territoriales ni los desafíos de sostenibilidad que enfrenta a largo plazo.

3.2.2 Innovación y liderazgo tecnológico

Estados Unidos se posiciona como uno de los líderes globales en innovación tecnológica en el ámbito energético, sustentado por una potente inversión pública y privada en investigación, desarrollo e implementación de nuevas tecnologías. Uno de los campos en los que Estados Unidos ha destacado es en el almacenamiento energético a gran escala. El país ha experimentado una rápida expansión en la instalación de baterías estacionarias, alcanzando una capacidad instalada de más de veintiséis gigavatios en 2024. Esta cifra representa un crecimiento significativo del 66 % con respecto al año anterior (EIA, 2024). La proliferación de estas baterías facilita la integración eficiente de fuentes renovables intermitentes, como la energía solar y eólica, fortaleciendo la estabilidad y flexibilidad de la red eléctrica nacional.

Adicionalmente, el país destaca en tecnologías emergentes como los reactores nucleares modulares, que se perfilan como

una alternativa prometedora para la generación estable y baja en emisiones. Proyectos piloto liderados por el Departamento de Energía y empresas privadas están desarrollando esta tecnología para facilitar una futura transición hacia un sistema eléctrico más descarbonizado (Baldwin *et al*., 2025).

Finalmente, Estados Unidos está invirtiendo en tecnologías de captura y almacenamiento de carbono, promoviendo proyectos de infraestructura específicos que buscan reducir significativamente las emisiones industriales y energéticas. Estas iniciativas se encuentran en fase avanzada de investigación y desarrollo, con apoyo financiero sustancial del gobierno federal, apuntando a consolidar el liderazgo tecnológico del país en la transición energética global.

3.2.3 Geopolítica energética: aliados y rivales

Estados Unidos desempeña un papel clave en la geopolítica energética global debido a su posición como importante productor, consumidor y exportador de energía. Su autosuficiencia energética relativa, especialmente gracias al auge del *shale gas* y *shale oil*, proporciona al país un margen estratégico considerable, reduciendo significativamente su dependencia de importaciones de energía y aumentando su influencia política y económica internacional (EIA, 2024).

Canadá es el principal socio energético de Estados Unidos, suministrando alrededor del 62 % del total de petróleo importado en 2023, así como una porción significativa del gas natural consumido en el país (EIA, 2024). Esta estrecha colaboración se basa en una infraestructura compartida robusta, incluyendo oleoductos y gasoductos transfronterizos, que facilita un suministro energético estable y seguro, fortaleciendo la alianza estratégica norteamericana y proporcionando estabilidad geopolítica.

Por otro lado, México también es un socio energético relevante, especialmente en cuanto a las exportaciones estadounidenses de gas natural y productos refinados de petróleo. El comercio energético con México no solo tiene implicaciones económicas significativas, sino que también juega un papel importante en la estabilidad regional y en las relaciones diplomáticas bilaterales entre ambos países.

La competencia estratégica en el ámbito energético enfrenta a Estados Unidos principalmente con Rusia y países de Oriente

Medio como Arabia Saudita. El rápido aumento de las exportaciones estadounidenses de GNL ha generado tensión comercial y geopolítica con Rusia, al reducir su tradicional dominio en los mercados energéticos europeos. Esta dinámica ha contribuido a realinear alianzas, reforzando vínculos con aliados europeos como parte de una estrategia conjunta para disminuir la dependencia energética europea respecto a Rusia (Escribano, 2025).

En Oriente Medio, Estados Unidos mantiene una relación compleja con Arabia Saudita y otros productores del golfo Pérsico. Aunque existe cooperación estratégica para mantener la estabilidad del mercado petrolero mundial, también se producen fricciones derivadas de diferencias políticas y diplomáticas, incluyendo temas relacionados con derechos humanos y conflictos regionales. Esta situación obliga a Estados Unidos a equilibrar cuidadosamente sus intereses energéticos y geopolíticos en la región (Cook, 2024).

Finalmente, la creciente rivalidad tecnológica y energética con China representa un desafío estratégico significativo. China, líder global en tecnologías renovables, compite directamente con Estados Unidos en mercados clave como las energías limpias y la infraestructura energética crítica, lo que acentúa la competencia tecnológica y geopolítica entre ambos países (IEA, 2023b).

3.2.4 El pragmatismo estadounidense ante la transición energética

Estados Unidos afronta la transición energética con un enfoque descentralizado y marcadamente pragmático. Sin una ley federal integral que imponga la neutralidad climática, el país presenta un panorama heterogéneo, con estados líderes como California o Nueva York que implementan ambiciosas políticas de descarbonización, mientras otros muestran una resistencia considerable a modificar sus modelos energéticos tradicionales (Setzer *et al*., 2024).

Este enfoque se ha consolidado con la aprobación de *la Inflation Reduction Act* en 2022, considerada la mayor inversión climática de la historia del país. La ley destina cerca de 370 000 millones de dólares a tecnologías limpias a través de créditos fiscales, subvenciones y ayudas directas orientadas a la expansión de las energías renovables, la electrificación del transporte, el almacenamiento energético, el hidrógeno limpio y la captura y almacenamiento de carbono (CCS) (U.S. Department of Energy, 2023). En lugar de imponer objetivos vinculantes de reducción de

emisiones, esta política busca transformar el sistema energético mediante la atracción de capital privado y el desarrollo de nuevos mercados (Hughes, 2022).

No obstante, la política climática estadounidense ha estado marcada por importantes oscilaciones derivadas del cambio de signo político en la Casa Blanca. Estados Unidos ha abandonado formalmente en varias ocasiones compromisos internacionales clave, como el Protocolo de Kioto (en 2001) y el Acuerdo de París (en 2020 y 2025). Estas rupturas reflejan la polarización interna sobre el cambio climático y generan incertidumbre a nivel global sobre el compromiso a largo plazo del país con la descarbonización (The White House, 2025).

Pese a ello, EE. UU. mantiene una estrategia sólida de apoyo a la innovación tecnológica, especialmente en sectores emergentes como la energía de fusión nuclear. Esta combinación de pragmatismo, incentivos económicos y liderazgo tecnológico refleja el enfoque distintivo de Estados Unidos en la transición energética, en la que la fusión nuclear se perfila como una apuesta estratégica a largo plazo.

3.2.5 Interés y estrategias en fusión nuclear

El interés de Estados Unidos en la energía de fusión nuclear se ha visto revitalizado por su potencial como fuente abundante y libre de carbono para asegurar la transición energética y el liderazgo tecnológico del país. La pasada administración Biden destacó la fusión como una tecnología disruptiva para alcanzar las metas de electricidad 100 % limpia en 2035 y cero emisiones netas en 2050, así como para reforzar el liderazgo de EE. UU. en la economía del siglo XXI (The White House, 2024).

Un aspecto relevante de la estrategia estadounidense sobre la fusión nuclear se relaciona directamente con la seguridad nacional, en particular con el Laboratorio Nacional Lawrence Livermore (LLNL). El Gobierno de EE. UU. considera el LLNL no solo como un centro de investigación energética, sino también como un «campo de pruebas virtual» para armas nucleares. La técnica empleada en el LLNL, conocida como confinamiento inercial, permite estudiar y simular fenómenos físicos similares a los de una detonación termonuclear, pero en condiciones controladas y de laboratorio, sin incumplir el Tratado de Prohibición Completa de Ensayos Nucleares (CTBT). Esto proporciona a Estados Unidos información clave para mantener la seguridad,

fiabilidad y eficacia de su arsenal nuclear sin realizar explosiones reales, reforzando así la conexión estratégica entre la investigación en fusión nuclear civil y la política de defensa del país (Mann y Wiper, 2022).

Este enfoque integrado refleja la prioridad estratégica que Washington otorga a la fusión: además de ser parte esencial de su agenda climática, la considera un ámbito en el que debe asegurar el liderazgo frente a otros competidores globales, dada la creciente percepción de que «la fusión se ha convertido en una carrera global». Al mismo tiempo, esta visión estratégica también se conecta directamente con la seguridad nacional.

3.2.6 Proyectos públicos y privados en fusión nuclear

Estados Unidos cuenta con una amplia gama de proyectos de fusión, tanto de iniciativa pública como privada, que conjuntamente conforman el ecosistema de I+D en este campo. En el sector público, el Departamento de Energía (DOE) financia laboratorios nacionales y universidades líderes en ciencia de plasmas y fusión, así como la participación estadounidense en el proyecto internacional ITER en Francia (Miller, 2023).

En paralelo, el sector privado estadounidense de fusión ha florecido en la última década, atrayendo inversiones de capital riesgo sin precedentes. Existen actualmente decenas de *startups* y empresas enfocadas en lograr reactores de fusión comercial, con enfoques diversos: desde *tokamaks* compactos de alto campo hasta conceptos alternativos como los reactores de haces de partículas de TAE Technologies o los sistemas de compresión magnética acelerada de *Helion Energy*.

Para aprovechar sinergias, el Gobierno ha lanzado programas de colaboración público-privada como INFUSE (*Innovation Network for Fusion Energy*) y el *Milestone-Based Development Program*, que apoyan con fondos compartidos proyectos en los que laboratorios nacionales trabajan junto a empresas emergentes (The White House, 2023). Esta integración de esfuerzos públicos y privados es un rasgo distintivo de la estrategia estadounidense: busca reproducir en la fusión el modelo de éxito de otras industrias tecnológicas, combinando la inversión gubernamental en investigación básica con la agilidad e innovación del sector privado.

3.2.7 Financiación y marco regulatorio de la fusión en EE. UU.

EE. UU. es un caso único de financiación de la investigación de fusión, al conjugar generosas subvenciones públicas con una fuerte apuesta por parte de la empresa privada. Esta convergencia de capital público y privado está creando un ecosistema robusto; no obstante, se reconoce que aún podrían requerirse decenas de miles de millones de dólares adicionales para llevar la fusión desde los experimentos actuales hasta plantas comerciales a gran escala (Qihan Zou, 2024).

En el plano regulatorio, Estados Unidos ha tomado pasos importantes para adecuar sus normas al carácter particular de las instalaciones de fusión, diferenciándolas de los reactores nucleares de fisión. Hasta fechas recientes, no existía un marco específico y las plantas de fusión podían quedar sujetas por analogía a la estricta regulación nuclear convencional. Sin embargo, en 2023 la Comisión Reguladora Nuclear (NRC) decidió clasificar los reactores de fusión proyectados bajo la categoría de «materia prima o derivada» en lugar de tratarlos como «instalaciones de utilización» tipo fisión. Esto implica requisitos de licenciamiento más flexibles y proporcionales al menor riesgo de la fusión, dado que en esta no existe posibilidad de reacción en cadena descontrolada ni se emplean materiales fisibles que puedan usarse directamente en armas (Zhang, 2024).

En la práctica, este marco regulatorio adaptado reduce barreras administrativas y costos para las empresas que desarrollan prototipos de fusión, al tiempo que mantiene las precauciones necesarias sobre el manejo de tritio y la seguridad radiológica de los componentes activados. Con estas medidas, EE. UU. busca equilibrar seguridad y promoción de la innovación, evitando que una sobrerregulación frene el incipiente sector de la fusión.

3.2.8 impacto geopolítico, económico y energético de la fusión nuclear

El desarrollo exitoso de la fusión nuclear tendría consecuencias de gran alcance para Estados Unidos en los ámbitos geopolítico, económico y energético. En primer lugar, consolidaría el liderazgo geoestratégico estadounidense. Dominar la tecnología de fusión supone asegurar una posición privilegiada en la futura estructura de poder global, al controlar una fuente de energía prácticamente inagotable y limpia. Varios analistas destacan que la nación que primero logre implementar reactores de fusión operativos podría dominar el mercado energético del futuro, obteniendo una ven-

taja de primer jugador difícil de revertir por décadas (Qihan Zou, 2024), y permitiendo proyectar su influencia mediante la exportación de tecnología y el establecimiento de acuerdos energéticos.

En términos económicos, la fusión nuclear exitosa representaría un salto industrial y de competitividad para Estados Unidos. Como nuevo sector energético, crearía posiblemente cientos de miles de empleos especializados y empresas alrededor del diseño, construcción y mantenimiento de plantas de fusión, con efectos multiplicadores en la economía.

En el plano energético y medioambiental, el impacto para EE. UU. sería igualmente transformador. La incorporación de la fusión al mix eléctrico permitiría a Estados Unidos alcanzar sus metas climáticas de 2050 con mayor facilidad, al proveer energía firme (no intermitente) y libre de emisiones de CO_2 que complementaría a las fuentes renovables (Qihan Zou, 2024).

3.3 China

3.3.1 crecimiento económico y consumo energético

Desde finales del siglo xx, China ha experimentado un crecimiento económico sin precedentes, impulsando una rápida industrialización y urbanización y elevando de manera significativa la demanda energética nacional (Huld, 2023). El consumo de energía refleja claramente esta dinámica. Mientras que el uso residencial se ha mantenido relativamente estable, el transporte y, sobre todo, la industria ha concentrado el grueso del aumento del consumo energético, en línea con el peso creciente del sector industrial en la economía china.

El mix energético del país ha estado dominado tradicionalmente por los combustibles fósiles, en particular el carbón. En 2023, este representaba el 60,8 % de la producción eléctrica, frente a un 3,1 % del gas natural. Aunque en los últimos años China ha incrementado de forma notable su capacidad en energías renovables, la magnitud de la demanda energética mantiene al carbón como pilar central del sistema.

Como resultado, China continúa ampliando su capacidad térmica para sostener el crecimiento económico y cubrir las necesidades industriales y residenciales, evidenciando la persistente depen-

dencia de los combustibles fósiles en un contexto de consumo energético a gran escala.

3.3.2 Seguridad energética y proyección internacional

La búsqueda de seguridad energética por parte de China implica inversiones significativas en campos de petróleo y gas en el extranjero, particularmente en África y Asia Central. Estos esfuerzos están diseñados para establecer cadenas de suministro a largo plazo y reducir la vulnerabilidad a interrupciones geopolíticas. Como indican Öğütçü y Öğütçü, una de las claves de esta estrategia incluye el desarrollo de una red de oleoductos y gaseoductos terrestres con países como Kazajistán, Turkmenistán y Uzbekistán para reducir su dependencia del transporte a través del estrecho de Malaca (Öğütçü y Öğütçü, 2017).

Estas inversiones generan relaciones asimétricas de dependencia, en las que los países proveedores dependen crecientemente del mercado chino, mientras Pekín consolida su acceso a recursos estratégicos y refuerza su poder de negociación regional.

La diplomacia energética de China refleja un enfoque dual: asegurar recursos para impulsar su crecimiento económico mientras se posiciona como un actor central en la gobernanza energética global. Al participar activamente en iniciativas energéticas internacionales y fomentar asociaciones bilaterales y multilaterales, China busca moldear un orden energético global que acomode sus intereses y promueva la estabilidad en los mercados energéticos.

3.3.3 Transición energética

La transición energética de China es un componente esencial de su estrategia nacional para equilibrar el crecimiento económico con la sostenibilidad ambiental y la seguridad energética. Como el mayor consumidor y productor de energía a nivel mundial (IEA, 2022), China ha implementado políticas y realizado inversiones significativas para transformar su matriz energética hacia fuentes más limpias y renovables.

Internamente, China ha adoptado políticas para equilibrar el crecimiento económico con la sostenibilidad ambiental. La promulgación de leyes energéticas recientes refleja este compromiso, promoviendo el desarrollo de energías renovables y apuntando hacia la neutralidad de carbono. Entre esta legislación, destaca la última ley

de energía, efectiva desde inicios de 2025, cuyo fin último es alcanzar la neutralidad de carbono en el año 2060 (Pozzi, 2025).

Para alcanzar la neutralidad de carbono en 2060, se estima que China necesitará instalar alrededor de 10 000 GW de capacidad de energías renovables, un objetivo que requerirá una expansión masiva de las infraestructuras y una inversión continua en tecnologías limpias (Zhongying y Sandholt, 2025). Sin embargo, esta transición convive con una fuerte inercia fósil: pese al despliegue masivo de renovables, China continúa ampliando su capacidad de generación a carbón para garantizar la estabilidad del sistema eléctrico y sostener el crecimiento económico.

Asimismo, es de destacar la fuerte apuesta por la energía nuclear, por la cual China pretende aumentar su generación de energía nuclear desde 10 GW hasta 277 GW entre 2010 y 2050 (IEA, 2023c). Esta estrategia explica, en parte, el interés posterior de China por la energía de fusión, apoyado en una base industrial y tecnológica ya consolidada.

3.3.4 Interés estratégico en la fusión nuclear

China considera la energía de fusión nuclear como un componente estratégico de su desarrollo a largo plazo, tanto para garantizar su seguridad energética como para consolidar su posición tecnológica global. Como gran importador neto masivo de petróleo y gas, Beijing percibe la dependencia energética externa como una vulnerabilidad de seguridad nacional (Qihan Zou, 2024). En este contexto, la fusión nuclear ofrecería, de lograrse comercialmente, una fuente casi inagotable de energía autóctona, reduciendo de forma estructural su exposición a los mercados internacionales de combustibles fósiles.

El interés de China en la fusión también está motivado por objetivos medioambientales y económicos internos. El país sigue dependiendo fuertemente del carbón para su generación eléctrica —más de la mitad de la electricidad china aún proviene de centrales a carbón—, lo que genera graves problemas de contaminación atmosférica y emisiones de CO_2. En este contexto, la fusión aparece en la planificación china como una solución a largo plazo para reemplazar gradualmente las plantas de carbón y satisfacer la creciente demanda energética con energía limpia constante.

Finalmente, la fusión representa para China una oportunidad estratégica de liderazgo tecnológico. El Gobierno chino entiende

que adelantarse en su desarrollo le permitiría dictar estándares, acumular propiedad intelectual y obtener una ventaja industrial competitiva difícil de revertir, reforzando su posición en la próxima generación de tecnologías energéticas.

3.3.5 Capacidades tecnológicas y estratégicas chinas en fusión nuclear

China se ha posicionado como un actor central en la carrera por la fusión nuclear, impulsando diversos proyectos que combinan la investigación científica con objetivos geoestratégicos. En su más reciente plan quinquenal, Beijing situó la fusión nuclear entre las máximas prioridades nacionales, respaldándola con una inversión estimada de mil quinientos millones de dólares anuales (aproximadamente el doble del presupuesto de EE. UU. en investigación de fusión nuclear) (BGR Group, 2024).

Uno de los pilares de este esfuerzo es el *Experimental Advanced Superconducting Tokamak* (EAST), un reactor experimental ubicado en Hefei y operado por la Academia China de Ciencias. Inaugurado en 2006 como el primer *tokamak* totalmente superconductivo de sección no circular en el mundo (BGR Group, 2024), EAST ha servido desde entonces de plataforma de pruebas abierta para científicos chinos e internacionales.

En paralelo, China está desarrollando el *China Fusion Engineering Test Reactor* (CFETR), concebido como eslabón intermedio entre los experimentos actuales y una futura planta de demostración comercial. El diseño de ingeniería del CFETR se completó en 2020 y las autoridades planean iniciar su construcción en el transcurso de esta década (IAEA, 2022).

A esta dimensión doméstica se suma la participación china en proyectos internacionales como ITER, que refuerza su perfil como actor científico cooperativo y le permite acumular experiencia en grandes programas de fusión a escala global.

3.3.6 Impacto geopolítico de la fusión nuclear

El posible advenimiento de la energía de fusión comercial en China tendría profundas implicaciones geopolíticas, alterando equilibrios de poder y dinámicas económicas a nivel global. En primer lugar, si China logra dominar la tecnología de fusión, transformaría su posición en el sistema energético mundial: pasaría de ser el mayor importador de recursos energéticos a convertirse en

un exportador neto de tecnología y quizás de energía (mediante proyectos en terceros países). A nivel doméstico, la fusión le permitiría a China alcanzar sus objetivos de desarrollo sostenible, garantizando energía abundante sin los estrangulamientos de importación que hoy condicionan su seguridad nacional.

Un éxito chino en fusión daría un impulso enorme al poder blando del país: sería presentado como un triunfo del modelo chino de inversión a largo plazo en ciencia e ingeniería, y como una contribución de China a la humanidad (Carayannis *et al*., 2021) Pekín podría ofrecer reactores de fusión o asistencia técnica a otras naciones, especialmente en el sur global, como parte de iniciativas de cooperación, potencialmente dentro del marco de la Iniciativa de la Franja y la Ruta (BRI).

En conclusión, la apuesta de China por la fusión nuclear no es solamente científica o económica, sino geopolítica en esencia. El país vislumbra la fusión como un disruptor del orden energético global que puede jugar a su favor: una vez dominada, le permitiría reconfigurar las relaciones de poder basadas en energía, ganar autonomía estratégica y proyectar su poder de nuevas formas.

4 Conclusiones

Al finalizar este trabajo, el consenso entre las fuentes consultadas y los expertos entrevistados es claro: la energía de fusión no estará lista para su uso práctico antes de 2045. Aunque hoy se conocen bien los principios científicos que la hacen posible y existen numerosos proyectos —tanto públicos como privados— dedicados a desarrollarla, todavía quedan por resolver importantes desafíos técnicos. Entre ellos se encuentran la dificultad de mantener el plasma a temperaturas extremas durante largos periodos de tiempo, la necesidad de regenerar y recuperar el tritio que sirve como combustible, o el desarrollo de materiales capaces de soportar las condiciones extremas del interior de un reactor de fusión. Incluso en el escenario más optimista, en el que se logre poner en marcha una primera generación de reactores funcionales hacia mediados de siglo, su rentabilidad económica no se alcanzaría hasta bien entrada la segunda mitad del siglo XXI.

Por lo tanto, aunque la energía de fusión podría alcanzar la viabilidad técnica en los próximos veinte años, los elevados costes de desarrollo e implantación hacen muy improbable que esta sea rentable económicamente.

Queda por determinar si el éxito se alcanza a través de un liderazgo del sector industrial, con financiación público-privada, como proponen empresas como *Gauss Fusion*, o si serán los grandes proyectos de investigación estatal y de colaboración internacional los que logren el objetivo final. El análisis realizado apunta a que la balanza se inclina hacia la visión de Joaquín Sánchez, en línea con autores como Parisi y Ball, quienes subrayan el papel central del liderazgo público en el éxito de esta tecnología. La gran inversión de actores como China y la Unión Europea, sumada a la incertidumbre a corto plazo de los proyectos privados, apunta a que la vía más probable sea la impulsada por estrategias estatales a largo plazo. No obstante, es importante destacar la importancia de la industria a la hora de construir las centrales nucleares, una vez asegurada la viabilidad comercial de la energía de fusión.

Desde una perspectiva geopolítica y energética, la fusión nuclear destaca por su enorme potencial disruptivo. No obstante, el alcance real de su impacto dependerá de cómo y hasta qué punto llegue a implementarse, así como de los marcos políticos, tecnológicos e institucionales en los que se integre.

La posibilidad de generar grandes cantidades de energía limpia y constante utilizando cantidades mínimas de combustible —a partir de recursos ampliamente disponibles como el deuterio y el litio— constituye una oportunidad estratégica sin precedentes para aquellos Estados que consigan dominar esta tecnología.

En el caso de la Unión Europea, la fusión se presenta como una herramienta clave para reducir drásticamente la dependencia energética del exterior, garantizar la estabilidad del suministro y reforzar su competitividad industrial a largo plazo. Esta apuesta se refleja claramente en el proyecto ITER, así como su liderazgo en coordinación científica mediante iniciativas como EUROfusion, que evidencian un compromiso sostenido en el tiempo.

Este compromiso no se limita al ámbito europeo. La implicación de la Unión Europea en proyectos internacionales como el JT-60SA en Japón o el K-STAR en Corea del Sur subraya su voluntad de alcanzar el liderazgo científico y mantener la cooperación internacional en el desarrollo de la fusión nuclear. Además, su esfuerzo regulatorio específico para adaptar el marco normativo a las particularidades de la fusión, simplificando procedimientos y diferenciándola claramente de la fisión nuclear, es otro indicativo de su apuesta estratégica.

Si la apuesta tiene éxito, la independencia energética de la Unión Europea mejoraría drásticamente, y podría convertirse en un revulsivo para mejorar la cohesión entre los Estados miembros, al facilitar políticas energéticas comunes y mitigar tensiones internas derivadas de la desigualdad en autosuficiencia energética.

Estados Unidos adopta un enfoque claramente dual en su apuesta por la energía de fusión. Por un lado, mantiene una sólida inversión pública en investigación fundamental a través de instituciones como el *National Ignition Facility* (NIF) y una fuerte apuesta por iniciativas privadas, reflejada en startups *como Helion Energy* o *TAE Technologies*. Esta combinación fomenta un marco de innovación ágil, capaz de adaptarse rápidamente a cambios tecnológicos y regulatorios.

Este modelo se ve reforzado por un sistema regulatorio flexible, diseñado expresamente para reducir las barreras administrativas al sector emergente de la fusión y diferenciar de forma clara esta tecnología de la energía nuclear convencional. Con ello, Estados Unidos busca acelerar la experimentación y atraer inversión privada sin renunciar a los estándares de seguridad necesarios.

No obstante, la apuesta estadounidense por la fusión no se limita al ámbito civil. El papel del NIF como herramienta para simular ensayos nucleares de forma segura y compatible con los tratados internacionales pone de manifiesto que la fusión también es percibida como un activo estratégico en el ámbito de la defensa. Esta dimensión militar subraya una característica clave del enfoque estadounidense: la fusión es entendida no solo como una futura fuente de energía, sino también como un elemento central de su poder tecnológico y estratégico.

China, a diferencia de otros actores, concibe la fusión nuclear como una herramienta esencial para asegurar su crecimiento económico, garantizar el suministro interno de energía a largo plazo y reducir su dependencia de combustibles fósiles importados, especialmente petróleo y gas natural, cuyos flujos comerciales actualmente condicionan su política exterior.

Su considerable capacidad inversora, manifestada en proyectos clave como el reactor experimental EAST y la planificación del reactor piloto CFETR, su ambicioso calendario de proyectos y su liderazgo global en patentes relacionadas con la fusión nuclear, evidencian una estrategia estatal decidida y sostenida. Además, la inclusión de la fusión dentro del marco estratégico de iniciativas internacionales como la BRI, ilustra claramente la intención

china de utilizar esta tecnología no solo como herramienta de seguridad energética, sino también como un medio para consolidar y expandir su influencia global y tecnológica.

Por lo tanto, se puede considerar la intención de China de utilizar la investigación en fusión nuclear como una herramienta del país asiático para extender su poder geopolítico más allá de su zona de influencia actual.

En consecuencia, el dominio de esta tecnología permitiría a sus pioneros reducir su exposición geopolítica, condicionar alianzas internacionales e incluso generar nuevos vínculos de dependencia con aquellos países que no dispongan de capacidad tecnológica propia. Por lo tanto, aunque la fusión no vaya a ser una panacea al problema de la energía, al menos a corto plazo, sí puede desempeñar un papel transformador en los sistemas energéticos y en la posición internacional de los actores que lideren su desarrollo.

El dominio de la tecnología de fusión podría implicar cambios sustanciales en el equilibrio global, condicionando las alianzas estratégicas y definiendo un nuevo reparto de poder internacional basado en la innovación tecnológica. En definitiva, la fusión nuclear representa una ventana hacia un futuro energético, geopolítico y económico significativamente distinto al actual, cuyo aprovechamiento dependerá de la visión estratégica y la capacidad tecnológica de los actores que hoy lideran su investigación.

Bibliografía

Alotaiba, T. (2024). Analysis: Why Abu Dhabi is betting on fusion [en línea]. Semafor. [Consulta: 2026]. Disponible en: https://www.semafor.com/article/10/21/2024/analysis-why-abu-dhabi-is-betting-on-fusion-tareq-alotaiba

Arnoux, R. (2011). Deuterium: a precious gift from the Big Bang [en línea]. ITER - the way to new energy. [Consulta: 2026]. Disponible en: https://www.iter.org/node/20687/deuterium-precious-gift-big-bang

Baldwin, D. et al. (2025). DOE distributed energy resource interconnection roadmap [en línea]. U. S. Department of Energy. [Consulta: 2026]. Disponible en: https://www.energy.gov/eere/i2x/doe-distributed-energy-resource-interconnection-roadmap

Barbarino, M. (2023). What is nuclear fusion? [en línea]. International Atomic Energy Agency (IAEA). [Consulta: 2026]. Disponible en: https://www.iaea.org/newscenter/news/what-is-nuclear-fusion

BGR Group. (2024). China advances nuclear fusion to strengthen comprehensive national power [en línea]. [Consulta: 2026]. Disponible en: https://bgrdc.com/wp-content/uploads/2024/10/BGR-Analysis_China-Advances-Nuclear-Fusion-to-Strengthen-Comprehensive-National-Power.pdf

Brans, P. (2024). A glimpse into the future for commercial fusion reactors [en línea]. ITER - The way to new energy. [Consulta: 2026]. Disponible en: https://www.iter.org/node/20687/glimpse-future-commercial-fusion-reactors

Carayannis, E. G., Draper, J. y Bhaneja, B. (2021). Towards fusion energy in the industry 5.0 and society 5.0 context: Call for a global commission for urgent action on fusion energy [en línea]. Journal of the Knowledge Economy. 12(4), pp. 1891-1904. [Consulta: 2026]. Disponible en: https://doi.org/10.1007/s13132-020-00695-5

Chatzis, I. y Barbarino, M. (2021). ¿Qué es la fusión y por qué es tan difícil de lograr? [en línea]. IAEA Bulletin. Vol. 62-2. [Consulta: 2026]. Disponible en: https://www.iaea.org/es/energia-de-fusion/que-es-la-fusion-y-por-que-es-tan-dificil-de-lograr

Clery, D. (2022). With historic explosion, a long sought fusion breakthrough [en línea]. Science. [Consulta: 2026]. Disponible en: https://www.science.org/content/article/historic-explosion-long-sought-fusion-breakthrough

Cook, S. A. (2024). Oil and national security: U.S.-Middle East Relations [en línea]. Council on Foreign Relations. [Consulta: 2026]. Disponible en: https://www.cfr.org/event/oil-and-national-security-us-middle-east-relations

De Chant, T. (2024). Fusion startup Tokamak Energy attracts $125M for its egg-like reactor design [en línea]. TechCrunch. [Consulta: 2026]. Disponible en: https://techcrunch.com/2024/11/20/fusion-startup-tokamak-energy-attracts-125m-for-its-egg-like-reactor-design/

Draghi, M. (2023). The Draghi report on EU competitiveness [en línea]. European Commission. [Consulta: 2026]. Disponible en: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

EIA. (2024). U.S. energy facts explained - consumption and production [en línea]. U. S. Energy Information Administration. [Consulta: 2026]. Disponible en: https://www.eia.gov/energyexplained/us-energy-facts/

Escribano, G. (2025). Europa contra el dominio energético [en línea]. Real Instituto Elcano. [Consulta: 2026]. Disponible en: https://www.realinstitutoelcano.org/comentarios/europa-contra-el-dominio-energetico/

European Commission (2021). In focus: Fusion power and the ITER Project [en línea]. Directorate-General for Communication. [Consulta: 2026]. Disponible en: https://commission.europa.eu/news/focus-fusion-power-and-iter-project-2021-05-17_en

—. (2023a). EU and Japan celebrate start of operations of the JT-60SA fusion reactor and reaffirm close cooperation on fusion energy [en línea]. Directorate-General for Energy. [Consulta: 2026]. Disponible en: https://energy.ec.europa.eu/news/eu-and-japan-celebrate-start-operations-jt-60sa-fusion-reactor-and-reaffirm-close-cooperation-fusion-2023-12-01_en

—. (2023b). EU – Gulf relations - European Commission [en línea]. Directorate-General for the Middle East, North Africa and the Gulf. [Consulta: 2026]. Disponible en: https://north-africa-middle-east-gulf.ec.europa.eu/what-we-do/eu-gulf-relations_en

—. (2024a). United States of America [en línea]. Directorate-General for Energy. [Consulta: 2026]. Disponible en: https://energy.ec.europa.eu/topics/international-cooperation/key-partner-countries-and-regions/united-states-america_en

—. (2024b). ITER – Performance [en línea]. Directorate-General for Communication. [Consulta: 2026]. Disponible en: https://commission.europa.eu/strategy-and-policy/eu-budget/performance-and-reporting/programme-performance-statements/iter-performance_en

—. (2025a). Fusion energy [en línea]. Directorate-General for Research and Innovation. [Consulta: 2026]. Disponible en: https://research-and-innovation.ec.europa.eu/research-area/energy/fusion-energy_en

—. (2025b) Fusion energy and ITER [en línea]. Directorate-General for Energy. [Consulta: 2026]. Disponible en: https://energy.ec.europa.eu/topics/research-and-technology/fusion-energy-and-iter_en

European Council. (2024). Cómo ha afectado a los mercados la invasión rusa de Ucrania: respuesta de la UE [en línea]. [Consulta: 2026]. Disponible en: https://www.consilium.europa.eu/es/policies/eu-response-russia-military-aggression-against-ukraine-archive/impact-of-russia-s-invasion-of-ukraine-on-the-markets-eu-response/

European Council. (2025). Where does the EU's gas come from? [en línea]. [Consulta: 2026]. Disponible en: https://www.consilium.europa.eu/en/infographics/where-does-the-eu-s-gas-come-from/

European Environment Agency. (2024). Trends and projections in Europe 2024 [en línea]. EEA REPORT 11/2024. [Consulta: 2026]. Disponible en: https://www.eea.europa.eu/en/analysis/publications/trends-and-projections-in-europe-2024

Eurostat. (2024). Shedding light on energy in the EU [en línea]. [Consulta: 2026]. Disponible en: https://data.europa.eu/doi/10.2785/88627.

Foster, S. y Elzinga, D. (2015). El papel de los combustibles fósiles en un sistema energético sostenible [en línea]. United Nations. [Consulta: 2026]. Disponible en: https://www.un-.org/es/chronicle/article/el-papel-de-los-combustibles-fosiles-en-un-sistema-energetico-sostenible

Fusion for Energy. (2018). The EU Council mandates the Commission to formally approve the new ITER baseline at the next ITER Council [en línea]. The European Joint Undertaking for ITER and the Development of Fusion Energy. [Consulta: 2026]. Disponible en: https://fusionforenergy.europa.eu/news/the-eu-council-mandates-the-commission-to-formally-approve-the-new-iter-baseline-at-the-next-iter-council/

Hughes, K. (2022). Wilson Center expert analysis of the Inflation Reduction Act [en línea]. Wilson Center. [Consulta: 2026]. Disponible en: https://5g.wilsoncenter.org/article/wilson-center-expert-analysis-inflation-reduction-act

Gondemberg, J. (2009). Nuclear energy in developing countries [en línea]. Daedalus. [Consulta: 2026]. Disponible en: https://www.amacad.org/publication/daedalus/nuclear-energy-developing-countries

Huld, A. (2023). La economía china en 2023: Un año de crecimiento y recuperación [en línea]. China Briefing News. [Consulta: 2026]. Disponible en: https://www.china-briefing.com/news/la-economia-china-en-2023-un-ano-de-crecimiento-y-recuperacion/

IAEA (2022). Demonstration Fusion Plants [en línea]. International Atomic Energy Agency. Vol. 62-2. [Consulta: 2026]. Disponible en: https://www.iaea.org/bulletin/demonstration-fusion-plants

Ibekwe, E. et al. (2024). Energy security in the global context: A comprehensive review of geopolitical dynamics and policies [en línea]. Engineering Science & Technology Journal. 5(1), pp. 152-168. [Consulta: 2026]. Disponible en: https://www.researchgate.net/publication/386014476_ENERGY_SECURITY_IN_THE_GLOBAL_CONTEXT_A_COMPREHENSIVE_REVIEW_OF_GEOPOLITICAL_DYNAMICS_AND_POLICIES

IEA (2022). China - Countries & Regions [en línea]. International Energy Agency. [Consulta: 2026]. Disponible en: https://www.iea.org/countries/china

—. (2023a). Middle East – Countries & Regions [en línea]. International Energy Agency. [Consulta: 2026]. Disponible en: https://www.iea.org/regions/middle-east

—. (2023b). World Energy Outlook 2023 – Analysis [en línea]. International Energy Agency. [Consulta: 2026]. Disponible en: https://www.iea.org/reports/world-energy-outlook-2023

—. (2023c). Nuclear power [en línea]. International Energy Agency. [Consulta: 2026]. Disponible en: https://www.iea.org/energy-system/electricity/nuclear-power

—. (2024). Japan - Countries & Regions [en línea]. International Energy Agency. [Consulta: 2026]. Disponible en: https://www.iea.org/countries/japan

ITER. (2024). ITER Members [en línea]. ITER - the way to new energy. [Consulta: 2026]. Disponible en: https://www.iter.org/about/iter-members

Jack, V. (2022). Nuclear fusion: The one relationship Russia and the West just can't break. Politico. [Consulta: 2026]. Disponible en: https://www.politico.eu/article/the-one-relationship-russia-and-eu-just-cant-break-iter-fusion-ukraine-war/

JT-60SA. (2024). JT-60SA certified as world's largest tokamak [en línea]. JT-60SA Advanced Superconductive Tokamak. [Consulta: 2026]. Disponible en: https://www.jt60sa.org/wp/jt-60sa-certified-as-worlds-largest-tokamak/

Korea Institute of Fusion Energy. (2020). KSTAR & ITER [en línea]. KFE: Korea Institute Of Fusion Energy. [Consulta: 2026]. Disponible en: https://www.kfe.re.kr/menu.es?mid=a20201050000

Krishnamurthy, R. V. (1998). Hydrogen isotopes [en línea]. En: Geochemistry. Encyclopedia of Earth Science. Dordrecht, Springer, pp. 326-330. [Consulta: 2026]. Disponible en: https://doi.org/10.1007/1-4020-4496-8_160

Mann, A. y Wiper, A. P. (2022). See the facility that tests whether nuclear weapons work [en línea]. Scientific American. [Consulta: 2026]. Disponible en: https://www.scientificamerican.com/article/see-the-facility-that-tests-whether-nuclear-weapons-work/

Massachusetts Institute of Technology. (2022). MIT expands research collaboration with Commonwealth Fusion Systems to build net energy fusion machine [en línea]. MIT News. [Consulta: 2026]. Disponible en: https://news.mit.edu/2022/mit-expands-research-collaboration-commonwealth-fusion-systems-sparc-0510

Matthews, D. (2024). Fusion is needed for European autonomy, says new industry body [en línea]. Science|Business. [Consulta: 2026]. Disponible en: https://sciencebusiness.net/news/nuclear-fusion/fusion-needed-european-autonomy-says-new-industry-body

Miller, S. (2023). Fusing particles and interests: The geopolitics of nuclear fusion [en línea]. Georgetown Security Studies Review. [Consulta: 2026]. Disponible en: https://gssr.georgetown.edu/the-forum/topics/technology/fusing-particles-and-interests-the-geopolitics-of-nuclear-fusion/

Ministerio para la Transición Ecológica y el Reto Demográfico. (2021). La Unión Europea en la lucha contra el cambio climático [en línea]. [Consulta: 2026]. Disponible en: https://www.miteco.gob.es/es/cambio-climatico/temas/el-proceso-internacional-de-lucha-contra-el-cambio-climatico/la-union-europea.html.

Nakićenović, N. y Swart, R. (eds.). (2000). Emissions Scenarios [en línea]. Intergovernmental Panel on Climate Change, Cambridge University Press. [Consulta: 2026]. Disponible en: https://www.ipcc.ch/site/assets/uploads/2018/03/emissions_scenarios-1.pdf

Öğütçü, C. y Öğütçü, M. (2017). China's expanding energy and geopolitical linkages with central Asia and Russia: Implications for businesses and governments [en línea]. Policy Center. [Consulta: 2026]. Disponible en: https://www.policycenter.ma/publications/china%E2%80%99s-expand-

ing-energy-and-geopolitical-linkages-central-asia-and-russia-implications

Parisi, J. y Ball, J. (2019). The future of fusion energy. World Scientific Ltd. ISBN: 978-1786345424.

Pearson, R. J., Antoniazzi, A. B. y Nuttall, W. J. (2018). Tritium supply and use: A key issue for the development of nuclear fusion energy [en línea]. Fusion Engineering and Design. Vol. 136, pp. 1140-1148. [Consulta: 2026]. Disponible en: https://doi.org/10.1016/j.fusengdes.2018.04.090

Pedersen, T. S. et al. (2016). Confirmation of the topology of the Wendelstein 7-X magnetic field to better than 1:100,000 [en línea]. Nature Communications. 7(1), p. 13493. [Consulta: 2026]. Disponible en: https://doi.org/10.1038/ncomms13493

Picot, W. (2021). ITER: el experimento de fusión más grande del mundo [en línea]. IAEA Bulletin. Vol. 62-2. [Consulta: 2026]. Disponible en: https://www.iaea.org/es/energia-de-fusion/iter-el-experimento-de-fusion-mas-grande-del-mundo

Pozzi, G. (2025). China's energy law 2025: Highlights for renewables, energy security, and private companies [en línea]. FiscalNote. [Consulta: 2026]. Disponible en: https://fiscalnote.com/blog/chinas-energy-law-2025

Qihan Zou, C. (2024). China and the race for nuclear fusion [en línea]. The Diplomat. [Consulta: 2026]. Disponible en: https://thediplomat.com/2024/06/china-and-the-race-for-nuclear-fusion/

Rademaekers, K. et al. (2018). Study on the impact of the ITER activities in the EU [en línea]. Trinomics. [Consulta: 2026]. Disponible en: https://trinomics.eu/project/iter-impacts/

Regal, C. (2024). The growing role of AI in nuclear energy investing [en línea]. VanEck. [Consulta: 2026]. Disponible en: https://www.vaneck.com/us/en/blogs/natural-resources/ai-and-nuclear-power/

Ritchie, H. (2024). What's the impact of artificial intelligence on energy demand? [en línea]. By the numbers. [Consulta: 2026]. Disponible en: https://www.sustainabilitybynumbers.com/p/ai-energy-demand

Roveda, M. (2025). Entrevista personal.

Sala, A. (2022). ¿Quién gana y quién pierde con la fusión nuclear? Así afectará al sector energético [en línea]. El Periódico. [Consulta: 2026]. Disponible en: https://www.elperiodico.com/

es/economia/20221214/gana-pierde-fusion-nuclear-afectara-79913030

Sánchez, J. (2025). Entrevista personal.

Setzer, J., Peterson, L. y Marner, D. (2024). Navigating net zero via the law [en línea]. Grantham Research Institute on climate change and the environment. [Consulta: 2026]. Disponible en: https://www.lse.ac.uk/granthaminstitute/news/navigating-net-zero-via-the-law/

Rubel, M. (2018). Fusion Neutrons: Tritium breeding and impact on wall materials and components of diagnostic systems. Journal of Fusion Energy. Vol. 38, pp. 315-329.

Sanfilippo, A., Vermeersch, M. y Benito, V. B. (2024). Energy transition strategies in the Gulf Cooperation Council countries [en línea]. Energy Strategy Reviews. Vol. 55. [Consulta: 2026]. Disponible en: https://doi.org/10.1016/j.esr.2024.101512

Smirnov, V. P. (2009). Tokamak foundation in USSR/Russia 1950–1990 [en línea]. Nuclear Fusion. 50(1). [Consulta: 2026]. Disponible en: https://doi.org/10.1088/0029-5515/50/1/014003

The White House. (2023). International partnerships in a new era of fusion energy development [en línea]. The White House. [Consulta: 2026]. Disponible en: https://bidenwhitehouse.archives.gov/ostp/news-updates/2023/12/02/international-partnerships-in-a-new-era-of-fusion-energy-development/

—. (2025). Putting America first in international environmental agreements [en línea]. Presidential actions. The White House. [Consulta: 2026]. Disponible en: https://www.whitehouse.gov/presidential-actions/2025/01/putting-america-first-in-international-environmental-agreements/

Timmermann, C. y Noboa, E. (2022). Energy sovereignty: A values-based conceptual analysis [en línea]. Science and engineering ethics. 28(6). [Consulta: 2026]. Disponible en: https://doi.org/10.1007/s11948-022-00409-x

U.S. Department of Energy. (2023). Inflation Reduction Act of 2022 [en línea]. [Consulta: 2026]. Disponible en: https://www.energy.gov/lpo/inflation-reduction-act-2022

Waldrop, M. M. (2024). Los retos de la energía de fusión nuclear [en línea]. Knowable Magazine. [Consulta: 2026]. Disponible en: https://doi.org/10.1146/knowable-012524-1

Zhang, C. (2024). Split of fusion regulation from fission codified by new law [en línea]. American Institute of Physics. [Consul-

ta: 2026]. Disponible en: https://ww2.aip.org/fyi/split-of-fusion-regulation-from-fission-codified-by-new-law

Zhongying, W. y Sandholt, K. (2025). Guest post: China will need 10,000GW of wind and solar by 2060 [en línea]. Carbon Brief. [Consulta: 2026]. Disponible en: https://www.carbonbrief.org/guest-post-china-will-need-10000gw-of-wind-and-solar-by-2060/

Zhou, Y., Sadler, J. D. y Hurricane, O. A. (2025). Instabilities and mixing in inertial confinement fusion [en línea]. Annual Review of Fluid Mechanics. Vol. 57, pp. 197-225. [Consulta: 2026]. Disponible en: https://doi.org/10.1146/annurev-fluid-022824-110008

Capítulo tercero

Impacto del «campo de batalla transparente» en la guerra de Ucrania y sus implicaciones para la doctrina militar española

Francisco Freire Rodríguez

«La guerra es el ámbito de la incertidumbre; tres cuartas partes de aquellas cosas sobre las que se construye la actuación en ella están sumidas en la niebla de una incertidumbre».

Carl von Clausewitz

Resumen

El presente estudio analiza el impacto del concepto de «campo de batalla transparente» —entendido como el fenómeno que se produce por la combinación de la capacidad de observar, procesar y actuar sobre el entorno operativo en tiempo casi real— en el desarrollo de la guerra de Ucrania, con el objetivo de evaluar sus implicaciones para la doctrina militar conjunta española. El trabajo se apoya en un enfoque metodológico combinado, que integra los métodos descriptivo, analítico, sintético y comparativo, con técnicas de revisión documental y entrevistas semiestructuradas a autoridades militares.

En primer lugar, se establece la definición de campo de batalla transparente a partir de sus componentes tecnológicos y conceptuales: drones, sensores, inteligencia artificial, conectividad, letalidad y «democratización». A continuación, se estudia su aplicación práctica en el conflicto ucraniano, donde se han observado los efectos más significativos sobre funciones conjuntas como mando y control, maniobra, información o fuegos, así como sobre

principios operativos como la sorpresa, la concentración y la continuidad. El análisis constata que la transparencia ha modificado profundamente la dinámica de las operaciones, imponiendo un entorno altamente letal y cambiante.

Por último, el estudio contrasta estas observaciones con la doctrina conjunta española, concluyendo que esta recoge, en términos generales, muchas de las implicaciones operacionales derivadas del fenómeno, especialmente a través de los conceptos asociados al mando y control, la gestión de la información y las operaciones multidominio. No obstante, también se detecta una falta de concreción en aspectos clave como la decepción y la integración de tecnologías, lo que sugiere oportunidades de mejora doctrinal ante las exigencias de un entorno operacional condicionado por la transparencia tecnológica.

Palabras clave

Transparencia, Guerra de Ucrania, Doctrina militar conjunta, Operaciones militares, Decepción.

Impact of the "transparent battlefield" on the Ukraine War and its implications for Spanish military doctrine

Abstract

This study analyzes the impact of the concept of the "transparent battlefield"— understood as the phenomenon resulting from the combination of the ability to observe, process, and act upon the operational environment in near real time—on the course of the war in Ukraine, with the aim of assessing its implications for Spanish joint military doctrine. The study is based on a combined methodological approach that integrates descriptive, analytical, synthetic, and comparative methods with literature review techniques and semi-structured interviews with military authorities.

Firstly, the definition of a transparent battlefield is established based on its technological and conceptual components: drones, sensors, artificial intelligence, connectivity, lethality, and "democratization." Secondly, the study examines its practical application in the Ukrainian conflict, where the most significant effects have been observed on

joint functions such as command and control, manoeuvre, information, and fires, as well as on operational principles like surprise, concentration, and continuity. The analysis confirms that transparency has profoundly altered the dynamics of operations, imposing a highly lethal and dynamic environment.

Finally, the study compares these findings with Spanish joint doctrine, concluding that, in general terms, it incorporates many of the operational implications of this phenomenon, particularly through concepts related to command and control, information management, and multi-domain operations. However, it also identifies a lack of specificity in key areas such as deception doctrine and technology improvement, suggesting opportunities for doctrinal improvement in response to the demands of an operational environment shaped by technological transparency.

Key words

Transparency, War in Ukraine, Joint military doctrine, Military operations, Deception.

Lista de abreviaturas

A2/AD	*Anti-Access/ Area Denial*
ACT	*Allied Command Transformation*
AEW	*Airborne Early Warning*
AI	*Air Interdiction*
AJP	*Allied Joint Publication*
ASAT	Sistema Anti-Satélite
C2	Mando y control
C2W	Guerra de mando y control
C3	Mando, control y comunicaciones
C4ISR	Mando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento
CMOPS	Comandante del Mando de Operaciones
CEMFAS	Curso de Estado Mayor de las FAS
CIS	Sistemas de Información y Comunicaciones
COMINT	*Communications Intelligence*

CUAS	*Counter-Unmanned Aerial Systems*
DIVDEF	División de Desarrollo de Fuerza
DRAE	Diccionario de la Real Academia Española
DEW	Armas de energía dirigida
EGLET	Escuela de Guerra y Liderazgo del Ejército de Tierra
EMACON	Estado Mayor Conjunto
EMAD	Estado Mayor de la Defensa
ET	Ejército de Tierra
EW	*Electronic Warfare*
FAS	Fuerzas Armadas
FAU	Fuerzas Armadas de Ucrania
FPV	*First Person View*
FOFA	*Follow-on Forces Attack*
GEOINT	Inteligencia geoespacial
GLOC	Línea de Comunicación Terrestre
GPS	*Global Positioning System*
HAPS	*High Altitude Pseudo-Satellites*
IA	Inteligencia artificial
IEEE	Instituto Español de Estudios Estratégicos
INFOOPS	Operaciones de Información
ISW	*Institute for the Study of War*
IFRI	*Institut Français des Relations Internationales*
IMINT	Inteligencia de imágenes
ISR	*Intelligence, Surveillance, and Reconnaissance*
JATEC	*Joint Analysis, Training and Education Centre*
JEMAD	Jefe del Estado Mayor de la Defensa
JOA	*Joint Operations Area*
LSCO	*Large-Scaled Combat Operations*
MADOC	Mando de Adiestramiento y Doctrina
MDO	Operaciones Multidominio

ME	Esfuerzo Principal
MILDEC	*Military Deception*
MOPS	Mando de Operaciones
NAC	Consejo del Atlántico Norte
NTISR	*Non-Traditional ISR*
NCW	*Network Centric Warfare*
NEC	*Network Enabled Capable*
OAV	Observador avanzado
OPSEC	Seguridad de las Operaciones
OSINT	*Open Source Intelligence*
OTAN	Organización del Tratado del Atlántico Norte
PC	Puesto de mando
PDC	Publicación Doctrinal Conjunta
RMA	*Revolution in Military Affairs*
RPAS	*Remoted Controlled Aerial System*
RSC	*Recce-Strike Complex*
SAR	*Synthetic Aperture Radar*
SEAD	Supresión de defensas aéreas enemigas
STRATCOM	Comunicación Estratégica
StS	*Sensor-to-Shooter*
TIC	Tecnologías de la Información y la Comunicación
TRADOC	*Transformation and Doctrine Command*
UAS	*Unmanned Aerial System*
UAV	*Unmanned Aerial Vehicle*
UGS	*Unmanned Ground System*
ZO	Zona de operaciones

1 Introducción. Concepto de «campo de batalla transparente»

1.1 Buscando la definición doctrinal

El campo de batalla transparente hace referencia a un escenario en el que prácticamente todos los elementos presentes en el teatro de operaciones pueden ser detectados, localizados y atacados en un plazo de tiempo muy breve (Frías, 2024). Este fenómeno pone en entredicho principios como la sorpresa y la concentración de fuerzas y presenta entornos operativos dónde las FAS deben adaptarse para poder seguir operando.

En la doctrina nacional no se contempla una definición concreta, si bien, la PDC-01 (B) deja entrever una aproximación al término al incluir, dentro del nuevo concepto de mando y control (C2) que requieren las operaciones multidominio (MDO), que este se logrará mediante varios habilitadores como «la gestión de la información, acompañada de la sensorización y digitalización del campo de batalla, que permitirán alcanzar un adecuado conocimiento de la situación» (EMAD, 2024: 111).

Por su parte, en el *US Army* también han descrito las características que presenta y que ayudan a definir el concepto: «LSCO[1] will be marked by the democratization and proliferation of advanced technologies and hyperconnected global communications, creating an increasingly transparent battlefield that makes it difficult to hide from the enemy» (TRADOC, 2024: 4).

También resulta destacable la aportada para el término transparencia por Garnier y Néron-Bance (2024: 3):

> «Transparency is defined as the ability to acquire and exploit geolocated, near-real-time awareness of a given operational environment thanks to a connectivity architecture linking networks of heterogeneous and redundant sensors, mass data processing systems, and effectors».

Del análisis de todo ello, se puede extraer componentes definitorios como drones y sensores, el procesamiento de datos, la conectividad, la letalidad de los medios efectores y la «democratización». Definir el campo de batalla transparente con precisión, requiere ahondar en estos conceptos de manera sistemática.

[1] *Large-Scaled Combat Operations*

1.2 Componentes del sistema

1.2.1 Los drones

La guerra de Ucrania ha visto como el uso de drones ha transformado profundamente el campo de batalla, marcando un antes y un después en la forma de concebir las operaciones militares. El uso masivo de drones, tanto comerciales como militares, ha complicado enormemente el movimiento, ya que cualquier concentración de fuerzas es detectada y atacada con rapidez.

El impacto de los drones en Ucrania también se observa en su proliferación y uso innovador. Chulilla (2024) estima que hay millones de drones en funcionamiento, muchos de ellos fabricados de forma local con componentes comerciales. Estos dispositivos son manejados por personal capacitado que los integra de manera efectiva en las operaciones. Una de las innovaciones más disruptivas ha sido el uso de drones kamikazes, capaces de destruir objetivos, incluyendo vehículos blindados, con un coste significativamente menor al de los sistemas tradicionales (Chulilla, 2024). Entre los más característicos están los denominados *First Person View* (FPV), basado por lo general en un dron cuadricóptero al que se le añade un explosivo, permitiendo que su ciclo *sensor-to-shooter* (StS) sea realmente corto.

El uso masivo y descentralizado de estos drones no solo produce efectos físicos, sino también efectos psicológicos en el adversario, generando saturación y desgaste (Garnier y Néron-Bancel, 2024).

Kagan *et al.* (2024) consideran que los drones tácticos han transformado el campo de batalla al permitir las siguientes posibilidades:

- Compensar carencias de artillería: su pequeño tamaño y coste relativo los hacen omnipresentes, permitiendo ataques rápidos y precisos.
- Descentralizar operaciones: miles de drones operados individualmente permiten atacar objetivos de forma rápida, flexible e independiente.
- Redefinir la noción de superioridad aérea: aunque un bando pueda mantener la superioridad aérea tradicional, no puede evitar que el adversario alcance una «superioridad aérea a baja altitud» mediante el uso extensivo de drones tácticos.

Además de la vigilancia, los drones han evolucionado para incluir municiones de merodeo (*loitering*), que combinan detección y ataque en una sola plataforma. Estos sistemas comenzaron a emplearse ampliamente en el conflicto de Nagorno-Karabaj donde aportaron importantes lecciones sobre el uso de UAS y sistemas de fuegos de precisión en la guerra moderna y su capacidad de atacar objetivos inmediatamente tras ser detectados (Antal, 2022).

No obstante, su desarrollo no se limita al ámbito aéreo. En el entorno marítimo, drones como el MQ-4C Triton y el Camcopter S-100 amplían las capacidades de vigilancia desde plataformas navales, mientras que proyectos como el Blackwing y los UUV (vehículos submarinos no tripulados) introducen capacidades autónomas en el ámbito submarino. Países como Turquía están incluso explorando portaaviones dedicados a drones (Garnier y Néron-Bancel, 2024).

En conjunto, estas innovaciones están creando un «continuo de vigilancia» que extiende la detección y el control aéreos, terrestres y marítimos, consolidando los drones como herramientas indispensables en los conflictos modernos.

1.2.2 Otros medios de vigilancia

Los avances tecnológicos en sensores más allá de los drones han ampliado la capacidad de vigilancia en múltiples dominios. Radares pasivos, de baja frecuencia y cuánticos desafían el sigilo, mientras que sensores hiperespectrales prometen detectar estructuras subterráneas, aunque su interpretación sigue siendo compleja (Garnier y Néron-Bancel, 2024).

En el ámbito aéreo, plataformas AEW y HAPS, como Stratobus o BalMan, ofrecen vigilancia prolongada y de alta resolución, superando incluso a los satélites por su proximidad al terreno. En el espacio, los satélites militares mejoran la observación, el COMINT y el guiado de armamento, mientras constelaciones civiles como Starlink proporcionan redundancia y resiliencia, como se ha comprobado en Ucrania (Garnier y Néron-Bancel, 2024).

Los satélites comerciales, como los de MAXAR, aportan imágenes de alta resolución que permiten localizar tropas, coordinar ataques y sincronizar operaciones complejas (MADOC, 2024b).

Asimismo, el concepto doctrinal NTISR (*Non-Traditional Intelligence, Surveillance, and Reconnaissance*) amplía las capa-

cidades ISR mediante plataformas no convencionales como aeronaves o drones civiles, especialmente útiles en zonas donde los activos tradicionales serían vulnerables. Según MADOC (2024b), esta capacidad de adaptación mediante recursos propios o de terceros es clave en conflictos actuales.

En conjunto, estas innovaciones potencian la vigilancia, aunque también imponen nuevos desafíos operacionales: el procesamiento de grandes volúmenes de datos y la creciente dependencia de infraestructuras tecnológicas en escenarios de alta intensidad.

1.2.3 El procesamiento de datos

Paradójicamente, el desafío en el campo de batalla contemporáneo ya no radica en la escasez de información, sino en cómo gestionar de manera eficaz su abundancia. Tal y como declara el TG Agüero

> «La profusión de información puede desconcertarnos cuando no es posible interpretarla. (…) Este problema de procesamiento puede ser abordado mediante la inteligencia artificial y así posibilitar su aprovechamiento para la toma de decisiones»[2].

Efectivamente, la guerra de Ucrania ha emergido como un laboratorio viviente para la aplicación militar de la inteligencia artificial (IA), marcando un hito en el desarrollo tecnológico en conflictos armados. Según Pardo de Santayana (2024), aunque esta guerra no esté completamente definida por la IA, sí está acelerando su evolución al proporcionar un campo de pruebas para sistemas y aplicaciones en constante mejora.

La IA ha demostrado ser particularmente eficaz en el procesamiento inicial de imágenes y señales acústicas. En el ciclo de inteligencia, la fase de explotación, que es principalmente cognitiva, resulta crucial para transformar datos recopilados en inteligencia útil para las operaciones. En este contexto, los avances tecnológicos, especialmente en IA, están revolucionando el proceso. Mientras que los analistas humanos enfrentan límites en la cantidad de información que pueden procesar, la IA complementa su trabajo al optimizar tareas básicas y masivas, permitiendo a los expertos concentrarse en análisis más complejos (Garnier y

[2] Entrevista al TG Agüero.

Néron-Bancel, 2024). Sin embargo, el éxito de esta integración depende de una adecuada colaboración entre las capacidades tecnológicas y las competencias especializadas de los analistas.

La IA en Ucrania, se ha utilizado para analizar imágenes por satélite, detectar movimientos enemigos y optimizar los procesos logísticos. Además, el reconocimiento facial ha sido empleado para identificar soldados rusos muertos y combatir la desinformación, mientras que algoritmos de aprendizaje automático han mejorado la evaluación de daños (Pardo de Santayana, 2024).

Por el lado ruso, aunque existe menos información abierta, se sabe que las FAS también han apostado por la IA. Rusia ha integrado esta tecnología en municiones de merodeo como el dron Lancet-3, que permiten analizar y atacar objetivos (Pardo de Santayana, 2024).

La guerra de Ucrania está estableciendo las bases para una nueva era en los conflictos armados, donde la IA desempeñará un papel central. Las lecciones extraídas de este conflicto contribuyen a definir los futuros conflictos. Como advierte Pardo de Santayana (2024), cada día que el conflicto persiste, las capacidades de la IA se perfeccionan, no para detener la guerra actual, sino para preparar el terreno para futuros enfrentamientos donde la tecnología puede ser el factor decisivo.

1.2.4 La conectividad

La transparencia en el campo de batalla se fundamenta en la interconexión de datos respaldada por tres pilares principales: sensores que recopilan información constantemente, herramientas que procesan y analizan estos datos para proporcionar contexto temporal y espacial, y redes que transmiten la información procesada de forma instantánea, asegurando su validez y utilidad. Este sistema ofrece, a quien debe tomar las decisiones, una visión que permite abarcar el espacio de batalla de un vistazo, facilitando decisiones rápidas y precisas.

De acuerdo con los análisis de Garnier y Néron-Bancel (2024: 24) «Connectivity is the key to this system (…) into which all sensors, effectors and deciders will be plugged and without which they lose their inherent superiority». Por ejemplo, los drones que operan en Ucrania dependen de redes como Starlink, que garantizan flujos de datos esenciales de alta velocidad para los puestos de mando. La transición hacia la «hiperconectividad» está transfor-

mando las capacidades operativas, con redes 5G que soportarán más de un millón de dispositivos por kilómetro cuadrado, multiplicando exponencialmente el flujo de datos.

Este acceso compartido a datos en tiempo real está reconfigurando el proceso de mando. La denominada «uberización» de los datos (Garnier y Néron-Bancel, 2024) favorece estructuras más horizontales, reduciendo el ciclo StS y la intermediación jerárquica. Aunque esto agiliza el ciclo de decisión, también obliga a adaptar las estructuras y procesos de mando para no perder el control de las operaciones.

1.2.5 La letalidad

El dominio terrestre está experimentando un incremento significativo en la letalidad debido a la saturación de medios de vigilancia y el aumento de la precisión de las armas, afectando negativamente a la capacidad de supervivencia de las fuerzas. A medida que los avances tecnológicos amplían el alcance y la precisión de los sensores y sistemas de ataque, la transparencia se ha centrado en la identificación y destrucción rápida de objetivos. Este enfoque, que puede observarse en conflictos recientes como el frente ucraniano, ha reducido la guerra a una dinámica de «encontrar y atacar» dentro de un ciclo de decisión extremadamente corto. En este modelo, la exposición en el campo de batalla equivale a la destrucción casi inmediata (Garnier y Néron-Bancel, 2024).

El concepto de *kill chain* describe una serie de acciones interrelacionadas necesarias para ejecutar un ataque exitoso[3]. Estas etapas incluyen detectar el objetivo (*find*), localizar su posición (*fix*), seguir sus movimientos (*track*), obtener datos de tiro (*target*), ejecutar el ataque (*engage*) y evaluar los efectos (*assess*). Los avances tecnológicos han simplificado y abaratado cada paso de la *kill chain* (Frías, 2023). Además, si bien las *kill-chain* tradicionales describen esta secuencia como un proceso lineal, el enfoque parece evolucionar hacia conceptos como las *kill-web*, donde múltiples sensores y plataformas de ataque están interconectados en una red flexible. Las nubes de combate, que integran datos de múltiples fuentes en tiempo real, potencian esta capacidad, aumentando la eficacia y la letalidad de las fuerzas en combate (MADOC, 2024b).

[3] En ámbito OTAN, la secuencia más empleada es la denominada F2T2EA.

Los sensores modernos, los sistemas de posicionamiento global (GPS) y los drones han hecho que la detección y localización de objetivos sean rápidas y accesibles. La introducción de municiones de guía terminal ha mejorado significativamente la precisión los distintos sistemas de armas, permitiendo destruir objetivos con muy pocos proyectiles. Por último, la capacidad de la IA para procesar enormes cantidades de datos acelera notablemente el proceso de *targeting*, reduciendo el tiempo entre la detección de un objetivo y su neutralización (Frías, 2024). Este avance, junto con la disponibilidad de armas *hiperveloces* que minimizan los tiempos de vuelo, ha hecho que las acciones de fuego sean más rápidas y letales que nunca, consolidando la preponderancia de los fuegos como factor decisivo en el combate moderno.

Efectivamente, Flint (2006) argumentaba que las FAS de los EE. UU. disponían de sistemas que permitían observar y destruir objetivos de forma remota a lo largo de todo el globo mediante la adecuada combinación de inteligencia entregada por disciplinas como la GEOINT y armamento avanzado de precisión. En la actualidad, la explotación de la GEOINT gracias a la sensorización del campo de batalla ha permitido a los actores militares obtener una conciencia situacional sin precedentes ni restricciones geográficas. Del mismo modo que anticipaba Flint, también se ha podido optimizar la sincronización de ataques y maximizar la letalidad de los sistemas de armas de precisión, extendiendo el alcance del poder de los Estados participantes a través de sus FAS.

1.2.6 La «democratización»

La transparencia en el campo de batalla no depende exclusivamente de recursos estatales, sino que también incluye un cierto componente de «democratización», de acuerdo con definiciones como la procedente del TRADOC y mencionada anteriormente. Según TRADOC (2024), la disponibilidad de herramientas como satélites privados y drones comerciales ha permitido el acceso a capacidades de vigilancia y reconocimiento que antes estaban limitadas a fuerzas militares. La integración de estos medios civiles en las operaciones ha reducido la dependencia de infraestructuras militares especializadas, ofreciendo soluciones alternativas que garantizan una vigilancia constante del entorno. Además, la velocidad con la que evolucionan estas tecnologías y su mayor facilidad de sustitución han permitido que las fuerzas en combate mantengan una elevada conciencia situacional redefiniendo

el concepto de ventaja informativa en los conflictos modernos, donde la descentralización del acceso a la inteligencia juega un papel clave en la toma de decisiones.

Un resultado clave de esta «democratización» es la inteligencia de fuente abierta (OSINT), que ha ganado protagonismo en conflictos como el ruso-ucraniano. Comunidades de analistas civiles, denominados «osinters», utilizan redes sociales y plataformas públicas para rastrear acciones tácticas con un detalle sin precedentes[4]. Además, el empleo de aplicaciones civiles ha transformado las operaciones. En Ucrania, plataformas como Diia, Delta, MilChat o MyGun permiten comunicar, intercambiar datos tácticos, calcular trayectorias y ejecutar fuegos basados en tecnologías civiles (Garnier y Néron-Bancel, 2024). Watling sentencia que «In Ukraine, civilians were deliberately integrated into the defensive ISR net» (2024: 86) participando activamente en los ciclos de inteligencia de las operaciones gracias a la tecnología. Este acceso abierto a la transparencia está redefiniendo la recopilación de inteligencia, ofreciendo herramientas que antes eran exclusivas de las Fuerzas Armadas.

1.3 Concepto de RSC

Para entender las consecuencias reales que en la actualidad tiene el campo de batalla transparente es necesario conocer lo que son los *Recce-Strike Complex* (RSC) y su presencia en la guerra de Ucrania.

Frías (2023) hace una sencilla pero soberbia descripción de los RSC desde sus orígenes. Según el autor, la introducción de las «armas inteligentes» en los años ochenta marcó un punto de inflexión en la concepción del combate. El uso de tecnologías avanzadas, como armas guiadas y sistemas de reconocimiento, derivó en la conceptualización del RSC, un conjunto de sistemas que integraba capacidades reconocimiento y ataque para maximizar su efectividad.

Un RSC combina dos tipos principales de sistemas, cada uno con funciones críticas para alcanzar la supremacía en el campo de batalla: los sistemas defensivos, diseñados para proteger las capacidades propias frente a las amenazas enemigas y los siste-

[4] Sitios web como *oryxspioenkop.com* documentan pérdidas materiales con evidencias visuales, mientras que otros como *understandingwar.org* elaboran mapas y análisis operativos comparables al trabajo militar profesional.

mas ofensivos, cuyo objetivo es desgastar y destruir las capacidades del RSC enemigo (Frías, 2023).

1.4 Preanálisis: primeras consecuencias

A lo largo de la historia, los avances tecnológicos han buscado constantemente mejorar la transparencia en los conflictos armados. Estos avances facilitan una mayor visibilidad, pero también desencadenan una competición continua entre tecnologías, donde cada avance en transparencia genera contramedidas para preservar la opacidad (Garnier y Néron-Bancel, 2024).

Hoy en día, la mejora en la capacidad de observación parece prometer superar la «niebla de la guerra», ofreciendo una aparente transparencia en el campo de batalla al reducir la opacidad y las limitaciones informativas propias del conflicto. Sin embargo, esto implicaría incorrectamente que la transparencia es una propiedad intrínseca del campo de batalla, cuando en realidad es un estado transitorio que depende de sistemas de recopilación, análisis y explotación de datos. Para Frías (2024), es el resultado del despliegue masivo de sensores y de un sistema C2 capaz de procesar la información recopilada y asignar objetivos a vectores de fuego. Cuando solo un bando dispone de estas capacidades, la ventaja es decisiva. Esto se observó en el conflicto de Nagorno-Karabaj de 2020, donde los azeríes emplearon UAV de reconocimiento, artillería convencional, municiones guiadas y UAV suicidas para dominar el teatro de operaciones frente a los armenios, quienes dependían de medios de observación tradicionales como los OAV. Garnier y Néron-Bancel (2024) consolidan esta afirmación al postular que la transparencia no es solo una característica, sino un objetivo que debe alcanzarse y protegerse frente al enemigo, quien también busca explotar esta ventaja.

Aunque la capacidad tecnológica permite adquirir y explotar un conocimiento geolocalizado en tiempo casi real, esto no elimina la incertidumbre inherente a la guerra. La transparencia en el campo de batalla no solo se basa en tecnologías avanzadas, sino que también implica una lucha recíproca para dificultar la comprensión del enemigo. Este análisis es clave para entender si este paradigma redefine las reglas del conflicto o simplemente añade una capa adicional de complejidad.

A pesar de sus ventajas, este concepto se enfoca en la creencia errónea de que la claridad visual proporcionada por medios

tecnológicos equivale a una claridad cognitiva que garantizaría la comprensión total de las acciones o intenciones del adversario. Sin embargo, esta equiparación es problemática, ya que la transparencia es el opuesto de la opacidad, pero no necesariamente de la incertidumbre, que sigue siendo una constante intrínseca a la dimensión humana del conflicto (Garnier y Néron-Bancel, 2024).

En esencia, la transparencia en el campo de batalla no elimina la incertidumbre inherente a la guerra. Las tecnologías avanzadas han redefinido los parámetros operativos, pero el elemento humano y la naturaleza dinámica del combate aseguran que la incertidumbre y el azar permanezcan como constantes inevitables. En su obra, Watling ejemplifica errores en las percepciones humanas, para finalmente terminar sentenciando que «humans are easily distracted, vulnerable to assumptions» (2024: 15).

En suma, aunque la tecnología ofrece un conocimiento de la situación sin precedentes, el factor humano y la naturaleza dinámica de la guerra aseguran que la incertidumbre y la fricción continúen siendo elementos presentes en el combate moderno, dificultando el entendimiento o comprensión de la situación.

1.5 Ver y entender

Para tratar de extraer consecuencias más claras, se desarrolla a continuación una matriz que contemple las situaciones posibles en la relación de visibilidad física de un actor y la comprensión cognitiva de sus intenciones.

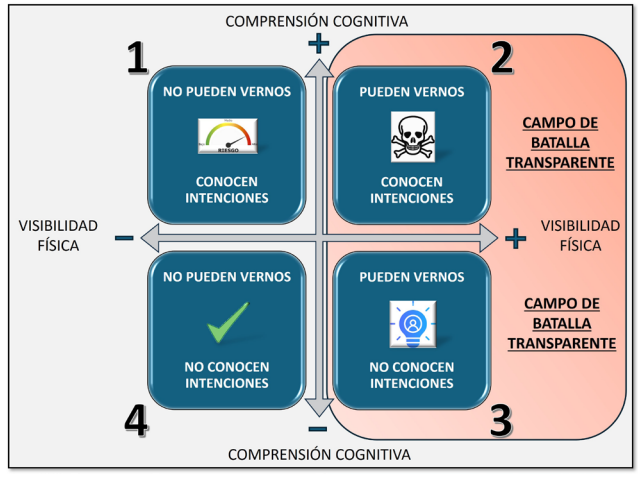


Gráfico 1. Matriz de Visibilidad física – Comprensión cognitiva Fuente: elaboración propia

Asumir que el campo de batalla transparente es una realidad que irá consolidándose en todos los conflictos modernos, parece orientar a que los entornos de las operaciones se desarrollarán siempre en las condiciones de los sectores 2 y 3. Ante esta situación, evitar que el adversario comprenda las operaciones propias es imprescindible, por lo que una parte del planeamiento debe orientarse a crear las condiciones necesarias para alcanzar el entorno 3. Para ello, la decepción militar es, más que nunca, fundamental.

Trabajar en los sectores 1 y 4 implicará la necesidad de incorporar tecnologías que anulen permanente o temporalmente la visibilidad. En ese caso y una vez alcanzadas esas condiciones, el sector 1 se vuelve un sector extremadamente peligroso, por la situación de desventaja que puede crear una percepción errónea de la realidad, al poder el adversario comprender nuestras acciones a pesar de no poder verlas. El sector 4 será el más adecuado para desarrollar las operaciones propias, y de nuevo ocultar nuestras intenciones y confundir al adversario serán las herramientas cruciales. Por supuesto, el sector 2 es una situación de absoluta desventaja, que debe ser evitada por todos los medios.

En este contexto, la transparencia física del campo de batalla no elimina el elemento de incertidumbre. Incluso cuando cada detalle parece controlado y planeado, optar por entrar en combate implica aceptar el azar como una constante (Garnier y Néron-Bancel, 2024). La guerra, por tanto, sigue siendo una combinatoria de previsión y riesgo que desafía cualquier intento de determinismo matemático.

Estos escenarios destacan que la transparencia, aunque ventajosa, no garantiza la victoria por sí sola. Salvo en casos de errores severos, superar la transparencia requiere habilidades complejas y un alto nivel de agilidad mental. Esto refuerza la idea de que la transparencia es solo un componente de un sistema de capacidades más amplio. Adaptarse y anticiparse a sus límites mediante métodos de ocultación, engaño y un planeamiento robusto sigue siendo esencial para mantener la ventaja en el campo de batalla, transparente o no.

1.6 La diferencia entre ver y entender: la decepción

La decepción militar (MILDEC), que son «el conjunto de medidas dirigidas a inducir a error al enemigo por medio de la

manipulación, la deformación o la falsificación de evidencias para hacerle actuar de forma perjudicial a sus intereses» (definición doctrinal del ET) ha conseguido que incluso con un conocimiento claro de las posiciones enemigas, el resultado de una acción no está asegurado. Factores tangibles como el terreno, la potencia de fuego y la densidad de tropas interactúan con factores intangibles, entre los que destacan la cohesión, la moral y la habilidad de los mandos. Aquí, la fricción descrita por Clausewitz (2005) —las contingencias e incertidumbres propias de la guerra— continúa desempeñando un papel crucial.

No obstante, la doctrina conjunta española no parece desarrollar de forma específica el concepto de decepción, más allá de tratarlo tangencialmente en el marco de algunas funciones conjuntas o principios operativos, pero sin entrar en detalles sobre cómo debe concebirse la decepción en el marco nacional. En términos generales, ni el CMOPS ni el director del IEEE ni el director de la EGLET pueden aportar información sobre doctrina nacional que desarrolle la decepción[5]. Sin embargo, este último oficial general hace una interesante reflexión al mencionar que «existen numerosos ejemplos históricos de planes de decepción exitosos», sugiriendo la importancia de la historia como fuente de aprendizaje sobre la decepción. Pero también el propio GB. Frías lamenta precisamente que «una de las carencias de nuestra educación militar es un buen estudio de la Historia Militar»[6].

Por su lado, es destacable los enfoques de otros países y ejércitos. Por poner algún ejemplo, el *US Army* integra el engaño en su arte operacional mediante programas específicos de adiestramiento[7] (MADOC, 2024b); Francia ha actualizado recientemente su doctrina sobre el engaño para adaptarla a un entorno de alta visibilidad, priorizando también los efectos psicológicos (Garnier y Néron-Bancel, 2024); Rusia tienen un nutrido y extenso abanico de principios y métodos de engaño, como la simulación de «debilidad» o de «fatiga», para explotar oportunidades y efectos cognitivos en sus adversarios (Jójárt, 2024).

[5] Entrevistas al TG Agüero, GB. Bados y GB Frías.

[6] Entrevista al GB Frías

[7] Curso de Planificadores de Decepción del Ejército de EE. UU. (*US Army Deception Planners Course*) y Curso de Entrenamiento Conjunto de Decepción Militar (*US Joint MILDEC Training Course*).

2 Estudio de caso: la guerra de Ucrania (2022)

2.1 Introducción

Kagan *et al.,* (2024) compara la guerra de Ucrania con la guerra civil española–en su papel como campo de pruebas para tecnologías y doctrinas que probablemente definan futuros conflictos entre grandes potencias. Jójárt (2024) considera que la experiencia de la guerra en Ucrania influirá profundamente en el pensamiento militar ruso durante las próximas décadas, al ser la mayor contienda librada por Rusia desde la Gran Guerra Patria (1941-1945), proporcionando experiencia de primera mano a Rusia, al mismo tiempo que les sirve de campo de pruebas para observar las capacidades de armamento y doctrinas de la OTAN. Independientemente del prisma, esta guerra probablemente condicionará el futuro de todas las FAS modernas.

Una vez descritos los componentes que influyen en la generación de un campo de batalla transparente, a continuación, se procederá a analizar las consecuencias vistas en las campañas ofensivas y contraofensivas llevadas a cabo en presencia de este en la guerra de Ucrania. El presente estudio se centra en el análisis del conflicto en torno a dos componentes contenidos en la doctrina nacional en vigor: las funciones conjuntas y los principios operativos (Ministerio de Defensa, 2024). Esta estructura permitirá obtener un modelo teórico sintetizado de implicaciones del campo de batalla transparente en la guerra de Ucrania, que además será comparable con la doctrina nacional.

2.2 Análisis de las funciones conjuntas

2.2.1 Mando y control

El conflicto en Ucrania presenta un entorno complejo para el mando y control, resaltando la necesidad de infraestructuras resilientes y seguras para mantener la superioridad informativa y la conexión en red. La digitalización del campo de batalla, la migración de datos a la nube y la hibridación de sistemas de comunicación, combinando redes civiles y militares, han permitido dar continuidad a las capacidades C3 en un entorno altamente dinámico, reduciendo la vulnerabilidad ante ataques físicos. Un claro ejemplo de esta tendencia es el empleo de satélites Starlink para

mitigar la pérdida de comunicaciones, así como la colaboración con empresas civiles para trasladar grandes volúmenes de información a infraestructuras en la nube, minimizando la exposición de los centros de datos físicos a ataques enemigos (Martí, 2024).

La gestión de la información plantea retos ante el exceso de datos que pueden generar infoxicación y afectar la eficacia del mando. Aunque la inteligencia artificial contribuye a su procesamiento, sigue condicionada por sesgos humanos. En Ucrania, se han documentado casos donde mandos priorizaron información procedente de retaguardia frente a unidades en contacto, fruto de esta sobrecarga informativa (Garnier y Néron-Bancel, 2024). Esta transparencia excesiva ha generado distorsiones en la toma de decisiones, demostrando la necesidad de estructurar de forma equilibrada la jerarquización de la información en el C2. El TG Agüero coincide con esta idea al manifestar que se debe contar con «Puestos de Mando minimalistas, capaces de trabajar en red, que delegan la ejecución en los escalones subordinados y controlan solamente aspectos muy específicos de la conducción», al mismo tiempo que advierte sobre los impedimentos que pueden aparecer para conseguir esto, debido a que los «medios técnicos actuales permiten un seguimiento de las operaciones muy seductor para el Mando, si bien innecesario y contraproducente»[8].

Desde luego, la problemática de la sobrecarga informativa no es nueva. Toffler (1970) advertía sobre cómo la aceleración de los flujos de información podía paralizar la toma de decisiones. En este contexto, el conflicto en Ucrania ha demostrado ser un caso paradigmático del uso masivo de imágenes, vídeos y narrativas informativas como herramienta de guerra. Tanto Rusia como Ucrania han explotado estos medios para influir en la percepción pública y en los procesos de decisión, generando un entorno en el que la rapidez con la que se difunde la información puede ser tan decisiva como las propias acciones militares. La capacidad de discriminar entre información relevante y «ruido» informativo se vuelve, por tanto, un elemento clave en la eficacia del C2 en escenarios contemporáneos.

El modelo de mando y control ruso ha mostrado una evolución hacia una mayor descentralización dentro de sus parámetros doctrinales tradicionales. Sin embargo, esta descentralización parcial no ha sido tan patente en todos los aspectos. La explotación de capacidades satelitales rusas ha sido ineficaz en el campo de

[8] Entrevista al TG Agüero.

batalla, a pesar de contar con una flota significativa de satélites militares. La falta de integración eficiente entre su infraestructura espacial y las operaciones terrestres ha impedido que Rusia obtenga ventajas estratégicas decisivas (El Radar, 2023).

Ucrania, por su lado y a pesar de no contar con satélites propios, ha usado imágenes satelitales de alta resolución procedentes de terceros, ha optimizado la identificación de movimientos rusos y ha incrementado la precisión de los ataques y la efectividad en la evaluación de daños (Dickey y Gleason, 2024). Esta experiencia destaca la importancia de la integración efectiva de capacidades espaciales con el mando y control, un aspecto en el que Ucrania ha demostrado mayor agilidad que Rusia.

Es de destacar que Rusia dispone de sistemas antisatélite (ASAT) como el misil Nudol, diseñado para neutralizar satélites en órbita baja, y el sistema láser Peresvet, capaz de cegar sus sensores ópticos (Dickey y Gleason, 2024). Sin embargo, el uso de capacidades cinéticas como el Nudol, no se ha materializado en el conflicto, probablemente por las implicaciones políticas que puede tener la destrucción física de un satélite. González (2025) considera que la explotación satelital todavía es ampliamente compartida por varios actores, civiles y militares, por lo que inutilizar un satélite empleado por un adversario puede conllevar pérdidas de servicios a actores ajenos al conflicto, y con ello una posible escalada y ampliación del conflicto a terceros, con consecuencias político-estratégicas no deseadas. Esto hace que la acciones en el espacio sean todavía difíciles de aplicar en conflictos no globales.

El análisis de estos factores resalta la necesidad de que las FAS prioricen la interoperabilidad entre distintos sistemas de C2 y refuercen la protección de sus redes ante amenazas cibernéticas y bloqueos de señal GPS. La creciente dependencia de infraestructuras digitales y espaciales impone la necesidad de desarrollar estrategias que garanticen la resiliencia en entornos altamente disputados. La experiencia en Ucrania ha demostrado que el éxito en el mando y control no solo depende de la sofisticación tecnológica, sino también de la capacidad para integrar eficazmente la información y evitar la saturación de los diferentes escalones de mando de cara a la toma de decisiones.

2.2.2 Maniobra

El conflicto en Ucrania ha ejemplificado cómo la evolución tecnológica condiciona el desarrollo de la maniobra operacional. Tras las

contraofensivas ucranianas de 2022, la guerra adoptó un carácter predominantemente posicional, caracterizado por frentes estáticos y combates de escasa movilidad, más bien parecidos a los vistos en la I Guerra Mundial. Este escenario ha restringido la ejecución de maniobras profundas capaces de penetrar defensas y explotar éxitos en retaguardia. Ni Rusia ni Ucrania han logrado claramente superar este desafío, como evidenciaron los casos de Bajmut (2023) y Avdiivka (2024), donde los avances quedaron limitados por la rápida reorganización de las defensas enemigas. De acuerdo con Kagan *et al*. (2024), la clave del problema para obtener resultados en la guerra de Ucrania radica en restaurar la maniobra operacional.

El progresivo estancamiento del conflicto responde a dos factores interrelacionados. En primer lugar, la creciente transparencia del campo de batalla, por la proliferación de sensores y su conectividad, ha restringido la libertad de movimiento y ha reducido la sorpresa operacional. En segundo lugar, la letalidad del fuego indirecto ha amplificado el desgaste sobre cualquier unidad, incrementando la vulnerabilidad de las fuerzas atacantes. Este fenómeno ha alimentado el debate doctrinal entre guerra de maniobra y guerra de desgaste. Los defensores de esta última argumentan que la transparencia ha eliminado la posibilidad de explotar la movilidad, transformando los enfrentamientos en duelos de fuegos indirectos sobre un terreno expuesto y altamente peligroso (Garnier y Néron-Bancel, 2024).

Jójart (2024) también coincide en estos puntos y añade que el estancamiento operacional ha llevado a repensar las estrategias tradicionales. En este contexto, los debates en Rusia han cuestionado la viabilidad de la estrategia de aniquilación en conflictos entre Estados con capacidades avanzadas, priorizando en su lugar una lógica de desgaste como método más efectivo frente a adversarios con reservas estratégicas considerables o coaliciones con alto poder de reposición. Henrotin (2023) señala que esta evolución ha desplazado el foco estratégico hacia la resiliencia económica e industrial, donde la prolongación del conflicto puede favorecer a la parte con mayor capacidad de reposición. En este sentido, el planeamiento operacional debe adaptarse a la realidad de conflictos de desgaste, donde la iniciativa se mantiene no solo mediante la maniobra, sino a través de la capacidad de sostener esfuerzos prolongados.

Romper el estancamiento en estos conflictos requiere anular la transparencia del campo de batalla enemigo afectando a sus

RSC, lo que podría lograrse mediante la destrucción de sus subsistemas de observación, fuegos o mando y control. El GB Frías analiza todas estas posibilidades para finalmente decantarse por la destrucción de los sensores/C2 como primera y mejor opción, puesto que «deja al enemigo ciego e incapaz de reaccionar con fuegos; si se destruyen los vectores de fuegos, solo lo dejamos con capacidad de reacción degradada». Por último, el general sentencia que para conseguir esto «Es necesario conocer en profundidad el sistema de sensores enemigo, identificar sus puntos débiles y actuar sobre ellos»[9].

La aviación, tradicionalmente el principal medio para contrarrestar estos sistemas de fuego, ha enfrentado dificultades debido a la densidad de las defensas antiaéreas. Sin embargo, Frías (2024) también considera que la eliminación de sistemas antiaéreos de largo alcance permitiría exponer el resto de la defensa antiaérea al fuego de la propia aviación, para posteriormente abrir la posibilidad de nuevos ataques aéreos que degraden los vectores de fuego de los RSC enemigos. Esto facilitaría la obtención de superioridad aérea en sectores clave, posibilitando con ello la viabilidad de la maniobra en un entorno operacional como el de la guerra de Ucrania.

Ante un panorama donde la transparencia y la letalidad del fuego reducen la capacidad de maniobra, las adaptaciones tecnológicas serán clave para restaurar su viabilidad operacional. La combinación de nuevas tecnologías con métodos tradicionales de ocultación y engaño será fundamental para recuperar la iniciativa y garantizar la efectividad operativa en futuros conflictos.

2.2.3 Fuegos

El uso masivo de sistemas ISR ha proporcionado a los comandantes una visión persistente del entorno operativo, permitiendo una integración eficaz de sensores y fuegos de precisión. Como resultado, la identificación y ataque de posiciones de artillería, depósitos logísticos y puestos de mando se ha vuelto más eficiente, reduciendo la necesidad de grandes volúmenes de munición y consolidando el concepto de «un disparo, una baja» (Kimmitt, 2024). Este cambio ha incrementado la capacidad de destrucción con un menor gasto de recursos, optimizando la eficiencia.

[9] Entrevista al GB Frías.

Ante la imposibilidad de establecer superioridad aérea, Ucrania ha adaptado sus fuegos de largo alcance para compensar la falta de aviación de ala fija, integrándolos con maniobras terrestres como alternativa a la interdicción aérea. Un ejemplo claro fue la batalla de Kherson en 2022, donde el empleo de artillería de precisión permitió alcanzar objetivos en profundidad sin apoyo aéreo, afectando la libertad de acción de las fuerzas rusas (Kagan *et al*., 2024). Este tipo de operaciones demuestra la importancia de coordinar los fuegos con las maniobras terrestres para maximizar su impacto operacional.

La materialización de esos fuegos en gran parte de la profundidad operacional ha modificado la dinámica del combate, imponiendo un desgaste sistemático sobre las unidades de maniobra incluso antes de que alcancen sus posiciones iniciales. En este contexto, el enfrentamiento entre RSC se ha convertido en una fase clave del conflicto. El GB Frías determina rotundamente que «Es imperativo degradar la operación del "complejo de reconocimiento y ataque" rival, al tiempo que se preserva el propio»[10]. Por ello, la supervivencia de la artillería ucraniana ha sido un factor determinante en la capacidad de penetración de sus fuerzas, apoyándose en sistemas avanzados como HIMARS y en la neutralización de la aviación rusa mediante defensa aérea y EW (Kagan *et al*., 2024).

Consecuencia de lo anterior, la zona de comunicaciones y zona de combate retrasada, tradicionalmente consideradas más seguras, han perdido su invulnerabilidad ante los ataques en profundidad. Los ataques ucranianos contra aeródromos rusos en Berdyansk y Lugansk en octubre de 2023 ilustran cómo la expansión del alcance de los sistemas de ataque ha incrementado la vulnerabilidad de los centros logísticos y de mando (Garnier y Néron-Bancel, 2024). Esto también lleva a replantearse que el alcance de los misiles balísticos obliga a reconsiderar el ámbito de aplicación de la defensa antiaérea y antimisil, que ya no puede concebirse únicamente para el interior de la zona de operaciones. Aquí, el TG. Agüero plantea que los PC «Para sobrevivir […] deberían estar, si pueden, fuera de la Zona de Operaciones Conjunta (JOA)» e incluso «contar con protección frente a Misiles Balísticos, bunquerizándose [sic.] cuando sea posible»[11].

[10] Entrevista al GB Frías.

[11] Entrevista al TG Agüero.

El CMOPS también muestra su preocupación por la logística, cuyos órganos «no pueden ubicarse fuera de la JOA»[12] por la propia razón de ser de sus actividades. Según el entrevistado, «su protección deberá basarse en su dispersión, replicación, pequeña huella y utilización de infraestructuras civiles»[13]. Efectivamente, la interrupción de la logística también ha sido un objetivo básico para los ataques en profundidad de cara a degradar la capacidad ofensiva rusa, con ataques dirigidos a líneas de comunicación terrestre (GLOC), depósitos de suministros y puntos de paso obligado. Estas acciones han buscado no solo debilitar la sostenibilidad del esfuerzo ruso en el frente, sino también impedir la movilización de reservas operacionales, afectando directamente la capacidad de refuerzo y explotación del enemigo (Kagan *et al*., 2024).

Dentro de esta estrategia de interdicción, especialmente significativos han sido los ataques contra depósitos de combustible, impactando en el sostenimiento de las fuerzas rusas. A lo largo del conflicto, Ucrania ha ejecutado operaciones contra instalaciones críticas en Crimea, Belgorod y Kursk, utilizando drones y misiles de largo alcance para limitar el abastecimiento de vehículos blindados y aeronaves. La destrucción de infraestructuras petroleras, como la refinería en Krasnodar, afectó temporalmente la producción de combustible, restringiendo la capacidad operativa rusa en el frente. De manera similar, los ataques coordinados contra redes ferroviarias y depósitos logísticos han retrasado los despliegues, exponiendo vulnerabilidades en la estructura de transporte del adversario (Rodríguez, 2024).

En el dominio marítimo, el empleo de drones navales ha permitido a Ucrania proyectar poder a distancia sin exponer a su personal, convirtiéndose en una herramienta clave en la lucha contra la Flota del mar Negro rusa. La combinación de motos acuáticas explosivas y sistemas de guiado remoto ha demostrado la viabilidad de la guerra asimétrica en el ámbito naval, obligando a la flota rusa a reposicionarse y reforzar sus defensas. Esta estrategia ha limitado la operatividad rusa en el mar Negro, condicionando su capacidad de proyectar fuerzas desde Crimea y afectando su influencia sobre las rutas de suministro marítimo (Martí, 2024). De nuevo y de una manera similar al dominio aéreo, a pesar de que Rusia disponía de una fuerza aérea y una flota superiores,

12 Entrevista al TG Agüero.

13 Entrevista al TG Agüero.

Ucrania ha podido privar a las fuerzas rusas de libertad de acción mediante la explotación del empleo de drones.

El conflicto en Ucrania ha consolidado un nuevo paradigma en el empleo de los fuegos. La combinación de sistemas ISR y ataques en profundidad desde diferentes medios productores han permitido a ambos bandos degradar capacidades ofensivas adversarias. La integración de sistemas no tripulados, la coordinación entre fuegos y maniobra, y el ataque a nodos críticos han sido elementos clave para reducir la libertad de acción del adversario. Si la maniobra ha sido una de las grandes perjudicadas por el campo de batalla transparente, los fuegos se han alzado como dominantes en el conflicto, equilibrando capacidades entre ambos bandos, tanto en operaciones ofensivas, como defensivas.

2.2.4 Información

En Ucrania, se ha podido apreciar la creciente relevancia del dominio cognitivo, donde la desinformación y la guerra psicológica desempeñan un papel determinante en la moral, la percepción del conflicto y la toma de decisiones. Ucrania ha sabido explotar el entorno informativo para fortalecer su narrativa y garantizar el apoyo internacional. La difusión de éxitos militares a través de redes sociales y medios de comunicación, gracias también a la «democratización» de las operaciones a través de la población civil, ha sido clave para movilizar la opinión pública en otros estados, facilitando el continuo flujo de asistencia militar y financiera. La capacidad de capitalizar el impacto psicológico de la guerra ha consolidado una imagen de resistencia efectiva, un factor crucial para mantener la cohesión interna y la credibilidad ante sus colaboradores (Rodríguez, 2024). Así, la información no solo ha servido como un mecanismo de defensa y legitimación, sino también como una herramienta de proyección de poder, condicionando la respuesta internacional al conflicto para sostener el apoyo de material y militar, imprescindible en el carácter de desgaste que adquirió el conflicto.

A nivel puramente operacional, el empleo coordinado de acciones en los dominios cognitivo y ciberespacial ha sido determinante en el apoyo a la maniobra. Boyer y Becker (2024) destacan que, en la operación en el *oblast* de Kursk de 2024, Ucrania aplicó un alto nivel de secreto (OPSEC), restringiendo las comunicaciones electrónicas para evitar intercepciones y empleando acciones de desinformación dirigidas a confundir al adversario sobre las

verdaderas intenciones de la maniobra. Este enfoque fue complementado con una integración eficaz de EW y ataques en profundidad contra sistemas ISR rusos, limitando la capacidad de detección del enemigo y facilitando la maniobra terrestre para la ocupación de territorio ruso, sin una respuesta inmediata.

Además del empleo de fuegos de precisión, las fuerzas ucranianas han recurrido a estrategias de decepción para contrarrestar la transparencia del campo de batalla y desorientar al enemigo. Un ejemplo significativo fue la simulación de desembarcos anfibios en el mar Negro por parte de la flota rusa, lo que llevó a Ucrania a desviar recursos hacia sectores que finalmente no fueron atacados (Rodríguez, 2024). También se han utilizado drones como señuelos para forzar a las defensas antiaéreas rusas a revelar sus posiciones, facilitando ataques contra baterías de misiles y radares (Martí, 2024). TRADOC (2024) también respalda este enfoque y enfatiza que la desinformación y la sobrecarga cognitiva se han convertido en herramientas esenciales para alterar la percepción del enemigo y condicionar sus decisiones. Estos casos demuestran que, incluso en un entorno de alta visibilidad, el engaño empleando métodos ya vistos en otros conflictos del pasado, sigue siendo una herramienta clave para obtener ventajas operacionales.

2.3 Análisis de los principios operativos

2.3.1 Sorpresa

Durante el conflicto en Ucrania, ambas partes han recurrido a estrategias de desinformación y maniobras inesperadas para generar incertidumbre en el enemigo. Aunque la vigilancia constante dificulta el secretismo, operaciones como la contraofensiva de Járkov en 2022, donde Ucrania reunió cinco brigadas sin ser detectada (Garnier y Néron-Bancel, 2024), sugieren que la sorpresa sigue siendo posible con planeamiento meticuloso, inteligencia precisa y una combinación de fuegos, EW y operaciones en profundidad.

Otros métodos como la aplicación de esfuerzos en varios puntos para ocultar el esfuerzo principal, como en la contraofensiva ucraniana hacia Melitopol (2023) o la reinvasión rusa de Járkov (2024) también se han visto en las campañas. La introducción de tecnologías innovadoras ha generado valiosas oportunidades,

como el impacto de los HIMARS en las acciones de interdicción o el uso ruso de EW para interferir comunicaciones y navegación (Kagan *et al*., 2024). No obstante, la sorpresa es efímera y solo resulta decisiva si se explota de inmediato, aislando sectores de penetración y retrasando la respuesta del enemigo con ataques de largo alcance sobre líneas logísticas y PC.

Otros muchos ejemplos que buscaban la sorpresa ya se han tratado anteriormente: la maniobra diversiva en el mar Negro para simulación de desembarcos por parte de la flota rusa obligó a Ucrania a desviar recursos a sectores nunca atacados (Rodríguez, 2024); la ofensiva de Kursk de 2024 que logró sorprender a las fuerzas rusas mediante la minimización de la huella electrónica, la difusión de información falsa y ataques a infraestructuras ISR enemigas para degradar su capacidad de detección (Boyer y Becker, 2024); el uso generalizado de drones señuelo que permitió engañar a las defensas antiaéreas rusas, revelando sus posiciones y facilitando ataques de precisión (Martí, 2024). Todo ello, a pesar de la visibilidad del entorno, permitieron materializar éxitos locales y potencialmente explotables a nivel operacional.

En realidad, la sorpresa no solo parece seguir siendo posible, sino que es un aspecto capital de la guerra. El TG Agüero reflexiona sobre las contraofensivas ucranianas de 2022 y 2023, y sobre la importancia de la sorpresa:

> «La contraofensiva ucraniana en el verano de 2023 vino precedida de otra muy exitosa unos meses antes. Tras una ruptura del frente sorpresiva, no sabemos las razones por las que el Mando ucraniano frenó la explotación de su éxito; falta de apoyo logístico, agotamiento de su capacidad ofensiva, temor a enfrentarse a obstáculos o posiciones defensivas más organizadas, consolidar lo ganado ante una posible reacción rusa… Sea como fuere, el terreno que no se reconquistó entonces no pudo recuperarse posteriormente. Es probable que el éxito de aquella contraofensiva sorprendiera a los ucranianos ¿Habría sorprendido a los rusos si no hubiera sorprendido antes a sus adversarios? Sin embargo, la esperada ofensiva ucraniana durante el verano de 2023 no dio los frutos previstos. Los ucranianos habían acumulado más medios pero los rusos se habían organizado mejor, aprendiendo la lección. Ante una confrontación equilibrada, la sorpresa parece proporcionar más réditos que la preparación»[14].

[14] Entrevista al TG Agüero.

También lo hace el GB Bados, desglosando posibles errores de la contraofensiva del 2023, a la que achaca haber sido una «contraofensiva «telegrafiada» y por ello presentar una «ausencia de sorpresa»[15], como motivo principal de su fracaso.

Del Castillo (2024) sostiene que la transparencia tecnológica no elimina la sorpresa si el adversario no puede reaccionar a tiempo, permitiendo aprovechar brechas en su proceso de mando y control. Por su parte, Frías (2024) concluye que la sorpresa, bien aplicada, sigue siendo un elemento crucial para alterar el equilibrio del combate y explotar vulnerabilidades en un entorno dominado por la vigilancia constante. Y finalmente, el TG Agüero también considera que el efecto sorpresa es el «único factor que parece permitir movimientos rápidos en este conflicto»[16].

El entorno operativo actual favorece la detección temprana, pero no impide la sorpresa si se emplean métodos adecuados. Como demuestran las campañas en Ucrania, la combinación de guerra electrónica, ciberataques y operaciones de engaño puede crear ventanas de «opacidad» que interrumpan temporalmente la capacidad del enemigo para analizar la situación y tomar decisiones, permitiendo alcanzar la sorpresa necesaria para llevar la iniciativa ante el adversario.

2.3.2 Concentración

El éxito ofensivo en los conflictos actuales no depende únicamente de la acumulación masiva de fuerzas, sino de la capacidad para generar superioridad localizada y temporal en sectores clave. Esta superioridad debe mantenerse el tiempo suficiente para alcanzar los objetivos operacionales sin comprometer la estabilidad general de la zona de operaciones (Kagan *et al*., 2024). La concentración eficaz requiere no solo una adecuada disposición de fuerzas, sino también la integración de sistemas de apoyo que permitan sostener la maniobra sin exponerse a contraataques inmediatos.

Durante las fases de penetración, explotación y consolidación, la protección de las concentraciones críticas es fundamental. Esto exige un RSC robusto y autónomo, apoyado por EW y CUAS para neutralizar la capacidad de respuesta enemiga. La integración de drones no solo ha complementado la artillería y las maniobras mecanizadas, sino que se ha convertido en un elemento clave

15 Entrevista al GB Bados.

16 Entrevista al TG Agüero.

para preservar la iniciativa en el campo de batalla, dificultando la reconfiguración de las fuerzas enemigas (Kagan *et al*., 2024).

En escenarios donde la concentración física de fuerzas es inviable o arriesgada, la dispersión controlada y el uso de formas alternativas de masa han demostrado ser herramientas eficaces. Estrategias como el empleo de enjambres de drones señuelo han permitido dispersar los recursos enemigos, obligándolos a dividir su capacidad de respuesta y generando una ventaja relativa sin necesidad de concentrar grandes unidades (Garnier y Néron-Bancel, 2024). Este enfoque amplía las opciones de maniobra y reduce la vulnerabilidad ante fuegos de precisión o ataques en profundidad.

El general Valerii Zaluzhnyi, excomandante en jefe de las Fuerzas Armadas de Ucrania, enfatizaba que los drones y otras plataformas autónomas han pasado de ser un complemento para convertirse en un pilar central de las operaciones militares. Su capacidad para compensar la inferioridad en recursos frente a Rusia ha sido clave en la evolución del conflicto. Zaluzhnyi (2024) destacaba, además, que estos sistemas permiten superar las limitaciones de la guerra posicional, desarticulando las líneas enemigas sin recurrir a grandes concentraciones de tropas, reduciendo bajas propias y maximizando el impacto sobre el adversario. Esta evolución confirma la tendencia hacia un modelo de combate donde la automatización y el dominio del espectro electromagnético se consolidan como factores determinantes en la obtención de ventajas operacionales sostenibles.

2.3.3 Continuidad

La sostenibilidad de la ofensiva en Ucrania depende de su capacidad para mantener el impulso hacia los objetivos operacionales sin permitir que el adversario recupere la iniciativa. Esto exige no solo la progresión constante de la maniobra, sino también el refuerzo simultáneo de capacidades de apoyo que permitan sostener la acción en el tiempo. La expansión de la cobertura de defensa aérea y antimisiles, el sostenimiento continuo de las fuerzas en avance y la consolidación de posiciones clave a lo largo del eje de explotación son elementos esenciales para evitar que la ofensiva pierda eficacia antes de alcanzar sus objetivos (Kagan *et al*., 2024).

Como no podría ser de otra manera, la logística juega un papel clave en ese sostenimiento del esfuerzo, condicionando el éxito.

Tratando la ofensiva ucraniana de Kursk en 2024, el GB Bados considera que la operación «supuso un sobre estiramiento de las líneas logísticas como consecuencia de la ampliación del frente, lo que supuso la imposibilidad del mantenimiento de ese frente con los recursos adecuados por la falta de personal y medios necesarios para mantenerlo»[17]. En última instancia, y a pesar de haber atacado por sorpresa en ese punto, el no poder atender al principio de continuidad puede terminar por llevar a no consolidar objetivos operacionales.

Garantizar la continuidad también implica neutralizar la capacidad de reorganización del enemigo. Incluso tras aislar fuerzas defensivas, es crucial impedir su reconstitución o su capacidad para interferir en las operaciones ofensivas, empleando la interdicción de nodos logísticos, por ejemplo. La supresión temporal del RSC enemigo también ha sido determinante para reducir el coste y asegurar la progresión hasta objetivos operacionales en profundidad (Kagan *et al*., 2024). De este modo, el esfuerzo no solo debe centrarse en la maniobra en sí misma, sino en la ejecución sincronizada de acciones complementarias que garanticen su éxito y reduzcan la posibilidad de una reacción efectiva del adversario.

El conflicto en Ucrania ha demostrado que la continuidad no es solo un problema de movilidad, sino de integración de esfuerzos en múltiples dominios. La combinación de superioridad aérea local, guerra electrónica y fuegos de largo alcance resulta tan decisiva como la maniobra terrestre para sostener el impulso ofensivo. La clave radica en impedir que el enemigo imponga tiempos de recuperación, asegurando que la ofensiva avance con la menor fricción posible hasta la consecución de sus objetivos.

2.4 Conclusiones. Síntesis del modelo teórico

A continuación, se presentan las conclusiones derivadas del estudio, estructuradas en relación con los componentes doctrinales previstos. Estas síntesis de lecciones operacionales extraídas de las campañas de la guerra de Ucrania que guardan una relación directa con los componentes estudiados del campo de batalla transparente, conforman los modelos teóricos que serán comparados con la doctrina en vigor durante el apartado siguiente.

[17] Entrevista al GB Bados.

2.4.1 Mando y control

En un entorno de alta transparencia, el mando y control debe garantizar continuidad operativa y evitar la saturación informativa. La descentralización, siguiendo la filosofía de Mando orientado a la misión, y la redundancia de comunicaciones mediante redes híbridas permiten sostener el mando en entornos hostiles.

El C2 debe integrarse con capacidades multidominio, sincronizando ISR, EW y ciberdefensa para mantener la ventaja operativa. El espacio se ha convertido en un dominio crítico, ya que el acceso a satélites y sensores define la superioridad en la producción de inteligencia y explotación de sistemas de armas.

Por último, la negación de la transparencia enemiga mediante guerra electrónica y ataques a redes ISR es clave para evitar que el adversario explote su propia ventaja tecnológica.

2.4.2 Maniobra

La maniobra operacional ha sido restringida por la transparencia del campo de batalla y la letalidad del fuego indirecto, lo que ha favorecido la guerra de desgaste sobre la movilidad.

La neutralización del ISR o de los fuegos enemigos es una condición previa para cualquier maniobra exitosa. Sin esta acción, cualquier intento de penetración quedará expuesto y tendrá altas probabilidades de ser degradado.

La combinación de ocultación, engaño y tecnologías emergentes favorece recuperar parte de la iniciativa y generar oportunidades de maniobra en entornos altamente vigilados.

2.4.3 Fuegos

En un entorno de alta transparencia, los fuegos se han convertido de nuevo en un eje de diseño para las campañas. La integración de ISR avanzado con armamento de precisión ha permitido atacar objetivos clave con una reducción relativamente significativa del consumo de munición y un incremento en la letalidad.

Ante la dificultad de obtener superioridad aérea, los fuegos de largo alcance pueden asumir funciones de interdicción en gran parte de la profundidad. En este contexto, la retaguardia ya no es invulnerable a pesar de las condiciones de superioridad aérea, y los ataques contra nodos logísticos, puestos de mando

y redes de comunicación serán altamente prioritarios para limitar la libertad de acción del adversario, si bien la forma de realizarlos se ha diversificado más allá de la aviación. Los fuegos ya no solo buscan la destrucción de fuerzas enemigas, sino que alteran el ritmo operacional del adversario, limitando su capacidad de reconstituirse y sostener el combate incluso en la zona de comunicaciones.

La defensa aérea es un pilar central, compensando la falta de superioridad aérea en escenarios donde la aviación enemiga es teóricamente superior de manera persistente. La intercepción de misiles, aeronaves tripuladas y drones de cualquier clase requiere un sistema escalonado y multiefector de defensa, combinando capacidades aéreas y antiaéreas con tecnologías emergentes.

Dado que la saturación del espacio de batalla con drones y municiones guiadas seguirá aumentando, la automatización de la defensa aérea y su integración con otros sistemas de combate serán esenciales para garantizar la resiliencia operativa. La capacidad de una fuerza para adaptarse a estos desafíos determinará su capacidad de supervivencia y libertad de acción en el combate moderno.

La guerra naval ha seguido la misma tendencia, con drones navales y armas de precisión permitiendo la negación del mar sin exposición directa. La integración de fuegos con sistemas no tripulados y guerra electrónica ha demostrado ser esencial para imponer un desgaste constante y condicionar las acciones del enemigo.

2.4.4 Información

El modelo teórico de información se basa en el dominio del entorno informativo para condicionar la percepción del adversario, reforzar la cohesión interna y generar ventajas estratégicas beneficiosas para el nivel operacional.

Las operaciones de información (INFOOPS) son imprescindibles, no solo para afectar a la moral del adversario y proteger la propia, sino también para condicionar el entorno político y estratégico aliado. La capacidad de un actor para controlar la narrativa del conflicto puede traducirse en ventajas como la movilización de apoyo internacional o la desmoralización de las fuerzas enemigas.

En este contexto, la sincronización de acciones en los dominios cognitivo y ciberespacial es fundamental. No basta con la difu-

sión de propaganda o la manipulación informativa, sino que estas acciones deben integrarse con medidas OPSEC, guerra electrónica y operaciones de decepción para reforzar su impacto y posibilitar competir en entornos de alta transparencia.

La decepción operacional sigue siendo viable incluso en un entorno de alta transparencia. Los ataques diversivos, el uso de señuelos y la sobrecarga informativa pueden forzar al enemigo a tomar decisiones erróneas o desviar recursos de manera inefectiva.

SUBCOMPONENTE	CONCLUSIONES
Mando y control	- Sistemas C3 descentralizados y resilientes ante acciones físicas y cognitivas - Integración multidominio - Espacio como dominio clave con gran potencial - Negación de la transparencia al enemigo
Maniobra	- La transparencia genera tendencia a la guerra posicional y de desgaste - Neutralizar el ISR o fuegos enemigos es requisito previo a la maniobra - Integración de ocultación, engaño y tecnologías emergentes para favorecer la maniobra

SUBCOMPONENTE	CONCLUSIONES
Fuegos	- Imprescindibles en las campañas - Fuegos de largo alcance pueden suplir carencias de poder aéreo y generar efectos similares, en presencia de defensa aérea - Generan pérdida de seguridad en la retaguardia y mayor posibilidad de interdicción - Integración eficaz de sistemas no tripulados y acciones multidominio en el sistema de fuego - Defensa aérea escalonada y automatizada para contrarrestar todas las amenazas, convencionales y no convencionales
Información	- INFOOPS como herramientas clave para afectar a la moral del adversario, proteger la propia y conseguir apoyos estratégicos - Sincronización de acciones en el dominio cognitivo y ciber - Ataques diversivos, señuelos y sobrecarga informativa del adversario favorecen la decepción operacional

Tabla 1. Modelo teórico sobre funciones conjuntas en la guerra de Ucrania
Fuente: elaboración propia

2.4.5 Sorpresa

A pesar de la alta transparencia del campo de batalla, la sorpresa sigue siendo un principio operativo viable cuando se combinan decepción, ocultación y explotación rápida de oportunidades. La vigilancia constante dificulta el secretismo, pero no impide generar incertidumbre en el enemigo mediante desinformación, minimización de huella electrónica y ataques a infraestructuras ISR.

La sorpresa en conflictos modernos no se basa únicamente en la ocultación de fuerzas, sino en la capacidad para generar percepciones erróneas en el adversario y explotar los retrasos en su toma de decisiones. La guerra electrónica, los ciberataques y las operaciones diversivas pueden crear ventanas de opacidad temporales, afectando la capacidad del enemigo para analizar la situación y reaccionar a tiempo.

Para ello, es esencial aislar sectores de penetración y degradar la capacidad de respuesta enemiga con ataques sobre sus nodos de mando y logística. La sorpresa ya no consiste solo en atacar donde no se espera, sino en impedir que el enemigo reaccione con la suficiente rapidez.

El uso de tecnologías, como los HIMARS en interdicción o el empleo de drones señuelo para exponer defensas antiaéreas, demuestra que la sorpresa puede lograrse incluso en un entorno donde la detección es casi inmediata. La clave radica en interrumpir el proceso de decisión del adversario y explotar las brechas generadas antes de que pueda adaptarse.

2.4.6 Concentración

El éxito ofensivo en conflictos modernos no depende necesariamente de la acumulación masiva de fuerzas, sino de la generación de superioridad localizada y temporal en sectores clave. En los casos en los que sea necesario la concentración física, su protección es esencial durante las fases de penetración, explotación y consolidación. Un RSC robusto y autónomo, combinado con EW y CUAS, puede permitir neutralizar la capacidad de respuesta enemiga y evitar la disrupción de la ofensiva.

Cuando la concentración física de fuerzas es inviable o arriesgada, la dispersión controlada y el uso de formas alternativas de masa han demostrado ser eficaces. Estrategias como el uso de enjambres de drones señuelo permiten dispersar la capacidad de

respuesta del enemigo, generando una ventaja relativa sin necesidad de concentrar grandes unidades.

El uso de sistemas autónomos y el dominio del espectro electromagnético han modificado la forma en que se logra la concentración en combate. La capacidad de los drones para degradar la capacidad operativa del adversario sin recurrir a grandes acumulaciones de tropas reduce las bajas propias y maximiza el impacto operacional.

2.4.7 Continuidad

La continuidad de la ofensiva es esencial para evitar que el adversario recupere la iniciativa antes de alcanzar los objetivos operacionales. Mantener el impulso ofensivo requiere no solo una progresión constante y sostenida de la maniobra, sino también el refuerzo simultáneo de capacidades de apoyo, como el sostenimiento logístico, la consolidación de posiciones y la expansión de la cobertura de defensa antiaérea.

La integración de esfuerzos en múltiples dominios también ofrece una importante palanca a la hora de sostener el impulso ofensivo. Superioridad aérea local, guerra electrónica y fuegos de largo alcance deben combinarse con la maniobra terrestre para evitar que el enemigo imponga tiempos de recuperación y generar una progresión sostenida con la menor fricción posible.

Garantizar la continuidad implica impedir la reorganización del enemigo incluso después de aislar sus fuerzas defensivas. Todo ello pasa por lograr neutralizar su capacidad de reconstitución y reacción mediante supresión del RSC, ataques en profundidad e interdicción logística. La ofensiva no solo debe centrarse en el avance territorial, sino en la ejecución sincronizada de acciones complementarias que aseguren su éxito y minimicen la reacción enemiga

SUBCOMPONENTE	CONCLUSIONES
Sorpresa	- Requiere combinar decepción, ocultación y explotación rápida (impedir que el enemigo comprenda intenciones propias, que observe movimientos propios y que reaccione a tiempo y eficazmente) - Uso de tecnologías e innovaciones para interrumpir proceso de decisión enemigo
Concentración	- Generar superioridad localizada y temporal en sectores clave - Proteger las concentraciones físicas necesarias - Buscar formas alternativas de masa, como el empleo de sistemas autónomos extensivamente o la dispersión del enemigo
Continuidad	- Progresión sostenida de la maniobra, apoyada de forma continuada por fuegos, protección y apoyo logístico. - Integración de apoyos en todos los dominios - Impedir constantemente la reorganización de capacidades del enemigo, sobre todo de fuegos

Tabla 2. Modelo teórico sobre principios operativos en la guerra de Ucrania
Fuente: elaboración propia

3 Implicaciones doctrinales

3.1 Introducción

Llegado este punto y tras analizar las campañas de la guerra de Ucrania previstas para el presente trabajo bajo los efectos de un campo de batalla transparente, a continuación, se establece la relación comparativa entre los modelos teóricos extraídos del conflicto actual con las premisas doctrinales previstas en los textos oficiales, concretamente en la PDC-01(B) y la PDC-3, ambos máximos exponentes de la doctrina conjunta de operaciones objeto del presente trabajo.

Este análisis permitirá evaluar en qué medida la doctrina conjunta española recoge las implicaciones operacionales derivadas de la alta transparencia en el entorno de combate moderno. Para ello, se examinarán las funciones conjuntas y principios operativos estudiados en función de su capacidad para responder a los desafíos detectados en Ucrania, identificando aquellas áreas en las que la doctrina proporciona un marco suficiente y aquellas en las que podría beneficiarse de una mayor adaptación.

3.2 Implicaciones para la doctrina conjunta

3.2.1 Mando y control

El concepto de C3 resiliente ante acciones físicas y cognitivas está indirectamente recogido en la doctrina mediante la necesidad de asegurar la continuidad del mando y la interoperabilidad en entornos disputados en todos los dominios (Ministerio de Defensa, 2024). Por su parte en la PDC-3 se describe que un sistema de mando y control debe ser «robusto, redundante y protegido para facilitar el desarrollo de la operación» (EMAD, 2021: 99). La descentralización y el concepto de mando orientado a la misión está completamente recogido en ambas PDC (Ministerio de Defensa, 2024 y EMAD, 2021).

La integración multidominio es un aspecto nuclear en ambas doctrinas. La PDC-01(B) define las MDO como aquellas que requieren una integración efectiva de todos los dominios, incluyendo el terrestre, marítimo, aéreo, espacial, ciberespacial y cognitivo (Ministerio de Defensa, 2024). La PDC-3 complementa esta visión

al señalar que la interoperabilidad y conectividad son esenciales para la efectividad de las operaciones (EMAD, 2021).

El espacio como dominio clave también está reconocido. La PDC-01(B) describe el dominio espacial como un ámbito global con un impacto creciente en las operaciones militares (Ministerio de Defensa, 2024). Si bien es cierto que su explotación no está desarrollada con el mismo nivel de detalle que otros dominios, especialmente en la PDC-3 que todavía lo concibe como aeroespacial (EMAD, 2021).

La negación de la transparencia al enemigo se encuentra respaldada en la doctrina militar española, aunque no de manera explícita. La PDC-01(B) establece la importancia de la negación de la libertad de acción al adversario mediante la combinación de medios cinéticos y no cinéticos, incluyendo la guerra electrónica y la ciberdefensa, lo que limita su capacidad de reconocimiento y targeting en la zona de operaciones (Ministerio de Defensa, 2024). Además, el documento destaca que la integración de capacidades en todos los ámbitos es esencial para restringir la capacidad del adversario de desplegar y emplear sus sistemas de combate. La PDC-3 no menciona explícitamente la negación de la transparencia al enemigo, pero sí proporciona fundamentos que la respaldan. Destaca el control del espectro electromagnético y la guerra electrónica como herramientas clave para interrumpir redes de comunicaciones enemigas y degradar su capacidad de adquisición de blancos. También menciona la supresión de sistemas de vigilancia y reconocimiento enemigos para limitar su conocimiento del entorno operativo (EMAD, 2021). Estos principios, aunque implícitos, justifican la necesidad de consolidar la negación de transparencia como una función clave del mando y control en la doctrina.

3.2.2 Maniobra

La PDC-01(B) y la PDC-3 contienen referencias parciales a la maniobra, alineándose con algunas de las lecciones de la guerra en Ucrania, aunque sin abordar explícitamente ciertos elementos clave. La doctrina reconoce que la alta visibilidad en el campo de batalla afecta a la movilidad y favorece una guerra posicional, aunque no lo desarrolla como un factor determinante en la pérdida de la maniobra operacional, la cual va más allá del movimiento de capacidades (EMAD, 2021). Se menciona que la maniobra debe buscar posiciones de ventaja desde las que des-

organizar al adversario y, sobre todo, obtener efectos decisivos (Ministerio de Defensa, 2024), lo que sugiere una tendencia a eludir el desgaste prolongado.

Respecto a la neutralización del ISR y fuegos enemigos como requisito previo a la maniobra, la doctrina destaca la interdicción y la supresión de sistemas C2 como medios para degradar la capacidad operativa del enemigo antes de una ofensiva. Se menciona que los fuegos profundos y la EW deben emplearse para impedir la reconfiguración del adversario y limitar su capacidad de respuesta (EMAD, 2021). Sin embargo, no se establece una metodología clara sobre cómo lograrlo de manera sistemática.

En cuanto a la integración de ocultación, decepción y tecnologías emergentes para favorecer la maniobra, la doctrina reconoce el uso de estas medidas, pero especialmente menciona la importancia de la decepción para ocultar las intenciones al adversario, hasta el momento y lugar apropiados para aplicar la capacidad de combate sobre el enemigo (EMAD, 2021), siendo las actividades de la función conjunta maniobra las encargadas de garantizar que las capacidades son dispuestas en lugar y momento oportunos (Ministerio de Defensa, 2024) mostrando una relación intrínseca entre todos los conceptos.

No obstante, como se ha comentado, no se detalla su aplicación específica ni el papel de las tecnologías emergentes como los sistemas autónomos, de cara a la restauración de la maniobra operacional, aunque sí es cierto que las tecnologías ocupan un papel predominante a lo largo de ambos textos doctrinales en lo relativo a la importancia de todas ellas para el éxito de las operaciones.

3.2.3 Fuegos

La PDC-01(B) y la PDC-3 contienen referencias parciales a la función conjunta fuegos, alineándose con algunas de las lecciones de la guerra en Ucrania, aunque, de nuevo, ciertos aspectos no se abordan de manera explícita.

La doctrina reconoce que los fuegos son imprescindibles en las campañas, destacando su papel en la interdicción y la limitación de la libertad de acción del enemigo. Se enfatiza la importancia de la integración del targeting conjunto, combinando fuegos con ISR para maximizar su efectividad (EMAD, 2021).

El uso de fuegos de largo alcance como alternativa parcial al poder aéreo está mencionado en la doctrina, en el contexto de la interdicción, sin necesidad de superioridad aérea. No obstante, no se desarrolla explícitamente cómo estos fuegos pueden compensar la carencia de aviación en un entorno de fuerte defensa aérea enemiga (EMAD, 2021).

La pérdida de seguridad en la retaguardia y la mayor posibilidad de interdicción a unidades propias pueden detectarse en la doctrina cuando desarrolla conceptos como el A2/AD (*Anti-Access/ Area Denial*). El AD busca la restricción de libertad de acción dentro de una zona mediante el uso integrado y de gran alcance de sensores, sistemas de misiles y mando y control centralizado (Ministerio de Defensa, 2024 y EMAD, 2021), tal y como se concibe en el concepto de campo de batalla transparente a través de los RSC. Esto orienta a entender que las fuerzas propias sufrirán los efectos de los fuegos a lo largo de toda la profundidad del despliegue, más allá de las fuerzas en contacto. En el sentido contrario, los alcances propios también deberán continuar atacando áreas en retaguardia enemiga para generar efectos de palanca sobre las fuerzas en contacto, mediante la interdicción y, efectivamente, la doctrina contempla ampliamente este aspecto, sin especificar la necesidad de que sea aéreo.

Respecto a la integración de sistemas no tripulados y acciones multidominio en los fuegos, la doctrina menciona la importancia de la coordinación con capacidades cibernéticas, guerra electrónica y fuego de precisión unificados bajo el proceso de *targeting* (Ministerio de Defensa, 2024). No obstante, no se aborda en profundidad el papel específico de drones navales o terrestres en la negación de espacios al enemigo.

Por último, la defensa aérea escalonada y automatizada para contrarrestar amenazas convencionales y no convencionales no está recogida de manera explícita en la doctrina. Aunque se menciona la importancia de la defensa aérea y la protección de fuerzas, no se desarrolla un enfoque integral que contemple la automatización y la respuesta a drones y municiones merodeadoras (EMAD, 2021). Sí se contempla la «obligación de incorporar la tecnología a las capacidades militares» (Ministerio de Defensa, 2024: 7) como tendencia general de los conflictos, mencionando a los sistemas autónomos, lo que hace que la doctrina no sea ajena a la situación general actual.

3.2.4 Información

La PDC-01(B) y la PDC-3 recogen las implicaciones de la función conjunta información, incluyendo el impacto de las INFOOPS en la moral del adversario, la sincronización del dominio cognitivo y ciberespacial, y el uso de la decepción como herramienta operacional.

Las INFOOPS son descritas como una función clave para influir en la voluntad, percepciones y capacidades del adversario, protegiendo al mismo tiempo la narrativa propia. Concretamente, reconoce su papel en la cohesión interna y el apoyo estratégico, destacando la importancia de integrar la comunicación estratégica (STRATCOM) para inducir actitudes favorables a las operaciones (EMAD, 2021).

La sincronización de acciones en el dominio cognitivo y ciberespacial está presente en la doctrina, mencionando la necesidad de combinar guerra electrónica y las INFOOPS para afectar el proceso de decisión del adversario (EMAD, 2021). No obstante, no se especifica con claridad cómo esta sincronización debe integrarse a nivel operacional para facilitar maniobras y operaciones ofensivas.

Por otro lado, el uso de ataques diversivos, señuelos y sobrecarga informativa como parte de la decepción militar y orientada a confundir al adversario no se contempla explícitamente. De hecho, la decepción es ampliamente mencionada en la doctrina, pero no se encuentra desarrollada intensivamente, ni en la PDC-1(B) ni en la PDC-3. Es decir, las formas de aplicar la decepción u organizar los planes de decepción no se encuentran desarrollados a nivel conjunto. Realmente, esta carencia resulta llamativa, dada la importancia que se le atribuye al engaño/decepción dentro de las operaciones en ambientes de alta transparencia en general, y en la guerra de Ucrania en particular.

3.2.5 Sorpresa

La PDC-01(B) recoge el principio de sorpresa, estableciendo que su éxito depende de la ejecución rápida, la confidencialidad y el engaño. La doctrina enfatiza que la sorpresa genera confusión en el enemigo, afectando su cohesión y moral, lo que permite obtener y mantener la iniciativa. Asimismo, reconoce la dificultad de lograr la sorpresa en un entorno donde las nuevas tecnologías incrementan la transparencia del campo de batalla, subrayando la necesidad de medidas de ocultación, negación de información y acciones inesperadas (Ministerio de Defensa, 2024).

El uso de decepción, ocultación y explotación rápida para impedir que el enemigo comprenda las intenciones propias y reaccione a tiempo está asociado al mencionado concepto de decepción militar. Como ya se ha comentado, es destacable la necesidad de ocultar las verdaderas intenciones hasta el momento oportuno, para explotar vulnerabilidades críticas del adversario (EMAD, 2021). No obstante, la doctrina no desarrolla concretamente cómo debe ser su aplicación ni cómo este enfoque debe integrarse en las operaciones.

Respecto al uso de tecnologías e innovaciones, la doctrina menciona que la sorpresa interrumpe el proceso de decisión del enemigo al obligarlo a reaccionar en condiciones imprevistas y desfavorables. Mediante el uso de tecnologías e innovaciones, se pueden generar dilemas que desorganizan su respuesta y lo fuerzan a emplear procedimientos desconocidos o ineficaces, reduciendo su capacidad de adaptación (Ministerio de Defensa, 2024), por lo que la doctrina contempla esta forma de alcanzar la sorpresa.

3.2.6 Concentración

La PDC-01(B) establece que la concentración «consiste en aplicar la potencia de combate de forma sincronizada sobre un mismo objetivo para lograr efectos decisivos» (Ministerio de Defensa, 2024: 36). La doctrina contempla esa superioridad mediante la potencia de combate y la concurrencia sobre un objetivo concreto, por lo que puede ser compatible con la situación existente en Ucrania, si se tiene en cuenta que no especifica que sea necesariamente física y permanente.

Lo que es cierto es que cuando se materialice la reunión de esa potencia de combate debe ser bajo un sistema de protección acorde. La necesidad de proteger a la fuerza se menciona en la doctrina, destacando la importancia de medidas de ocultación, dispersión y protección contra fuegos de precisión, máxime cuando el alcance en los conflictos actuales traspasa las áreas de operaciones próximas y se extienden a lo largo de toda la profundidad del despliegue, tal y como se ha desarrollado en el apartado «Fuegos».

En cuanto a las formas alternativas de masa, la doctrina menciona el uso de sistemas autónomos y medios no tripulados para reforzar las capacidades operativas, pero no profundiza en su empleo como un sustituto parcial de las concentraciones tradicionales de fuerzas. No obstante, ese enfoque no resulta dispar de lo expuesto hasta ahora en cuanto a la incorporación de tecnologías a las capacidades militares.

3.2.7 Continuidad

La PDC-01(B) establece la continuidad como un principio esencial para garantizar la progresión sostenida de las operaciones y evitar que el adversario recupere la iniciativa. Esta destaca la importancia de mantener el esfuerzo operativo, resistiendo y recuperándose ante cualquier degradación del entorno (Ministerio de Defensa, 2024). Sin embargo, su enfoque es más generalista en comparación con las lecciones extraídas de la guerra en Ucrania.

La necesidad de una progresión constante y sostenida de la maniobra, respaldada por fuegos, protección y logística, está alineada con la doctrina, que menciona la finalidad de actuar y apoyar la acción sin interrupción, garantizando el impulso operacional (Ministerio de Defensa, 2024). Los apoyos deben ser desde todos los dominios y, si bien el principio de continuidad no lo trata así explícitamente, la doctrina sí contempla las MDO como paradigma de actuación de las FAS para ser competitivas en los entornos operativos actuales.

El concepto de impedir constantemente la reorganización de las capacidades del enemigo, especialmente de sus fuegos, se encuentra parcialmente recogido en la doctrina bajo la importancia de imponer la propia voluntad y resistir ante condiciones desfavorables (Ministerio de Defensa, 2024). De acuerdo con la experiencia en Ucrania, se demuestra que esta continuidad depende directamente de acciones de interdicción en profundidad contra C2 y logística, y supresión del RSC enemigo para desarticular la capacidad y posibilidad de respuesta del adversario.

4 Conclusiones

4.1 Recopilación de ideas

4.1.1 La transparencia

El concepto de campo de batalla transparente no es completamente nuevo, sino más bien una aspiración permanente a lo largo de la historia militar. Desde los medios más rudimentarios hasta las tecnologías más sofisticadas, los comandantes siempre han buscado obtener la mayor visibilidad posible del entorno operativo. Sin embargo, los avances tecnológicos actuales han llevado

esta búsqueda al extremo, configurando un entorno en el que ver y actuar con rapidez se convierte en una capacidad crítica.

El campo de batalla transparente debe entenderse como un sistema complejo de tecnologías interconectadas que permiten observar y generar efectos en el espacio de batalla de forma casi inmediata. Esta capacidad condiciona enormemente las operaciones, sobre todo las ofensivas.

No obstante, y a pesar de las primeras impresiones que puedan generarse, la visibilidad no garantiza la comprensión. La información puede manipularse, y el ser humano, como parte del sistema C3, sigue siendo vulnerable. En este sentido, la decepción militar cobra un valor capital, ya que permite inducir decisiones erróneas al comandante enemigo incluso en entornos altamente transparentes, manteniendo así la incertidumbre como elemento inherente a la guerra. Íntimamente relacionado con esto, está la sorpresa, elemento en especial decisivo en las operaciones.

4.1.2 La transparencia y la guerra de Ucrania

La guerra de Ucrania se ha consolidado como un banco de pruebas clave para los conflictos modernos de alta intensidad, especialmente en lo que respecta al impacto del campo de batalla transparente. Las lecciones extraídas de este conflicto permiten analizar la aplicabilidad de doctrinas actuales y, en particular, de los efectos provocados por la creciente visibilidad del entorno operativo.

Especialmente destacable es la denominada «democratización» de la tecnología, que ha ampliado el acceso a capacidades ISR y de mando, pero también ha incrementado la necesidad de automatizar el tratamiento de datos mediante inteligencia artificial. Automatizar procesos no solo facilita la gestión de información masiva, sino que mejora la supervivencia frente a amenazas físicas como los drones. La EW y los sistemas CUAS han sido fundamentales en este aspecto. Del mismo modo ocurre con los satélites, si bien este ámbito y el dominio en el que despliegan todavía tienen un amplio margen de evolución e integración.

Por otro lado, la saturación de sensores y fuegos de alta precisión ha limitado severamente la maniobra, exigiendo anulaciones temporales del sistema de fuegos enemigo y una defensa aérea adaptada a las nuevas amenazas. En este contexto, las acciones de información, la decepción militar y la seguridad de las opera-

ciones adquieren un valor incalculable, permitiendo operar bajo principios clásicos —sorpresa, concentración, continuidad— en entornos marcados por una transparencia creciente.

4.1.3 La transparencia, la guerra de Ucrania y la doctrina

El análisis realizado sugiere que la doctrina conjunta nacional recoge, en líneas generales, los principales aspectos observados en la guerra de Ucrania en relación con el campo de batalla transparente. Aunque no aborda de forma detallada todos los elementos específicos derivados de este fenómeno, sí incorpora aquellos que pueden considerarse esenciales o críticos.

La doctrina conjunta nacional contempla en gran medida el «qué hay que hacer», aunque en general no especifica «cómo hacerlo». Esto no es necesariamente negativo, ya que también ofrece flexibilidad dentro de unos márgenes establecidos. Es cierto que algunos puntos específicos podrían incluirse, pero no es menos cierto que, de hacerlo, se podría correr el riesgo de una obsolescencia prematura por el avance incipiente de las tecnologías e innovaciones, convirtiendo a la doctrina en no válida. Esta sería una vulnerabilidad evidente para el éxito de las operaciones. No obstante, esa irrupción tecnológica puede estar colapsando la respuesta efectiva al entorno debido a una deficiencia en la capacidad de adaptación (un *shock*), pero no parece ser un problema de contenido de la doctrina, sino de su aplicación práctica en situaciones reales.

Un caso singular es el tratamiento de la decepción militar. Aunque se reconoce su valor doctrinal, su desarrollo en profundidad es limitado, especialmente si se compara con marcos aliados como el de Estados Unidos o Francia, que conciben cursos específicos o han actualizado este aspecto en su doctrina. Además, no parece haber una dinámica institucional plenamente consolidada sobre la enseñanza y la gestión del conocimiento relativos a la decepción y la obtención de la sorpresa en el planeamiento y conducción de las operaciones militares. En este contexto, el estudio de la historia militar —particularmente de casos en los que la sorpresa y la decepción fueron determinantes— podría representar una herramienta valiosa para suplir algunas carencias doctrinales y reforzar aquellas capacidades menos desarrolladas en los textos normativos, pero esenciales para operar eficazmente en escenarios de alta transparencia.

Por otro lado, el propio concepto de «campo de batalla transparente» no figura expresamente en la doctrina vigente y esto se considera

imprescindible para una conceptualización unificada que permita abordar sus implicaciones de manera sistemática y coherente.

4.2 Resultados

La guerra de Ucrania ha mostrado que, incluso en un entorno de alta visibilidad proporcionado por las tecnologías, es posible proteger las intenciones propias mediante un uso efectivo de la decepción y la innovación para sobreponerse a la transparencia. Esta capacidad para manipular la percepción del comandante enemigo y adelantarse a su toma de decisiones, aun cuando existe una visibilidad física elevada, demuestra que la comprensión sigue siendo dependiente de factores humanos y cognitivos.

En consecuencia, la tecnología por sí sola no es la solución para conocer las intenciones enemigas, y, por tanto, las operaciones pueden continuar desarrollándose bajo sus efectos y aplicando los preceptos doctrinales correspondientes. Esto obligó a revisar si dichos preceptos son adecuados o suficientes. La comparación entre las observaciones extraídas de la guerra de Ucrania y los contenidos doctrinales nacionales permiten constatar que los contenidos fundamentales y determinantes sí se encuentran presentes en la doctrina vigente.

A la luz de los resultados, se puede establecer que la transparencia no es la solución definitiva a las operaciones por el mero hecho de permitir una máxima visibilidad sobre las mismas. Estas continúan desarrollándose en presencia de una alta visibilidad física y bajo las funciones y principios doctrinales estudiados, que, además, parecen contemplar los aspectos críticos detectados en las campañas de la guerra de Ucrania. Por ello, puede concluirse que la doctrina militar conjunta en vigor en España recoge, de manera suficiente, las implicaciones operacionales derivadas del campo de batalla transparente, al menos en lo que respecta a los componentes doctrinales analizados en el presente trabajo. Aunque no siempre lo hace de forma explícita o con un desarrollo detallado, incorpora los elementos esenciales que permiten operar en entornos caracterizados por una alta visibilidad y por la creciente integración tecnológica. La flexibilidad inherente a la redacción doctrinal, lejos de suponer una limitación, refuerza su aplicabilidad en contextos operacionales dinámicos y complejos. Este trabajo aspira a contribuir, precisamente, a esa evolución constante, proponiendo una reflexión crítica que favorezca el perfeccionamiento doctrinal y la eficacia futura de las FAS.

Bibliografía

Agüero Martínez, J. A. (2025). *Entrevista al Comandante del Mando de Operaciones*. Madrid.

Antal, J. (2022). *Seven seconds to die.* Havertown, Casemate Publishers. ISBN 978-1-63624-124-1.

Bados Nieto, V. M. (2025). *Entrevista al Director del Instituto Español de Estudios Estratégicos*. Madrid.

Barno, D. y Bensahel, N. (2022). The other big lessons that the US Army should learn from Ukraine [en línea]. War on the Rocks. [Consulta: 2 agosto 2024]. Disponible en: https://warontherocks.com/2022/06/the-other-big-lessons-that-the-u-s-army-should-learn-from-ukraine/[18]

Boyd, J. R. (2018). A discourse on Winning and Lossing [en línea]. Alabama, Air University Press. [Consulta: 14 diciembre 2024]. Disponible en: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0151_Boyd_Discourse_Winning_Losing.pdf[19]

Boyer, D. y Becker R. K. (2024). How Ukraine overcame the transparent battlefield to achieve operational surprise in Kursk [en línea]. [Consulta: 10 diciembre 2024]. Disponible en: https://oe.t2com.army.mil/product/how-ukraine-overcame-the-transparent-battlefield-to-achieve-operational-surprise-in-kursk/

Calduch, R. (2014). *Métodos y técnicas de investigación internacional*. 2.ª edición. Madrid, Universidad Complutense de Madrid.

Calvo Albero, J. L. (2022). Estrategia militar de la OTAN: doctrinas y conceptos estratégicos. Recepción en España [en línea]. Revista de Estudios en Seguridad Internacional. 8(1), pp. 53-70. [Consulta: 6 diciembre 2024]. Disponible en: https://seguridadinternacional.es/resi/html/estrategia-militar-de-la-otan-doctrinas-y-conceptos-estrategicos-recepcion-en-espana/[20]

Chulilla, J. L. (2024). Avances tecnológicos de los drones en la guerra de Ucrania | Estrategia podcast 104 [en línea]. Glob-

[18] Fuente consultada, pero no utilizada en el trabajo.

[19] *Idem*.

[20] *Idem*.

al Strategy. [Consulta: 6 diciembre 2024]. Disponible en: https://global-strategy.org/drones-guerra-ucrania/

Clausewitz, C. von (2005). *De la guerra. Versión íntegra*. Madrid, Ed. La Esfera de los Libros. ISBN: 978-84-9060-226-3[21].

Colom Piella, G. (2006). La revolución en los asuntos militares [en línea]. Boletín de Información. Ministerio de Defensa, CESEDEN. [Consulta: 6 diciembre 2024]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4573356[22]

Del Castillo, J. A. (2024). El campo de batalla 'transparente', el dominio cognitivo 'opaco' [en línea]. The Objective. [Consulta: 25 febrero 2025]. Disponible en: https://theobjective.com/internacional/2024-12-17/campo-batalla-transparente-dominio-cognitivo-opaco

Dickey, R. y Gleason, M. P. (2024). Space and war in Ukraine. Beyond the satellites [en línea]. AETHER. A Journal of Strategic Airpower & Spacepower. 3(1), pp. 20-35. [Consulta: 22 agosto 2024]. Disponible en: https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-3_Number-1/Dickey_Gleason.pdf

El Grand Continent. (2025). Guerra en Ucrania: 2022-2025, una cronología de la línea de frente [en línea]. El Grand Continent. [Consulta: 6 marzo 2025]. Disponible en: https://legrandcontinent.eu/es/2025/02/24/guerra-en-ucrania-2022-2025-una-cronologia-de-la-linea-de-frente/[23]

El Radar. (2019). Armas de energía dirigida una nueva ventaja, si se acelera el desarrollo de doctrina y tecnologías [en línea]. El Radar. [Consulta: 5 agosto 2024]. Disponible en: https://www.elradar.es/armas-de-energia-dirigida-una-nueva-ventaja-si-se-acelera-el-desarrollo-de-doctrina-y-tecnologias/[24]

—. (2023). Por qué están fracasando los satélites espaciales rusos en la guerra de Ucrania [en línea]. El Radar. [Consulta: 24 agosto 2024]. Disponible en: https://www.elradar.es/porque-estan-fracasando-los-satelites-espaciales-rusos-en-la-guerra-de-ucrania/

EMAD. (2021). *PDC-3. Doctrina de Operaciones*. Madrid, Ministerio de Defensa.

[21] *Idem*.
[22] *Idem*.
[23] *Idem*.
[24] *Idem*.

—. (2023). *Instrucción Comunicada 09/23 del JEMAD: Desarrollo de doctrina conjunta (IDDC)*. Madrid, Ministerio de Defensa[25].

Flint, C. (2006). *Introduction to Geopolitics*. Abingdon, Routledge.

Frías Sánchez, C. J. (2014). El cambio doctrinal, clave de la innovación militar [en línea]. GESI. [Consulta: 6 diciembre 2024]. Disponible en: https://www.ugr.es/~gesi/analisis/15-2014.pdf[26]

—. (2022). Doctrine interarmées: mission impossible? [en línea]. Revue Défense Nationale. Hors-série (HS3), pp. 93-107. [Consulta: 2 abril 2025]. Disponible en: https://doi.org/10.3917/rdna.hs09.0093[27]

—. (2023). ¿Un campo de batalla «transparente»? [en línea] Revista Ejército. N.º 987. [Consulta: 6 diciembre 2024]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9301839

—. (2024). Rusia, Ucrania y el campo de batalla «transparente» [en línea]. Documento de Opinión IEEE 18/2024. [Consulta: 6 diciembre 2024]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9671839

—. (2025). *Entrevista al Director de la Escuela de Guerra y Liderazgo del Ejército de Tierra*. Madrid.

Gady, F. S. (2023). Russia-Ukraine War: How an Army of Drones Changed the Battlefield [en línea]. Foreign Policy. [Consulta: 6 diciembre 2024]. Disponible en: https://foreignpolicy.com/2023/12/06/ukraine-russia-war-drones-stalemate-frontline-counteroffensive-strategy/[28]

Garnier, G. y Néron-Bancel, P. (2024). "At the Other Side of the Hill": The Benefits and False Promises of Battlefield Transparency [en línea]. Focus stratégique. Ifri Studies. N.º 118. [Consulta: 6 diciembre 2024]. Disponible en: https://www.ifri.org/en/studies/other-side-hill-benefits-and-false-promises-battlefield-transparency

González Cámara, R. (2025). Operaciones espaciales*. XXVI Curso de Estado Mayor de las FAS*. Madrid, CESEDEN.

Halem, H. (2023). Ukraine's Lessons for Future Combat: Unmanned Aerial Systems and Deep Strike [en línea]. Pa-

[25] *Idem*.
[26] *Idem*.
[27] *Idem*.
[28] *Idem*.

rameters. 53(4). [Consulta: 22 agosto 2024]. Disponible en: https://press.armywarcollege.edu/parameters/vol53/iss4/9/[29]

Hallex, M. A. y Cottom T. S. (2020). Proliferated commercial satellite constellations: implications for national security [en línea]. JFQ. N.º 97, pp. 20-29. [Consulta: 25 agosto 2024]. Disponible en: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_20-29_Hallex-Cottom.pdf?ver=2020-03-31-130614-940[30]

Henrotin, J. (2023). ¿Qué es una contraofensiva? [en línea]. El Grand Continent. [Consulta: 6 marzo 2025]. Disponible en: https://legrandcontinent.eu/es/2023/06/13/que-es-una-contraofensiva/

Howard, M. (2002). *Clausewitz: A Very Short Introduction*. Oxford, Oxford University Press. ISBN 0-19-280257-7[31].

Jiménez Gavilán, D. (2024). Perfilando el combate futuro [en línea]. Ejército. N.º 990, pp. 44-49. [Consulta: 3 diciembre 2024]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/j/ejercito_990.pdf[32]

Jójárt, K. (2024). The war against Ukraine through the prism of Russian military thought [en línea]. Journal of Strategic Studies. 47(6-7), pp. 801-831. [Consulta: 9 enero 2025]. Disponible en: https://doi.org/10.1080/01402390.2024.2414079

Jordán, J. (2014). Innovación y Revolución en los Asuntos Militares: una perspectiva no convencional [en línea]. defensa.com. [Consulta: 6 diciembre 2024]. Disponible en: https://www.defensa.com/analisis-gesi/innovacion-revolucion-asuntos-militares-perspectiva-no[33]

—. (2017). Innovaciones y Revoluciones en los Asuntos Militares [en línea]. Global Strategy. [Consulta: 6 diciembre 2024]. Disponible en: https://global-strategy.org/innovaciones-revoluciones-asuntos-militares/[34]

[29] *Idem*.
[30] *Idem*.
[31] *Idem*.
[32] *Idem*.
[33] *Idem*.
[34] *Idem*.

—. (2023a). Doctrina militar en Histocast [en línea]. Global Strategy. [Consulta: 6 diciembre 2024]. Disponible en: https://global-strategy.org/que-es-la-doctrina-militar/[35]

—. (2023b). Qué es la doctrina militar [en línea]. Global Strategy. [Consulta: 6 diciembre 2024]. Disponible en: https://global-strategy.org/la-doctrina-militar/

Kagan, F. W. et al. (2024). Ukraine and the Problem of Restoring Maneuver in Contemporary War [en línea]. Institute for the Study of War. [Consulta: 6 diciembre 2024]. Disponible en: https://www.understandingwar.org/backgrounder/ukraine-and-problem-restoring-maneuver-contemporary-war

Kimmitt, M. T. (2024). 'One shot, one kill': How Ukraine-Russia war is changing warfare [en línea]. Político. [Consulta: 9 agosto 2024]. Disponible en: https://www.politico.eu/article/developments-from-ukraine-precision-warfare-on-the-cheap/

MADOC. (2024a). *Observaciones sobre la guerra de Ucrania (Enero 2023-Mayo 2024)*. Granada, Dirección de Investigación, Doctrina, Orgánica y Materiales, Ejército de Tierra[36].

—. (2024b). *Tendencias 2022-2023. Volumen II. Inteligencia*. Granada, Dirección de Investigación, Doctrina, Orgánica y Materiales, Ejército de Tierra.

Martí, C. (2024). El papel de la tecnología en los recientes conflictos de Ucrania y Gaza. Una valoración inicial [en línea]. Real Instituto Elcano. [Consulta: 18 febrero 2025]. Disponible en: https://www.realinstitutoelcano.org/analisis/el-papel-de-la-tecnologia-en-los-recientes-conflictos-de-ucrania-y-gaza-una-valoracion-inicial/

Merino, A. (2024). Dos años de guerra en Ucrania: una lucha de territorio con el frente estancado [en línea]. El Orden Mundial. [Consulta: 29 enero 2025]. Disponible en: https://elordenmundial.com/mapas-y-graficos/dos-anos-guerra-ucrania-lucha-territorio-frente-estancado/[37]

Ministerio de Defensa. (2024). *PDC-01(B). Doctrina para el Empleo de las Fuerzas Armadas*. Ministerio de Defensa, Secretaría General Técnica.

Pardo de Santayana, J. (2024). La inteligencia artificial y la guerra de Ucrania [en línea]. Cuadernos de estrategia. Ministerio de

[35] *Idem*.
[36] *Idem*.
[37] *Idem*.

Defensa, IEEE. [Consulta: 6 diciembre 2024]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9666375

Prats, J. M. (2014). La guerra de mando y control y la teoría del OODA Loop [en línea]. Boletín de Información. N.º 268. [Consulta: 11 diciembre 2024]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4604097.pdf[38]

Rodríguez, Y. (2024). Lecciones militares estratégicas de la Guerra de Ucrania [en línea]. Revista de Estudios en Seguridad Internacional. 10(1), pp. 17-38. [Consulta: 6 marzo 2025]. Disponible en: http://dx.doi.org/10.18847/1.19.3

Tzu, S. (2020). *El arte de la guerra*. Ed. Titivillus (epubLIBRE).[39]

Toffler, A. (1973). *El "shock" del futuro.* Barcelona, Plaza & Janes Editores. ISBN: 84-01-41020-7.

TRADOC. (2024). Operational Environment 2024-2034: Large-Scale Combat Operations [en línea]. United States Army Training and Doctrine Command. [Consulta: 6 diciembre 2024]. Disponible en: https://oe.t2com.army.mil/file/2025OCT31_T2COMG2_OE_2024_2035_LSCO_Assessment1.0.pdf?f=1256f015

Vego, M. (1990). Recce-Strike Complexes in Soviet Theory and Practice [en línea]. Fort Leavenworth, US Combined Arms Center. [Consulta: 28 dciembre 2024]. Disponible en: https://apps.dtic.mil/sti/pdfs/ADA231900.pdf[40]

Watling, J. (2024). *The Arms of the Future: Technology and Close Combat in the Twenty-First Century*. Royal United Services Institute (RUSI). Londres, Bloomsbury Academic. ISBN 978-1-3503-5298-8.

Zaluzhnyi, V. (2024). On the modern design of military operations In the russo-ukrainian war: In the fight for the initiative. En: The design of war has changed. CNN. [Consulta: 7 marzo 2025]. Disponible en: https://s3.documentcloud.org/documents/24400154/ukraine-valerii-zaluzhnyi-essay-design-of-war.pdf

[38] *Idem*.
[39] *Idem*.
[40] *Idem*.

Capítulo cuarto

Paradigma de seguridad en el Antropoceno: un análisis de las Estrategias de Seguridad Nacional de España y Francia

Jaime Graus Thiesen

Resumen

El Antropoceno, caracterizado por el impacto humano en el sistema terrestre, plantea retos sin precedentes como el cambio climático, la pérdida de biodiversidad y los desastres naturales. Las teorías clásicas de seguridad, representadas por John Herz y Kenneth Waltz, priorizan la seguridad estatal y las dinámicas interestatales, pero no abordan adecuadamente las amenazas transnacionales y ecológicas contemporáneas.

Simon Dalby propone un cambio de paradigma hacia una seguridad basada en la sostenibilidad y la justicia climática, reconociendo que las actividades humanas modernas representan riesgos globales. Este enfoque redefine la seguridad para incluir la resiliencia frente a desafíos sistémicos.

En este contexto, la Estrategia de Seguridad Nacional de España (2021) incorpora el cambio climático como un multiplicador de riesgos, alineándose con políticas internacionales como la Agenda 2030. Por otro lado, la Revisión Estratégica de Francia (2022) mantiene un enfoque tradicional, centrado en amenazas geopolíticas y militares, relegando el cambio climático a un rol secundario.

Este estudio resalta la relevancia de integrar las dinámicas del Antropoceno en las estrategias de seguridad nacional para responder a los desafíos del siglo XXI. Su análisis aporta una perspectiva crítica para entender las tensiones entre paradigmas tradicionales y emergentes, subrayando la necesidad de un enfoque más inclusivo y sostenible.

Palabras clave

Antropoceno, Paradigma de seguridad, Estrategia de Seguridad Nacional, Potencia de fuego civil, Cambio climático.

Security Paradigm in the Anthropocene: An analysis of the National Security Strategies of Spain and France

Abstract

This study addresses the security paradigm within the context of the Anthropocene, examining Simon Dalby's theories and their application to the national security strategies of Spain (2021) and France (2022). The objective is to analyse whether these strategies reflect a new security paradigm focused on global and ecological threats or remain framed within traditional models centred on state defence and military threats. The Anthropocene, characterized by human impact on the Earth system, poses unprecedented challenges such as climate change, biodiversity loss, and natural disasters. Classical security theories, represented by John Herz and Kenneth Waltz, prioritize state security and interstate dynamics but fail to adequately address contemporary transnational and ecological threats. Simon Dalby proposes a paradigm shift towards security based on sustainability and climate justice, recognizing that modern human activities constitute global risks. This approach redefines security to include resilience to systemic challenges. In this context, Spain's National Security Strategy (2021) incorporates climate change as a risk multiplier, aligning with international policies such as the 2030 Agenda. Conversely, France's Strategic Review (2022) maintains a traditional approach focused on geopolitical and military threats, relegating climate change to a secondary role.

This study highlights the relevance of integrating Anthropocene dynamics into national security strategies to address 21st-century challenges. Its analysis provides a critical perspective for understanding tensions between traditional and emerging paradigms, underscoring the need for a more inclusive and sustainable approach.

Key words

Anthropocene, Cecurity paradigm, National security strategy, Civilian firepower, Climate change.

Lista de abreviaturas

ESN	Estrategia de Seguridad Nacional.
GEI	Emisiones de gases de efecto invernadero.
LPEC	Ley de Planificación Energética y Climática.
PNACC	Plan Nacional de Adaptación al Cambio Climático.
PNUD	Programa de las Naciones Unidas para el Desarrollo.
RNE	Revisión Nacional Estratégica.
SFEC	Estrategia Francesa de Energía y Clima.
SGPE	Secretaría General de Planificación Ecológica.

1 Introducción

En el siglo XXI, la seguridad internacional enfrenta nuevos desafíos debido a la creciente interconexión global y al profundo impacto humano sobre el medio ambiente. Este contexto se conoce como Antropoceno, una era geológica definida por la influencia humana en los sistemas de la Tierra.

Aunque el término aún no es oficial en geología, Antropoceno simboliza hasta qué punto las actividades humanas, desde la industrialización hasta la urbanización masiva, han alterado el clima, los ecosistemas y los ciclos naturales del planeta. Como resultado, fenómenos como el cambio climático, la pérdida de biodiversidad o las pandemias se han convertido en amenazas de gran escala que trascienden fronteras y desafían las nociones clásicas de seguridad.

Tradicionalmente, las estrategias de seguridad nacional se han centrado en conflictos militares, defensa territorial y rivalidades entre Estados. Enfoques teóricos clásicos, como el «dilema de seguridad» de John Herz de 1950 y el realismo estructural de Kenneth Waltz de 1979, consideran la anarquía internacional y el poder militar como ejes centrales de la seguridad del Estado.

Sin embargo, estas perspectivas, formuladas en la Guerra Fría y otras épocas, resultan insuficientes ante los retos transnacionales y sistémicos del mundo actual. Crisis globales como el cambio climático, las pandemias, la degradación ambiental o las ciberamenazas evidencian que las amenazas ya no se limitan a ejércitos invasores ni a tensiones diplomáticas tradicionales, sino que emergen de la propia interacción entre el ser humano y el planeta.

Ante esta realidad, diversos pensadores han abogado por redefinir el concepto de seguridad para el siglo XXI. Entre ellos, destaca Simon Dalby, quien como se aprecia en el capítulo I, plantea la necesidad de un nuevo paradigma de seguridad en el Antropoceno.

Este paradigma reconoce que la supervivencia y estabilidad de las sociedades dependen tanto de factores ecológicos globales como de factores político-militares. Dalby y otros autores contemporáneos sostienen que la seguridad debe ampliarse para incluir la seguridad ecológica, la justicia climática y la resiliencia comunitaria frente a perturbaciones sistémicas.

En palabras sencillas, esto implica considerar que proteger a la población ya no consiste únicamente en garantizar fronteras seguras o disuadir ataques militares, sino también en preservar las condiciones ambientales que sustentan la vida humana.

España y Francia, dos naciones europeas con posturas históricas diferentes en materia de defensa y política exterior, ofrecen un interesante estudio comparativo para examinar cómo se está (o no) adoptando este nuevo enfoque de seguridad. Ambas han actualizado recientemente sus directrices estratégicas nacionales, España con su Estrategia de Seguridad Nacional 2021 (ESN 2021) y Francia con su Revisión Nacional Estratégica 2022 (RNE 2022), incorporando en mayor o menor medida las preocupaciones del mundo actual.

La investigación utiliza como base teórica el paradigma del Antropoceno, propuesto por Simon Dalby (2016-2023), que destaca la necesidad de incluir la sostenibilidad, la justicia climática y la resiliencia en las políticas de seguridad.

Además, el marco teórico de Simon Dalby ofrece una perspectiva crítica para evaluar si estos planes reflejan un cambio hacia un paradigma más sostenible e inclusivo.

El propósito de este trabajo es contribuir al debate académico sobre cómo las políticas de seguridad pueden adaptarse a los desafíos del Antropoceno. A través de este análisis, se espera mostrar si España y Francia avanzan hacia estrategias que prioricen la sostenibilidad y la resiliencia, elementos clave en las agendas internacionales como la Agenda 2030 y el Acuerdo de París.

En resumen, esta investigación busca, no solo analizar las políticas de seguridad de estos dos países, sino también subrayar la importancia de un cambio en el enfoque global hacia una seguridad que aborde los riesgos medioambientales y climáticos como parte integral de las estrategias para el futuro.

1.1 Marco teórico

1.2 Consideraciones generales

El presente capítulo aborda los fundamentos teóricos necesarios para comprender el cambio de paradigma en el concepto de seguridad en el contexto del Antropoceno. En un mundo marcado por la creciente influencia de las actividades humanas sobre los

sistemas naturales, el Antropoceno emerge como un desafío que trasciende las lógicas tradicionales de las relaciones internacionales y redefine las prioridades estratégicas globales. Este marco introduce amenazas sistémicas, como el cambio climático y la pérdida de biodiversidad, que cuestionan las teorías clásicas de seguridad centradas en el Estado y las amenazas militares.

En primer lugar, se presentará el concepto de Antropoceno como el contexto histórico y ecológico que sustenta la necesidad de un nuevo enfoque. Luego, se analizará el paradigma clásico de seguridad desarrollado por John Herz (1950) y Kenneth Waltz (1979), cuyos principios de anarquía y equilibrio de poder han dominado durante décadas. Posteriormente, se explorará el cambio de paradigma propuesto por Thomas Kuhn (Khun, 1962), cuya teoría de revoluciones científicas ofrece una perspectiva clave para interpretar esta transición, hacia el nuevo paradigma que plantea el informe del Programa de las Naciones Unidas para el desarrollo del 2022 (Nations, 2022).

Asimismo, se discutirá la «potencia de fuego civil» (Dalby, 2023a) y el «Pyroceno» (Pyne, 2019), conceptos que ilustran cómo las actividades humanas modernas han intensificado las amenazas globales. El Pyroceno, según Stephen J. Pyne define una era donde la industrialización ha convertido el fuego en una fuerza desestabilizadora del clima y los ecosistemas (Pyne, 2019). Simon Dalby, por su parte, introduce la potencia de fuego civil, señalando cómo la combustión constante de actividades humanas perpetúa desigualdades y afecta especialmente a las regiones más vulnerables (Dalby, 2023a).

Por último, el capítulo concluye con las contribuciones de Simon Dalby, quien propone un enfoque integral basado en la seguridad ecológica y la justicia climática. Esta estructura sienta las bases para comprender los retos y soluciones del paradigma de seguridad en el siglo XXI.

1.3 Antropoceno

El término «Antropoceno» se ha convertido en un concepto central para entender el impacto humano en el sistema terrestre. Acuñado por Eugene F. Stoermer[41] en 1980 y popularizado

[41] Eugene F. Stoermer (1934-2012), biólogo y profesor en la Universidad de Míchigan, conocido por haber acuñado el término «Antropoceno» en la década de 1980, para describir la era geológica en la que la actividad humana ha transformado significativamente el planeta.

por Paul Crutzen[42] en el año 2000, describe una posible nueva época geológica caracterizada por el impacto significativo de las actividades humanas sobre los procesos naturales del planeta (McCreary, 2019). Este concepto simboliza no solo un conjunto de problemas ambientales, sino una crisis sistémica que afecta los procesos biológicos, químicos y físicos de la Tierra (Angus, 2020a).

Una de las principales características de esta era es la transgresión de los límites planetarios identificados por Johan Rockström y Will Steffen, como el clima, la biodiversidad y los flujos biogeoquímicos. Al menos cuatro de estos límites ya han sido superados, lo que refleja la insostenibilidad del modelo de desarrollo actual (Rejane Issberner y Léna, 2023).

La «Gran Aceleración» de mediados del siglo xx destaca como un momento crucial donde el consumo desmedido de combustibles fósiles y el crecimiento industrial transformaron irreversiblemente los ecosistemas globales (Rejane Issberner y Léna, 2023).

En 2007, en un artículo de revista titulado: «El Antropoceno: ¿Están los humanos ahora abrumando a las grandes fuerzas de la naturaleza?», Steffen, Crutzen y McNeill volvieron a publicar los gráficos de la «Gran Aceleración», y sugirieron que se debería ver la segunda mitad del siglo xx como la Etapa 2 del «Antropoceno». (Angus, 2020a)

Ian Angus argumenta que la humanidad ha abandonado su estado interglacial natural y ha entrado en una etapa de «Tierra de invernadero», caracterizada por climas más cálidos, pérdida de biodiversidad y un aumento de eventos extremos como tormentas e inundaciones (Angus, 2020b).

Sin embargo, este impacto no es uniforme: las sociedades más ricas son responsables del 60 % de las emisiones de gases de efecto invernadero, mientras que las más pobres solo contribuyen con el 5 %, lo que subraya las desigualdades inherentes al sistema capitalista (Angus, 2020b). Términos como «Capitaloceno» y «Occidentaloceno» enfatizan el papel desproporcionado de las sociedades capitalistas occidentales en esta crisis (Rejane Issberner y Léna, 2023)

[42] «Premio Nobel por demostrar que los productos químicos ampliamente utilizados estaban destruyendo la capa de ozono en la atmósfera superior de la Tierra, con efectos potencialmente catastróficos para toda la vida en la Tierra» (Angus, 2020: 2).

El inicio del Antropoceno genera debate. Algunos investigadores sitúan su origen en la revolución agrícola, mientras que otros destacan la «Gran Aceleración» del siglo xx como el momento de impacto global más significativo. Esta perspectiva resalta el uso intensivo de combustibles fósiles y la producción industrial como factores determinantes (Angus, 2020b).

El Antropoceno representa un cambio cualitativo en la relación entre la humanidad y el planeta. Más allá de su formalización como época geológica, es una herramienta crucial para entender y abordar los desafíos globales actuales. Requiere de un cambio radical en las prácticas sociales, económicas y políticas, integrando la justicia social y la sostenibilidad ecológica como principios fundamentales (Rejane Issberner y Léna, 2023; Angus, 2020b).

1.4 Concepto clásico de seguridad y cambio de paradigma

El concepto de seguridad refleja un cambio profundo desde los enfoques clásicos de John Herz y Kenneth Waltz hacia nuevas perspectivas más globales. Herz (1950) destacó el dilema de seguridad, un ciclo de desconfianza generado por las medidas defensivas de los Estados, mientras que Waltz (1979) enfatizó el equilibrio de poder como pilar de estabilidad en un sistema internacional anárquico. Sin embargo, como plantea Thomas Kuhn (1962), los paradigmas cambian cuando no pueden resolver nuevas anomalías. Hoy, desafíos como el cambio climático y las pandemias exigen un replanteamiento, integrando sostenibilidad y cooperación global para redefinir la seguridad.

En los enfoques de seguridad clásicos de las relaciones internacionales, se prioriza la seguridad del Estado como actor central en el sistema internacional. Este enfoque está profundamente influido por el realismo clásico y se centra en las amenazas militares y la defensa territorial.

Las ideas de John Herz y Kenneth Waltz han ayudado a entender mejor cómo funciona la seguridad en el mundo. Aunque ambos parten de la idea de que no hay una autoridad global que controle a los Estados, sus enfoques tienen diferencias importantes.

El concepto central en el enfoque tradicional de seguridad de John Herz es el «dilema de seguridad», introducido en 1950. Describe cómo, en un sistema internacional anárquico, los esfuerzos de un Estado por garantizar su propia seguridad pueden, de forma

inadvertida, incrementar la inseguridad de otros. Este fenómeno genera un ciclo de acumulación de poder y desconfianza mutua que incrementa la competencia y el riesgo de conflictos (Calatrava, 2022).

El dilema no surge únicamente por las intenciones expansionistas de algunos Estados, sino que está profundamente arraigado en la estructura misma del sistema internacional. La anarquía, al carecer de una autoridad central que regule las relaciones interestatales, fomenta la incertidumbre sobre las intenciones futuras de otros actores. Esta incertidumbre obliga a los Estados a asumir lo peor y a prepararse para posibles amenazas, incluso cuando no existan intenciones agresivas iniciales (Herz, 1950).

El dilema de seguridad se desarrolla en un ciclo iterativo en el que las acciones defensivas de un Estado, tales como aumentar su capacidad militar, son interpretadas como amenazas por otros Estados, quienes a su vez toman medidas similares para compensar y defenderse. Este comportamiento crea un ambiente de desconfianza y competencia continua (Herz, 1950).

Aunque el dilema de seguridad presenta un panorama sombrío a primera vista, el autor reconoce que es posible mitigar sus efectos mediante la cooperación y la creación de confianza entre los Estados. Sin embargo, advierte que tales esfuerzos son difíciles de sostener a largo plazo, ya que el contexto anárquico tiende a revertir los periodos de estabilidad.

En relación con Kenneth Waltz, figura central del realismo estructural, redefine el enfoque tradicional de seguridad al priorizar la estructura del sistema internacional sobre las particularidades internas de los Estados. En su obra principal, Theory of International Politics (1979), establece que la anarquía internacional, entendida como la ausencia de un poder central regulador, constituye la base de la interacción entre los Estados (Waltz, 1979). Este principio condiciona su comportamiento al obligarlos a operar en un sistema de autoayuda, donde garantizar su supervivencia se convierte en la máxima prioridad (Moure, 2009).

El realismo estructural de Waltz introduce el equilibrio de poder como una característica espontánea y no intencionada del sistema internacional. Este equilibrio, indispensable para evitar la dominación de un actor sobre el resto, surge de la competencia inherente en un entorno anárquico (Waltz, 1979). A diferencia del realismo clásico, Waltz argumenta que no es necesario que los Estados busquen activamente este equilibrio; sus acciones

individuales, motivadas por la búsqueda de seguridad, lo generan de manera automática siempre que la anarquía prevalezca y los Estados prioricen su supervivencia. (Moure, 2009).

Un aspecto distintivo de su teoría es el énfasis en la estabilidad del sistema bipolar, como el observado durante la Guerra Fría (Waltz, 2000). Según Waltz, la bipolaridad reduce la incertidumbre y facilita la gestión del poder entre las superpotencias, disminuyendo las posibilidades de conflictos a gran escala. La estabilidad de este modelo contrasta con la multipolaridad, donde la mayor cantidad de actores complica el equilibrio y aumenta la probabilidad de errores estratégicos (Moure, 2009).

En conclusión, Herz describe el «dilema de seguridad», cuando un país refuerza su ejército para protegerse y otros países se sienten amenazados e imitan esa acción, generando desconfianza y competencia que pueden llevar a conflictos.

Por otro lado, Waltz se enfoca más en cómo está organizado el sistema internacional. Según él, todos los países se comportan de forma parecida porque quieren sobrevivir, pero lo que los diferencia es el poder que tienen. Waltz destaca que el equilibrio de poder, donde ningún país domina a los demás, es lo que mantiene la estabilidad. Además, cree que un sistema con solo dos grandes potencias, como durante la Guerra Fría, es más seguro que uno con muchos países fuertes.

Ambos autores han aportado ideas valiosas. Herz se centra en las relaciones y la desconfianza entre los países, mientras que Waltz analiza cómo el sistema global influye en su comportamiento.

La evolución entre sus ideas muestra un cambio: de enfocarse en los temores entre países a mirar cómo el sistema global afecta sus decisiones. Esto da herramientas para enfrentar los desafíos de seguridad actuales, donde los conflictos y la desconfianza siguen siendo parte del panorama.

Respecto al cambio de paradigma, Thomas Kuhn plantea que la ciencia avanza no de manera acumulativa, sino mediante cambios radicales llamados «revoluciones científicas».

Según Kuhn, un paradigma es el conjunto de teorías, métodos y supuestos que guía la práctica dentro de una comunidad. En los periodos de «ciencia normal», este marco domina hasta que se acumulan anomalías: problemas que no pueden ser resueltos dentro del paradigma vigente. Cuando estas anomalías se vuelven insostenibles, surge una crisis que lleva a la adopción de

un nuevo paradigma, transformando profundamente la forma de entender el campo (Khun, 1962).

Este enfoque es clave para entender el cambio necesario en el concepto de seguridad. El paradigma tradicional de Herz y Waltz, descrito anteriormente, centrado en la anarquía internacional, el equilibrio de poder y las amenazas interestatales, ha guiado durante décadas las estrategias de seguridad.

Sin embargo, el Antropoceno introduce anomalías que este paradigma no puede resolver: el cambio climático, las pandemias, la pérdida de biodiversidad y la degradación ambiental. Estas amenazas globales y transnacionales trascienden los límites de los Estados, cuestionando la lógica del paradigma tradicional.

Siguiendo la lógica de Kuhn, el Antropoceno representa una revolución conceptual en el ámbito de la seguridad. El nuevo paradigma redefine la seguridad como un concepto sistémico y global, centrado en la sostenibilidad y la resiliencia frente a amenazas ecológicas.

Este cambio no solo transforma las prioridades estratégicas, sino que también exige un marco que integre ciencia, política y cooperación internacional, marcando una ruptura definitiva con el paradigma clásico de Herz y Waltz.

1.5 El nuevo paradigma

El concepto de seguridad ha experimentado transformaciones profundas a lo largo de la historia, pasando de un enfoque centrado exclusivamente en la protección estatal a perspectivas más amplias que incluyen a los individuos, las comunidades y, recientemente, el planeta mismo.

Este cambio de paradigma se encuentra enmarcado en el contexto del Antropoceno, una era caracterizada por el impacto sin precedentes de la actividad humana en los sistemas naturales y sociales.

El informe especial de 2022 del Programa de las Naciones Unidas para el Desarrollo (PNUD), titulado «Las nuevas amenazas para la seguridad humana en el Antropoceno exigen una mayor solidaridad», plantea una evolución fundamental en el entendimiento de la seguridad. Este nuevo paradigma desafía las concepciones tradicionales y se propone como una respuesta integral y adaptada a las complejas interconexiones del mundo contemporáneo (Nations, 2022).

Las teorías clásicas de la seguridad, representadas por figuras como John Herz y Kenneth Waltz, proporcionan el punto de partida para entender este cambio.

Estas perspectivas, aunque fundamentales en su momento, se basaban en una visión centrada en el estado como unidad de análisis y en amenazas externas como el principal desafío.

Sin embargo, el surgimiento del Antropoceno ha desafiado los supuestos básicos de estas teorías. El Antropoceno no solo evidencia la capacidad humana para alterar profundamente los sistemas del planeta, sino que también introduce amenazas que no se limitan a fronteras nacionales ni responden exclusivamente a dinámicas estatales. Crisis como el cambio climático, la pérdida de biodiversidad, las pandemias, las desigualdades globales y las amenazas cibernéticas han puesto de manifiesto la insuficiencia de los enfoques tradicionales para abordar los desafíos contemporáneos (Mourad y Luers, 2017).

Aquí es donde el marco teórico de Thomas Kuhn y su concepto de cambio de paradigma resulta útil para comprender esta transición. Según Kuhn, los paradigmas científicos cambian cuando el paradigma existente no puede explicar anomalías significativas (Khun, 1962).

En este caso, las anomalías son las nuevas amenazas interconectadas del Antropoceno, que requieren una redefinición del concepto de seguridad.

El informe del PNUD de 2022 representa un esfuerzo por actualizar el paradigma de la seguridad humana para responder a las demandas del Antropoceno. Esta actualización se basa en tres pilares fundamentales: la protección, el empoderamiento y la solidaridad (Nations, 2022).

En primer lugar, la protección sigue siendo esencial, pero se extiende más allá de los límites del Estado-nación para incluir a los individuos y las comunidades vulnerables, así como los sistemas ecológicos que sustentan la vida. En segundo lugar, el empoderamiento se destaca como un componente central, enfatizando la capacidad de las personas para tomar decisiones y actuar frente a los desafíos. Finalmente, la solidaridad emerge como el eje transformador de este paradigma, reconociendo la interdependencia entre los seres humanos y entre estos y el planeta.

El Antropoceno plantea desafíos únicos que requieren un replanteamiento de las estrategias de seguridad. El cambio climático,

por ejemplo, no solo representa un peligro físico en términos de desastres naturales, sino que también incrementa la inseguridad alimentaria, los desplazamientos forzados y las tensiones sociales (Werrell y Femia, 2017). La pérdida de biodiversidad y la degradación de ecosistemas clave, como los bosques tropicales y los océanos, amenazan la estabilidad de los sistemas que sostienen la vida (Hawa, 2017).

Este nuevo paradigma no busca reemplazar las teorías clásicas de seguridad, sino complementarlas y ampliarlas para abordar las realidades del siglo XXI. Mientras que las perspectivas de Herz y Waltz siguen siendo relevantes en contextos interestatales, el paradigma del Antropoceno introduce una capa adicional que incluye la seguridad ecológica, la justicia global y la resiliencia comunitaria.

Este enfoque integrado refleja un cambio en el pensamiento sobre la seguridad, similar a los cambios de paradigma descritos por Kuhn, donde las soluciones tradicionales ya no son suficientes para explicar y abordar las anomalías emergentes (Chad M. Briggs, 2017).

En conclusión, el informe del PNUD de 2022 marca un cambio transformador en el concepto de seguridad humana. Al reconocer las complejas interconexiones del Antropoceno, este nuevo paradigma aboga por una seguridad basada en la protección, el empoderamiento y la solidaridad.

Este enfoque integral no solo responde a las amenazas inmediatas, sino que también busca transformar las relaciones entre los seres humanos y el planeta para construir un futuro más equitativo, resiliente y sostenible. Este cambio de paradigma representa una evolución necesaria y oportuna en un mundo que enfrenta desafíos sin precedentes.

1.6 El Pyroceno, la potencia de fuego civil y sus consecuancias

Stephen J. Pyne introduce el concepto de Pyroceno como una nueva era definida por el impacto transformador del fuego en el planeta, impulsado por actividades humanas modernas como la industrialización y el consumo masivo de energía (Pyne, 2019). Tal y como indican Callahan y Mankin, este exceso de fuego, reflejado en las emisiones industriales, desestabilizan los ecosistemas y agrava las desigualdades globales, afectando gravemente a las regiones más vulnerables (Callahan y Mankin, 2022).

Desde esta perspectiva, Simon Dalby complementa el análisis con la noción de «potencia de fuego civil», subrayando la necesidad de un cambio en nuestra relación con el fuego para mitigar los riesgos ambientales y socioeconómicos del Antropoceno (Dalby, 2023a).

Desde los primeros momentos en que los humanos aprendieron a controlar el fuego, este se convirtió en una herramienta poderosa para cambiar paisajes, cocinar alimentos y crear tecnologías. Sin embargo, en el mundo moderno, el uso del fuego ha pasado de ser una herramienta práctica a convertirse en una fuerza global que impacta profundamente el clima y los ecosistemas (Pyne, 2019). En este sentido, el concepto de Pyroceno encaja perfectamente dentro de la idea de potencia de fuego civil que plantea Simon Dalby en el contexto del Antropoceno (Dalby, 2023a).

La potencia de fuego civil no se refiere al uso de armas o herramientas militares, sino a la capacidad destructiva de las actividades humanas cotidianas, como la industrialización, el consumo de energía y la urbanización.

La acumulación de gases de efecto invernadero en la atmósfera, resultado de estas actividades, es una forma de «combustión» constante que desestabiliza los sistemas naturales y afecta de manera desigual a los países del mundo.

Los efectos del Pyroceno y de esta potencia de fuego civil se sienten especialmente en los países más vulnerables, que sufren los peores impactos del cambio climático, como sequías, incendios y desastres naturales, a pesar de ser los que menos han contribuido al problema. Por otro lado, los países ricos han obtenido beneficios de esta combustión industrial, perpetuando desigualdades globales.

El estudio «National Attribution of Historical Climate Damages» de Callahan y Mankin (2022) arroja luz sobre esta desigualdad. Según sus hallazgos, las emisiones históricas de los cinco principales emisores; Estados Unidos, China, Rusia, Brasil e India, han causado pérdidas de ingresos estimadas en seis billones de dólares desde 1990, equivalentes al 11 % del PIB global anual. Estas pérdidas económicas se concentran mayormente en países tropicales y de bajos ingresos, que sufren los mayores impactos debido a las temperaturas extremas y la degradación ambiental resultante (Callahan y Mankin, 2022).

El marco analítico desarrollado por Callahan y Mankin combina datos históricos con modelos climáticos para atribuir daños económicos a naciones específicas. Los resultados muestran que las naciones desarrolladas y emisoras han transferido riqueza desde los países más vulnerables hacia sus propias economías, beneficiándose de climas más favorables para la productividad agrícola y laboral. En contraste, las regiones tropicales, como el sur de Asia y África, enfrentan pérdidas devastadoras, incrementando las desigualdades económicas globales (Callahan y Mankin, 2022).

En resumen, el Pyroceno de Pyne (2019) y la potencia de fuego civil de Dalby (2023) describen la misma realidad desde perspectivas complementarias: el impacto desproporcionado de las actividades humanas en el clima y los ecosistemas. Ambos conceptos subrayan la necesidad urgente de repensar nuestra relación con el fuego y el planeta para evitar consecuencias catastróficas como las que constatan Callahan y Mankin (2022).

1.7 Simon Dalby y el nuevo enfoque de seguridad

Simon Dalby[43] centra sus intereses de investigación actuales en la discusión contemporánea sobre seguridad climática y el creciente debate sobre el Antropoceno y sus implicaciones para la geopolítica y la formulación de políticas.

El paradigma de seguridad en el Antropoceno, formulado por Simon Dalby, marca un punto de inflexión en la manera de conceptualizar y abordar las amenazas contemporáneas (Dalby, 2023a). En un mundo profundamente alterado por las actividades humanas, Dalby plantea que las teorías tradicionales de seguridad, diseñadas para un contexto de rivalidades interestatales y amenazas externas, han perdido eficacia frente a las dinámicas sistémicas y transnacionales que caracterizan esta nueva era (Dalby, 2023a).

En este sentido, su marco teórico proporciona un enfoque crítico y renovador para estudiar las estrategias de seguridad, considerando no solo a los Estados como actores principales, sino también las interacciones ecológicas y sociales que influyen en la estabilidad planetaria (Dalby 2023b).

[43] (UVIC, 2025): Datos obtenidos de la página web. Universidad de Victoria (Canadá), https://www.uvic.ca/research/centres/globalstudies/people/fellows/dalbysimon.php

La idea de que el Antropoceno introduce un escenario sin precedentes, donde las actividades humanas se convierten en fuerzas transformadoras de los sistemas planetarios, resulta central en el pensamiento de Dalby (2016).

Este contexto le lleva a cuestionar las nociones clásicas de seguridad, no como una crítica destructiva, sino como una reflexión que busca superar sus limitaciones y proponer alternativas más acordes con los retos actuales (Dalby, 2016).

Así, el paradigma de seguridad de Dalby parte de reconocer que las amenazas contemporáneas no se limitan a los conflictos armados ni a las rivalidades territoriales, sino que surgen de fenómenos como el cambio climático, la degradación ambiental, la pérdida de biodiversidad y la creciente desigualdad global (Dalby, 2023a).

A diferencia de las teorías clásicas como el realismo estructural de Kenneth Waltz (Moure, 2009) o el dilema de seguridad de John Herz (1950), que conceptualizan la seguridad como un fenómeno principalmente estatal, Dalby amplía el enfoque hacia un análisis global y multidimensional (Dalby, 2016).

En las teorías tradicionales, los Estados son concebidos como actores racionales que buscan maximizar su supervivencia en un sistema anárquico, donde la ausencia de una autoridad central fomenta la competencia por el poder y la desconfianza mutua. Estas teorías, durante la Guerra Fría, priorizaban la acumulación de poder militar y la disuasión como herramientas esenciales para mantener el equilibrio y la estabilidad (Castañeda y Merino, 2015).

Sin embargo, Dalby considera que este marco teórico resulta inadecuado para abordar los retos del Antropoceno. Las amenazas actuales, como el cambio climático y las alteraciones en los sistemas ecológicos globales, no pueden ser contenidas por fronteras ni resueltas mediante soluciones tradicionales basadas en la competencia y la autarquía. En lugar de ello, requieren respuestas coordinadas a nivel internacional, lo que supone un desafío fundamental para las teorías clásicas (Dalby, 2023a).

Este replanteamiento se concreta en conceptos como la «potencia de fuego civil», introducido por Dalby para describir cómo las actividades humanas, como la industrialización y la combustión masiva de combustibles fósiles, generan impactos globales que desestabilizan los sistemas naturales.

En este contexto, la «potencia de fuego civil» no solo representa una transformación de los riesgos de seguridad, sino también una llamada de atención sobre la verdadera naturaleza de las amenazas contemporáneas. A diferencia de las carreras armamentistas tradicionales, que operaban en el ámbito militar, esta potencia de fuego es una consecuencia directa de los modos de vida modernos y afecta a la seguridad en múltiples dimensiones, desde la económica hasta la ecológica (Dalby, 2023a).

Así, Dalby plantea que la verdadera amenaza no proviene de un enemigo externo, sino de las dinámicas internas de nuestras sociedades y economías, que perpetúan un modelo insostenible (Dalby, 2023b).

Al introducir la noción de seguridad ecológica como una categoría fundamental, Dalby destaca la importancia de proteger los sistemas ecológicos que sustentan la vida en el planeta. Este enfoque reconoce que la degradación ambiental no solo tiene consecuencias directas sobre los ecosistemas, sino que también afecta la estabilidad social, económica y política de las naciones. Por ejemplo, fenómenos como la pérdida de biodiversidad, el aumento del nivel del mar o las sequías prolongadas generan desplazamientos forzados, inseguridad alimentaria y tensiones geopolíticas, configurando un panorama de riesgos interconectados que trascienden las capacidades de los Estados individuales para responder (Dalby, 2023b).

Junto con la seguridad ecológica, Dalby incorpora la justicia climática como un pilar esencial de su paradigma. Este concepto pone de manifiesto las desigualdades inherentes al impacto del cambio climático, donde las naciones industrializadas, principales responsables históricas de las emisiones de gases de efecto invernadero, enfrentan menos riesgos directos que las regiones más vulnerables, como el sur de Asia, África subsahariana y América Latina (Dalby, 2023a).

Para Dalby, estas desigualdades no solo son éticamente problemáticas, sino que también representan un desafío para la estabilidad global. Abordar la justicia climática implica reconocer la responsabilidad histórica de las naciones desarrolladas y promover políticas que protejan a las comunidades más afectadas, integrando la sostenibilidad y la equidad en las estrategias de seguridad (Dalby, 2023a).

El concepto de «Pyroceno», desarrollado por Stephen Pyne (2019) y complementado por las ideas de Dalby, añade una

dimensión crítica al análisis de las amenazas del Antropoceno. En este marco, el fuego, que durante milenios fue una herramienta clave en la evolución humana, se convierte en una fuerza global que amplifica el cambio climático y desestabiliza los ecosistemas. La «potencia de fuego civil», según Dalby, refleja cómo las actividades humanas han transformado el uso del fuego en una amenaza sistémica que afecta tanto a las naciones más ricas como a las más pobres, aunque con impactos desiguales (Dalby, 2023a).

Este enfoque desafía las narrativas tradicionales de seguridad, que tienden a concebir las amenazas como fenómenos localizados y manejables dentro de marcos interestatales. En contraste, Dalby argumenta que la seguridad en el Antropoceno debe concebirse como un esfuerzo global que mitigue los impactos del cambio climático, reduzca la dependencia de los combustibles fósiles y promueva sistemas resilientes capaces de enfrentar los desafíos del futuro (Dalby, 2016).

En este sentido, el paradigma de Simon Dalby proporciona un marco teórico esencial para analizar las estrategias de seguridad nacional de España y Francia. Ambas naciones, como miembros de la Unión Europea y actores relevantes en la política internacional, enfrentan la presión de adaptar sus políticas de seguridad a los desafíos del Antropoceno.

Este trabajo analizará hasta qué punto estas estrategias reflejan los principios propuestos por Dalby, como la integración de la sostenibilidad, la justicia climática y la resiliencia frente a riesgos sistémicos.

Mientras que la Estrategia de Seguridad Nacional de España de 2021 reconoce el cambio climático como un «multiplicador de riesgos» y subraya la necesidad de fortalecer la resiliencia frente a desastres naturales, la Revisión Nacional Estratégica de Francia de 2022 parece adoptar un enfoque más tradicional, centrado en las amenazas militares y la estabilidad geopolítica.

Sin embargo, este análisis no busca emitir juicios prematuros, sino explorar en detalle cómo ambas estrategias incorporan, o no, las dinámicas globales del Antropoceno y qué implicaciones tiene esto para su efectividad en un contexto de riesgos crecientes.

Dalby resulta relevante como marco teórico porque ofrece una perspectiva crítica y transformadora que permite superar las limitaciones de las teorías clásicas. Su énfasis en la seguridad ecológica y la justicia climática, junto con su capacidad para articular

un enfoque integrado que abarca las dimensiones éticas, sociales y planetarias de la seguridad, lo posiciona como un referente clave para abordar los desafíos contemporáneos (Dalby, 2023a).

Este paradigma no solo enriquece el análisis académico, sino que también aporta herramientas prácticas para replantear las estrategias de seguridad en un mundo profundamente interconectado y afectado por las acciones humanas (Werrell *et al*., 2017).

En resumen, el paradigma de seguridad en el Antropoceno de Simon Dalby no solo cuestiona las nociones tradicionales, sino que también ofrece una visión renovada y oportuna para responder a las complejidades del siglo XXI (Dalby, 2023b). Este marco teórico será fundamental para analizar las estrategias de España y Francia, evaluando si se adaptan a las demandas de un mundo en transformación o si permanecen ancladas en enfoques obsoletos. Dalby se presenta, así, como un referente indispensable para reconfigurar la seguridad en un contexto global de riesgos sistémicos e interdependencia.

2 Estrategia de Seguridad Nacional de España

La Estrategia de Seguridad Nacional (ESN) de España 2021 constituye un marco esencial para abordar los desafíos del siglo XXI, combinando continuidad con una adaptación a nuevas realidades globales como la transición ecológica, las campañas de desinformación y el cambio climático.

Este capítulo analiza la ESN en tres dimensiones: primero, su estructura y objetivos estratégicos; segundo, el impacto del cambio climático en la seguridad nacional, y finalmente su alineación con las teorías contemporáneas de Simon Dalby y el paradigma del Antropoceno.

Este enfoque integral busca determinar si la estrategia española sigue un modelo tradicional o se adapta a los retos globales emergentes.

2.1 Principales características de la Estrategia de Seguridad Nacional de España 2021

La Estrategia de Seguridad Nacional (ESN 2021) establece un marco que combina la continuidad con la adaptación al cambio, en un contexto global marcado por la incertidumbre y las transformaciones aceleradas. La Estrategia refleja la herencia de

documentos anteriores, manteniendo una visión integral de la seguridad nacional, pero al mismo tiempo incorpora nuevas prioridades, como las campañas de desinformación y la transición ecológica, adaptándose a los retos actuales y futuros.

La ESN 2021 está estructurada en cinco capítulos que abordan los ejes fundamentales de la seguridad nacional:

El capítulo 1, titulado «Seguridad Global y Vectores de Transformación», analiza el contexto internacional marcado por la pandemia de COVID-19, que ha acelerado dinámicas globales preexistentes. Este escenario es descrito como una etapa de transición, donde la incertidumbre sobre el futuro convive con dos grandes motores de cambio: la transformación digital y la transición ecológica. Al mismo tiempo, se reconoce un aumento de la competencia geopolítica, lo que obliga a adoptar una visión estratégica que permita a España proteger sus intereses y responder a los desafíos del nuevo orden mundial. (ESN 2021).

El capítulo 2, denominado «Una España Segura y Resiliente», ofrece un análisis del papel estratégico de España como país de condición europea, mediterránea y atlántica. Este capítulo destaca su relación con regiones clave como Europa, el Magreb, África Subsahariana, América Latina, América del Norte y la región Asia-Pacífico, subrayando la necesidad de reforzar la resiliencia tanto interna como en colaboración con socios internacionales. España se percibe como un actor clave en su entorno geoestratégico, con un papel activo en la estabilidad regional y global (ESN 2021).

Por su parte, el capítulo 3, titulado «Riesgos y Amenazas», identifica los principales desafíos que enfrenta la seguridad nacional. Se destaca la interrelación y dinamismo de los riesgos, donde la desinformación se incorpora por primera vez como una amenaza relevante, junto con la tecnología y las estrategias híbridas, consideradas elementos transversales que afectan todos los ámbitos de seguridad. La incorporación de estos riesgos refleja una actualización necesaria para abordar las nuevas amenazas del siglo XXI, con especial atención a su impacto en la cohesión social y la estabilidad de las instituciones democráticas (ESN 2021).

En el capítulo 4, titulado «Un Planeamiento Estratégico Integrado», se establecen tres objetivos prioritarios que guían la acción de seguridad nacional en el próximo ciclo estratégico. En primer lugar, se propone avanzar en la gestión de crisis mediante la anticipación y la mejora de los mecanismos de respuesta (ESN 2021). En segundo lugar, se busca fortalecer la seguridad de

las capacidades tecnológicas y los sectores estratégicos, asegurando su protección frente a amenazas externas (ESN 2021). Por último, se pretende desarrollar capacidades preventivas, de detección y respuesta frente a las estrategias híbridas, especialmente aquellas que combinan desinformación y ciberataques (ESN 2021). Para lograr estos objetivos, se plantean tres ejes de acción: proteger, promover y participar, con medidas concretas como la creación de una reserva estratégica y el desarrollo de un sistema de alerta temprana basado en la tecnología (ESN 2021).

Finalmente, el capítulo 5, centrado en la «Gestión de Crisis en el Sistema de Seguridad Nacional», aborda la necesidad de reforzar la resiliencia del país en todas las etapas de una crisis, desde la prevención hasta la recuperación. Se proponen seis medidas clave, entre las que destacan la elaboración de un catálogo de recursos, la preparación de planes de respuesta, y la mejora de las comunicaciones interinstitucionales mediante soluciones tecnológicas. Asimismo, se subraya la integración de las comunidades autónomas en el Sistema de Seguridad Nacional, asegurando una coordinación efectiva a nivel nacional (ESN 2021).

Dentro de este marco, el cambio climático ocupa un lugar destacado como una de las principales amenazas a la seguridad nacional (ESN 2021). La ESN 2021 reconoce que el cambio climático no solo tiene un impacto medioambiental, sino que constituye un factor desestabilizador con efectos directos e indirectos en la seguridad. Fenómenos como los eventos meteorológicos extremos, la escasez de recursos naturales y la inestabilidad en regiones vulnerables generan nuevas amenazas, como las migraciones forzadas y las crisis humanitarias, que exigen respuestas coordinadas y preventivas. (ESN 2021).

En este sentido, la transición ecológica con una clara evolución hacia una economía descarbonizada, se presenta no solo como una necesidad medioambiental, sino como una herramienta estratégica para fortalecer la resiliencia de España frente a los efectos del cambio climático (ESN 2021).

La ESN 2021 apuesta por políticas de sostenibilidad, la protección de infraestructuras críticas y el uso de la tecnología y la innovación para anticipar y mitigar los riesgos asociados al clima. Esta visión sitúa a la seguridad climática como una prioridad transversal en el marco de la seguridad nacional (ESN 2021).

Uno de los aspectos más destacados es la mención al impacto del cambio climático en regiones vulnerables como el África

Subsahariana. La ESN 2021 subraya cómo las condiciones climáticas extremas y los desastres naturales agravan la fragilidad estructural ya existente en esta región (ESN 2021).

En particular, la crisis de gobernabilidad, la ausencia del Estado en grandes áreas y la presión sobre los recursos, provocada por el crecimiento demográfico, generan un caldo de cultivo para fenómenos como el terrorismo yihadista, los conflictos intercomunitarios y el tráfico ilícito (ESN 2021).

Esta situación, especialmente en el Sahel, no solo afecta a los países de la región, sino que extiende su inestabilidad hacia el norte de África y, en última instancia, repercute en la seguridad de Europa y de España (ESN 2021).

Además, la ESN 2021 establece una relación directa entre el deterioro medioambiental y la inestabilidad de los países del entorno inmediato de España, como el Magreb. La desertificación y la escasez de recursos esenciales, como el agua, incrementan las tensiones sociales y políticas, dando lugar a conflictos regionales y migraciones forzosas hacia Europa (ESN 2021).

Esta realidad demuestra que el cambio climático no es un fenómeno aislado, sino un factor que multiplica otras amenazas, afectando la estabilidad regional y la cohesión social.

En este contexto, la transición ecológica y la seguridad energética se integran en el Eje 2 «Promover» de la estrategia (ESN 2021).

La ESN 2021 apuesta por un modelo energético sostenible que reduzca la dependencia de los combustibles fósiles y refuerce la resiliencia energética de España. Para lograrlo, propone la actualización de la Estrategia de Seguridad Energética Nacional y la alineación de sus objetivos con el Pacto Verde Europeo y los Acuerdos de París. Asimismo, destaca la necesidad de diversificar las fuentes de energía y fomentar infraestructuras resilientes, subrayando la importancia de las energías renovables como una herramienta estratégica para avanzar hacia la descarbonización y, al mismo tiempo, garantizar la seguridad del suministro energético (ESN 2021).

Por otra parte, la ESN 2021 a través de su Eje 3 «Participar» (ESN 2021) refuerza su compromiso con la preservación del medio ambiente y el desarrollo sostenible, reconociendo la importancia de luchar contra el cambio climático en línea con los Acuerdos de París de 2015 y la Agenda 2030 (ESN 2021).

En este sentido, se incluyen dos Líneas de Acción concretas. La primera, la Línea de Acción 32, propone integrar la Agenda 2030 en las políticas de cooperación al desarrollo, con el objetivo de reforzar las capacidades de los países más vulnerables para prepararse frente al cambio climático. La segunda, la Línea de Acción 33, promueve los objetivos del área «paz, seguridad y cohesión social» del Plan Nacional de Adaptación al Cambio Climático 2021-2030, priorizando la detección temprana y la prevención de conflictos derivados de los efectos climáticos (ESN 2021).

En conclusión, la ESN 2021 combina continuidad con una adaptación clara a los desafíos emergentes. Se ofrece una visión integral y actualizada de la seguridad nacional, donde el cambio climático y la transición ecológica ocupan un lugar central, no solo por su impacto directo, sino también por su capacidad para amplificar otras amenazas. La apuesta por la resiliencia, la innovación tecnológica y la colaboración internacional se presenta como clave para garantizar la estabilidad y el progreso de España en un futuro incierto.

El cambio climático debe entenderse como un multiplicador de amenazas que, en el entorno ampliado de España: Magreb, Sahel y África Subsahariana, activa una cadena causal con efectos directos sobre la seguridad nacional.

El punto de partida es el deterioro climático: aumento de temperaturas, desertificación y episodios meteorológicos extremos. Este proceso incrementa la escasez de recursos, en particular agua y tierras cultivables, y agrava el impacto de los desastres naturales. Como consecuencia, se intensifican las crisis humanitarias y la inseguridad alimentaria. Cuando la supervivencia cotidiana queda condicionada por recursos cada vez más limitados, la competencia por la tierra y el acceso al agua tiende a traducirse en tensiones sociales y conflictos intercomunitarios.

A la vez, la debilidad institucional y los problemas de gobernabilidad reducen la capacidad de los Estados para contener esas dinámicas y atender a la población. En ese vacío, encuentran margen de expansión tanto el crimen organizado como los grupos yihadistas, que aprovechan la fragilidad estatal para consolidar rutas, financiación e influencia territorial. Desde esta perspectiva, el Magreb adquiere un relieve particular: los flujos migratorios que lo atraviesan generan presión política y social y, en determinados casos, convierten a estos países en espacios de tránsito y

contención. Este papel se ve agravado por el estrés hídrico y la desertificación, que alimentan tensiones internas y regionales y contribuyen a un escenario de inestabilidad creciente.

Para España y Europa, el impacto se percibe de forma directa y acumulativa. Las oleadas migratorias ponen a prueba de manera recurrente los sistemas de acogida y la cohesión social, elevando la fricción política y social. Paralelamente, la inseguridad en el Sahel y el Magreb actúa como catalizador del fortalecimiento de redes criminales asociadas a rutas irregulares y economías ilícitas, mientras que la presencia y expansión de actores yihadistas incrementa el riesgo de proyección de amenazas hacia el continente europeo, tanto por radicalización como por conectividad operativa.

Ante este escenario, la Estrategia de Seguridad Nacional 2021 plantea una respuesta de carácter preventivo y orientada a la resiliencia. Por un lado, impulsa la transición ecológica y la seguridad energética para reducir dependencias estructurales y reforzar infraestructuras críticas; por otro, apuesta por la cooperación internacional a través de marcos como la Agenda 2030 y el Acuerdo de París, apoyando programas que incrementen la resiliencia de los países más vulnerables. En la misma línea, el Plan Nacional de Adaptación al Cambio Climático 2021-2030 incorpora mecanismos de anticipación y alerta temprana, con el objetivo de mitigar dinámicas de inestabilidad vinculadas al clima y priorizar la estabilidad en regiones de origen relevantes para la seguridad de España.

2.2 El impacto del cambio climático en España

El cambio climático se presenta como uno de los mayores retos para España en la actualidad, según se desprende del Informe Anual de la Estrategia de Seguridad Nacional 2023. Este desafío no solo tiene implicaciones ambientales, sino también económicas, sociales y de seguridad. Las alteraciones climáticas están afectando de manera transversal a España, incrementando vulnerabilidades preexistentes y generando nuevas amenazas que requieren de respuestas inmediatas y coordinadas (IASN, 2023).

En primer lugar, cabe destacar que 2023 fue el año más cálido registrado a nivel global, un dato que subraya la urgencia de abordar esta problemática. Según la Organización Meteorológica Mundial (OMM), la temperatura media anual del planeta superó

en 1,45 °C los niveles preindustriales, acercándose peligrosamente a los límites establecidos por el Acuerdo de París (IASN, 2023).

Este patrón de calentamiento no es nuevo; desde 2015, todos los años se han situado entre los más cálidos desde que se tienen registros instrumentales en 1850. En el caso de España, esta tendencia se traduce en un incremento de la temperatura media de 0,22 °C por década desde 1961, con un aumento más pronunciado en verano (+0,26 °C/decenio) que en invierno (+0,19 °C/decenio). Este fenómeno ha intensificado la frecuencia y gravedad de las olas de calor, afectando tanto a la población como a los ecosistemas (IASN, 2023).

Los efectos del cambio climático en España son particularmente visibles en la incidencia de fenómenos meteorológicos extremos, como incendios forestales, inundaciones y sequías prolongadas. Durante 2023, el país experimentó una sequía meteorológica severa que derivó en déficits hídricos generalizados, afectando tanto a las cuencas superficiales como a los acuíferos subterráneos. De hecho, el año hidrológico 2022-2023 fue el decimoséptimo más seco desde 1961, con precipitaciones que alcanzaron solo el 90 % de su valor normal.

Esta situación se reflejó en los embalses, que cerraron el año con un 45 % de su capacidad, muy por debajo de la media de los últimos diez años (IASN, 2023). En particular, las cuencas internas de Cataluña, así como las del Segura, Guadalquivir y Mediterráneo andaluz, se enfrentaron a niveles críticos, con graves repercusiones para el abastecimiento humano, los regadíos agrícolas y la producción de energía hidroeléctrica (IASN, 2023).

El ascenso del nivel del mar es otro impacto destacado del calentamiento global. Las zonas costeras españolas, especialmente el estrecho de Gibraltar, el archipiélago canario y la costa atlántica, están sufriendo los efectos de la erosión, las inundaciones y la salinización. Estas alteraciones representan una amenaza significativa para la biodiversidad y los ecosistemas marinos, además de poner en riesgo infraestructuras críticas y comunidades costeras (IASN, 2023).

La desertificación es otro problema de gran relevancia en España, agravado por el aumento de las temperaturas y la disminución de la disponibilidad de agua para las plantas. Este fenómeno ha provocado que climas anteriormente templados se transformen en áridos, especialmente en las regiones del sur y el este peninsular.

En términos de biodiversidad, el calentamiento global está teniendo efectos devastadores sobre ecosistemas vulnerables y especies animales. La pérdida de biodiversidad es cada vez más pronunciada, especialmente en el medio marino.

En el Mediterráneo, el aumento de la temperatura del agua ha favorecido la llegada de especies invasoras de peces y algas, lo que está alterando los ecosistemas locales. Además, las especies autóctonas están cambiando su distribución geográfica hacia el norte, en busca de condiciones climáticas más favorables (IASN, 2023). Estos cambios tienen implicaciones directas para el sector pesquero, con repercusiones económicas y sociales significativas.

Por otro lado, las emisiones de gases de efecto invernadero (GEI) son el principal motor del cambio climático. Aunque España ha logrado reducir sus emisiones brutas en un 34,2 % respecto a 2005, las concentraciones de los principales GEI, como el dióxido de carbono, metano y óxido nitroso, alcanzaron máximos históricos en 2021 (IASN, 2023).

Para hacer frente a este panorama, España ha adoptado una serie de medidas estratégicas y planes de acción. Entre ellas, destaca el Plan Nacional de Adaptación al Cambio Climático (PNACC), que incluye programas específicos para la conservación de suelos, la reforestación y la prevención de incendios forestales (IASN, 2023).

Además, el Plan Forestal Español 2022-2032 propone 289 medidas distribuidas en veinticinco líneas de acción para garantizar una gestión forestal sostenible y proteger los ecosistemas más amenazados (IASN, 2023).

A nivel internacional, España lidera junto con Senegal la Alianza Internacional para la Resiliencia a la Sequía, una iniciativa que busca fomentar la cooperación global en la lucha contra este fenómeno (IASN, 2023).

En términos de perspectiva futura, se identifica el cambio climático como uno de los riesgos de mayor impacto y probabilidad para la seguridad nacional. Según el Mapa de Riesgos para la Seguridad Nacional 2023, este fenómeno ocupa la categoría de «intensidad alta» debido a sus consecuencias multifacéticas (IASN, 2023). Además, se prevé que las tendencias actuales de calentamiento global, sequías y fenómenos extremos se mantendrán, lo que exigirá una planificación aún más robusta y sostenible en los próximos años.

En conclusión, el cambio climático constituye uno de los mayores desafíos para España, afectando a múltiples sectores y dimensiones de la seguridad nacional. Los impactos, como el calentamiento global, la desertificación, la pérdida de biodiversidad y la escasez hídrica, están transformando el paisaje ambiental y social del país. A pesar de los esfuerzos por mitigar sus efectos mediante políticas nacionales e internacionales, la velocidad y magnitud de estos cambios requieren una mayor inversión en innovación, cooperación y resiliencia. La lucha contra el cambio climático no solo es una cuestión ambiental, sino una prioridad estratégica para garantizar el bienestar y la seguridad de las generaciones presentes y futuras.

2.3 Alineación con las teorías contemporáneas de Simon Dalby y el paradigma del Antropoceno

La ESN 2021 representa un hito importante en la evolución del concepto de seguridad, adaptándose a los retos emergentes del siglo XXI. Esta estrategia combina la continuidad con una clara adaptación al cambio, al incorporar de manera prioritaria elementos como la transición ecológica, la lucha contra el cambio climático y el impacto de las amenazas transversales (ESN 2021).

Desde esta perspectiva, la ESN 2021 refleja una alineación significativa con el nuevo paradigma de seguridad defendido por el pensador contemporáneo Simon Dalby, quien reconfigura la visión tradicional de seguridad para situar las amenazas ambientales y climáticas como elementos centrales de la inseguridad global (Dalby, 2023b).

El cambio climático es reconocido en la ESN 2021 como una amenaza transversal, es decir, un fenómeno que afecta múltiples ámbitos de la seguridad: desde la estabilidad política hasta la seguridad económica y social. Fenómenos como los eventos meteorológicos extremos, la escasez de recursos esenciales y la degradación ambiental generan impactos directos e indirectos sobre las sociedades, especialmente en regiones ya de por sí vulnerables (ESN 2021).

La ESN 2021 se hace eco de este enfoque, destacando que el cambio climático no opera de forma aislada, sino que multiplica y agrava las amenazas existentes.

Esta idea coincide con la perspectiva de Simon Dalby, quien argumenta que las condiciones ambientales deterioradas incrementan

problemas preexistentes como la pobreza, la inseguridad alimentaria, los conflictos étnicos y la crisis de gobernabilidad (Dalby, 2023a).

Dalby utiliza el concepto de «multiplicador de amenazas» para describir cómo el cambio climático interactúa con las dinámicas sociales, políticas y económicas, generando inestabilidad y desplazamientos forzados (Dalby, 2023b).

En este sentido, la ESN 2021 identifica el problema, al destacar la necesidad de abordar las causas estructurales del cambio climático y anticipar sus efectos desestabilizadores mediante políticas de prevención y adaptación (ESN 2021).

La estrategia identifica regiones específicas como el África Subsahariana y el Sahel, donde los efectos del cambio climático se manifiestan de forma particularmente aguda (ESN 2021). La ESN 2021 indica que las condiciones climáticas extremas, junto con el crecimiento demográfico y la escasez de recursos, agravan la fragilidad estructural de estas regiones. Este contexto favorece la aparición de amenazas como el terrorismo yihadista, los conflictos intercomunitarios y el tráfico ilícito, generando un «efecto de arrastre» que afecta también al norte de África y, en consecuencia, a Europa y España (ESN 2021).

Simon Dalby insiste en que las amenazas climáticas no pueden ser abordadas de forma local o fragmentada; requieren un enfoque global y multilateral. (Dalby, 2013).

En este sentido, la ESN 2021 coincide plenamente con esta idea al apostar por la cooperación internacional como una herramienta clave para mitigar los efectos del cambio climático y reforzar la resiliencia de las sociedades vulnerables (ESN 2021).

Continuando con el marco del Antropoceno, la seguridad nacional ya no puede centrarse únicamente en las amenazas militares tradicionales, sino que debe ampliarse para abordar los riesgos ambientales y climáticos que afectan la estabilidad global. Simon Dalby sostiene que el paradigma de seguridad debe ser redefinido en términos de sostenibilidad, donde la resiliencia ecológica y la gestión responsable de los recursos naturales se convierten en pilares fundamentales (Dalby, 2023b).

La ESN 2021 refleja esta transformación del concepto de seguridad al situar la transición ecológica (ESN 2021) y la lucha contra el cambio climático en el centro de su agenda (ESN 2021). La estrategia reconoce que las alteraciones climáticas y la degra-

dación ambiental no son solo problemas medioambientales, sino también factores desestabilizadores con repercusiones en la seguridad humana, la paz internacional y la gobernabilidad global. Este enfoque queda plasmado en varios puntos clave de la estrategia.

Por ejemplo, la ESN 2021 destaca la importancia de garantizar la seguridad energética mediante la reducción de la dependencia de combustibles fósiles y la promoción de un modelo energético sostenible. (ESN 2021). El Eje 2: Promover se centra en impulsar la transición ecológica como una herramienta estratégica para fortalecer la resiliencia del país frente a los riesgos climáticos. La apuesta por las energías renovables, la eficiencia energética y la diversificación de fuentes energéticas son medidas que no solo contribuyen a la lucha contra el cambio climático, sino que también refuerzan la soberanía energética y la estabilidad económica de España (ESN 2021).

En paralelo, la estrategia promueve la integración de la Agenda 2030 en las políticas de cooperación al desarrollo, con el objetivo de fortalecer las capacidades de los países más vulnerables frente al cambio climático. La Línea de Acción 32 propone medidas concretas para apoyar a estas naciones en la construcción de resiliencia y en la mitigación de los impactos climáticos. Del mismo modo, la Línea de Acción 33 se centra en la detección temprana de conflictos derivados del cambio climático, reconociendo la necesidad de identificar las regiones y poblaciones más vulnerables para evitar que estas situaciones desemboquen en crisis humanitarias y conflictos armados (ESN 2021).

Esta visión multidimensional del cambio climático se alinea perfectamente con el enfoque de Dalby, quien defiende que las políticas de seguridad deben ser preventivas y abordar las causas estructurales de la inseguridad (Dalby, 2023a). En lugar de reaccionar a las crisis, la estrategia española apuesta por la detección temprana, la adaptación y la cooperación internacional como pilares fundamentales para construir un entorno más seguro y resiliente.

Una de las contribuciones más importantes de la ESN 2021 es su análisis detallado del impacto del cambio climático en regiones específicas, particularmente en el África Subsahariana y el Magreb. La estrategia identifica estas zonas como especialmente vulnerables debido a la combinación de factores climáticos, demográficos y socioeconómicos (ESN 2021).

En el caso del África Subsahariana, la ESN subraya que los desastres naturales, las sequías prolongadas y la desertificación agravan una situación de fragilidad estructural ya existente. La falta de gobernabilidad, la ausencia del Estado en grandes áreas y la presión sobre los recursos naturales generan un caldo de cultivo para el surgimiento de amenazas como el terrorismo, los conflictos armados y el tráfico ilícito. Además, la estrategia destaca cómo esta inestabilidad se extiende hacia el norte de África, afectando directamente la seguridad regional y la estabilidad europea (ESN 2021).

Por otro lado, en el Magreb, el cambio climático se manifiesta principalmente a través de la escasez de agua y la degradación de los ecosistemas, lo que genera tensiones sociales y conflictos por recursos. Esta situación se ve agravada por la desertificación y los movimientos migratorios, que generan presión adicional sobre las fronteras europeas (ESN 2021).

La ESN 2021 aborda esta problemática desde una perspectiva preventiva, proponiendo medidas que fortalezcan la resiliencia de estas regiones y mitiguen los efectos del cambio climático a través de la cooperación internacional y el desarrollo sostenible.

La actual Estrategia de 2021, refleja una evolución importante en el concepto de seguridad nacional, alineándose con el nuevo paradigma de seguridad defendido por Simon Dalby. Al situar el cambio climático y la transición ecológica en el centro de su agenda, la estrategia española reconoce que los riesgos ambientales y climáticos son las nuevas fuentes de inseguridad global.

Simon Dalby argumenta que la seguridad debe ser redefinida en términos de sostenibilidad y resiliencia, con un enfoque preventivo y adaptativo (Dalby, 2023b). La ESN 2021 adopta esta lógica al proponer medidas concretas como la detección temprana de conflictos climáticos, la integración de la Agenda 2030 en las políticas de desarrollo y la promoción de un modelo energético sostenible basado en las energías renovables.

En definitiva, la ESN 2021 no solo responde a los retos del Antropoceno, sino que también se posiciona como un documento vanguardista que integra las recomendaciones de Dalby y otros teóricos contemporáneos, como Nyman, Rockström, Gaffney, Lewis y Maslin.

Al priorizar la cooperación internacional, la resiliencia climática y la transición ecológica, España adopta una visión integral y actua-

lizada de la seguridad, capaz de enfrentar los desafíos emergentes y garantizar la estabilidad a largo plazo.

3 Revisión Nacional Estrategia de Francia 2022

La Revisión Nacional Estratégica de Francia 2022 (RNE) surge en un contexto global de crecientes tensiones geopolíticas y crisis climáticas. Este capítulo analiza primero la estrategia de seguridad francesa desde una perspectiva general, destacando sus prioridades y objetivos principales. Luego, aborda cómo el cambio climático afecta al país, exponiendo sus desafíos ecológicos, sociales y económicos. Por último, se examina si esta revisión estratégica sigue un enfoque tradicional o si se alinea con el paradigma del Antropoceno propuesto por Simon Dalby.

3.1 Principales características de la revisión estrategica de Francia 2022

El contexto en el que surge la RNE está profundamente marcado por lo que el documento describe como una «fractura del orden mundial». Esta ruptura se manifiesta en varios frentes: la intensificación de las rivalidades estratégicas entre potencias como China, Rusia y Estados Unidos; el debilitamiento de los marcos multilaterales, y el retorno de conflictos de alta intensidad en Europa. Estos factores han obligado a Francia a revisar su enfoque estratégico, identificando no solo las amenazas más inmediatas, sino también los riesgos emergentes que podrían redefinir el panorama de seguridad en el siglo XXI (RNE, 2022).

Según la RNE, estas dinámicas exigen una respuesta global y coordinada que combine la modernización de nuestras capacidades, el fortalecimiento de nuestras alianzas y la defensa de la autonomía estratégica (RNE, 2022).

Uno de los elementos más destacados del diagnóstico es el retorno de los conflictos interestatales de alta intensidad, ejemplificado por la invasión rusa de Ucrania. Este conflicto no solo ha puesto en evidencia la vulnerabilidad de Europa frente a potencias revisionistas, sino que también ha generado una crisis energética y alimentaria global. Según el análisis francés, este evento marca un punto de inflexión estratégico, que confirma tendencias ya detectadas en revisiones anteriores, como la competencia cre-

ciente entre grandes potencias y el uso de estrategias híbridas (RNE, 2022).

En este contexto, Rusia se presenta como un actor desestabilizador que utiliza tanto la coerción militar como herramientas no convencionales, como la manipulación de recursos energéticos, para debilitar a sus adversarios (RNE, 2022).

Simultáneamente, China emerge como una potencia en ascenso, cuya influencia crece en múltiples frentes: económico, tecnológico y militar. El documento señala que el aumento de la capacidad nuclear china y su estrategia de expansión en regiones clave, como el Indo-Pacífico, representan un desafío directo al liderazgo occidental (RNE, 2022). Esta situación, unida a la creciente interdependencia económica con Beijing, obliga a Francia a equilibrar su respuesta, fortaleciendo sus alianzas con socios internacionales sin renunciar a su independencia estratégica (RNE, 2022).

Además de estas tensiones geopolíticas, la RNE identifica un crecimiento en las amenazas híbridas, que combinan acciones convencionales y no convencionales para socavar la estabilidad de los estados. Estas amenazas incluyen ciberataques, campañas de desinformación, el uso estratégico de las normas internacionales para debilitar a las democracias y la manipulación de flujos económicos y logísticos.

En el análisis francés, estas tácticas representan un desafío particular porque aprovechan las vulnerabilidades de las sociedades modernas, como su dependencia de infraestructuras digitales y su exposición a las crisis de confianza en las instituciones (RNE, 2022). Un ejemplo destacado es el uso de la desinformación en redes sociales para influir en procesos democráticos, una estrategia utilizada tanto por actores estatales como no estatales (RNE, 2022).

En este contexto, Francia también reconoce el papel desestabilizador del cambio climático y otros riesgos ambientales, como la pérdida de biodiversidad y la escasez de recursos hídricos (RNE, 2022). Aunque estos fenómenos no ocupan un lugar central en la estrategia, se mencionan como «multiplicadores de tensiones», que incrementan conflictos preexistentes y generan nuevas crisis, como migraciones masivas o inseguridad alimentaria (RNE, 2022).

Ante este diagnóstico, la RNE establece diez objetivos estratégicos que buscan garantizar la soberanía nacional, reforzar las

capacidades defensivas y consolidar el liderazgo de Francia dentro de Europa.

Entre estos objetivos, uno de los más destacados es la disuasión nuclear. Según el documento, esta capacidad tiene como propósito proteger a Francia de cualquier agresión estatal contra sus intereses vitales y garantizar su autonomía de decisión frente a intentos de chantaje (RNE, 2022).

En un mundo donde las amenazas nucleares han resurgido con fuerza, Francia apuesta por mantener un arsenal creíble y adaptado a los avances tecnológicos, como las armas hipersónicas y las operaciones híbridas (RNE, 2022).

Junto con la disuasión nuclear (RNE, 2022), otro eje central de la estrategia es el fortalecimiento de la resiliencia nacional. Este concepto, ampliamente desarrollado en el documento, se refiere a la capacidad de la nación para resistir y recuperarse de crisis prolongadas. Francia propone construir una «economía de guerra», que permita movilizar recursos industriales y humanos de manera eficiente durante situaciones de emergencia (RNE, 2022).

Además, se enfatiza la importancia de garantizar la ciberresiliencia, desarrollando capacidades avanzadas para mitigar los efectos de ciberataques y proteger infraestructuras críticas en sectores como la energía, el transporte y las comunicaciones (RNE, 2022).

En el ámbito europeo, la RNE subraya la necesidad de reforzar la autonomía estratégica de Europa como una condición indispensable para garantizar la seguridad continental (RNE, 2022). Francia asume un papel de liderazgo en este esfuerzo, promoviendo una cultura estratégica común y la reducción de la dependencia de aliados externos, especialmente en defensa y energía (RNE, 2022).

Esta visión incluye fortalecer las capacidades operativas de la Unión Europea y desarrollar una industria de defensa competitiva, capaz de responder a las necesidades del continente sin depender de suministros externos. A pesar de su enfoque ambicioso, la RNE no está exenta de limitaciones. Uno de los aspectos más criticados es su falta de integración transversal del cambio climático y otros riesgos ambientales en los objetivos estratégicos.

Aunque se reconocen como factores importantes, estos no se abordan de manera integral, lo que refleja una continuidad en enfoques tradicionales centrados en la disuasión militar y la modernización de las Fuerzas Armadas (RNE, 2022). Esta des-

conexión podría limitar la capacidad de Francia para liderar en áreas emergentes, como la sostenibilidad y la justicia climática, que son cada vez más centrales en la seguridad global.

Sin embargo, la autonomía energética emerge como un área donde Francia podría desempeñar un papel crucial, aprovechando su liderazgo en tecnologías nucleares para promover una transición hacia fuentes de energía más sostenibles. Este enfoque no solo fortalecería la resiliencia económica y estratégica del país, sino que también lo posicionaría como un modelo para otros estados europeos en la lucha contra el cambio climático (RNE, 2022).

En conclusión, la Revisión Nacional Estratégica de Francia 2022 refleja un esfuerzo significativo por adaptar la política de seguridad nacional a un mundo en transformación. Al combinar la disuasión nuclear, una reevaluación de la programación militar, la resiliencia económica y el liderazgo europeo, el documento posiciona a Francia como un actor clave en un orden internacional marcado por tensiones crecientes.

3.2 El impacto del cambio climático en Francia

El cambio climático inducido por las actividades humanas ha tenido un impacto profundo en Francia, superando en 2022 la capacidad del país para prevenir y gestionar crisis climáticas. Este año se caracterizó por la intensificación de los efectos climáticos y subrayó la necesidad urgente de reconocer la gravedad de la situación, así como de comprometer los recursos necesarios para fortalecer las acciones de adaptación y descarbonización en Francia, Europa y el ámbito internacional (HCC RANNC, 2023). En este contexto, resulta esencial analizar los principales efectos climáticos que afectaron al país y las respuestas planteadas para afrontarlos.

En primer lugar, es importante destacar que el año 2022 registró condiciones meteorológicas extremas en Francia. Las temperaturas fueron excepcionalmente altas, alcanzando un aumento de +2,9 °C en comparación con el período 1900-1930, según datos de Météo-France. Este incremento, combinado con un déficit de precipitaciones del 25 % respecto al promedio de 1991-2020, provocó una sequía superficial excepcional que afectó a tres cuartas partes del territorio francés entre julio y septiembre.

Estas condiciones adversas no solo afectaron los ecosistemas, sino que también tuvieron consecuencias directas en la agricul-

tura, reduciendo los rendimientos entre un 10 % y un 30 % en algunos sectores y provocando una disminución en la producción de forrajes en un 30 % en comparación con el promedio de cinco años. Además, la generación hidroeléctrica fue un 20 % inferior al promedio de 2015-2019 (HCC RANNC, 2023).

De forma simultánea, el suministro de agua potable se vio gravemente afectado en más de dos mil municipios, de los cuales siete experimentaron interrupciones totales del servicio durante varios días. Esto evidencia las limitaciones del sistema de gestión hídrica, a pesar de las revisiones implementadas en los últimos años (HCC RANNC, 2023).

Además, los incendios forestales alcanzaron niveles alarmantes en 2022, con más de 7800 incidentes registrados y una superficie quemada de 72 000 hectáreas. La capacidad de los recursos nacionales se vio desbordada, lo que requirió el apoyo de medios internacionales.

Asimismo, las olas de calor, cada vez más frecuentes, provocaron 2816 muertes adicionales en verano, contribuyendo a un total de más de 10 500 fallecimientos relacionados con el calor en los últimos ocho años (HCC RANNC, 2023).

En el ámbito sanitario, la expansión del mosquito tigre, portador del dengue, se convirtió en un problema creciente. En 2022, se identificaron 65 casos autóctonos de dengue en nueve focos de transmisión, el mayor brote documentado en Europa. Este mosquito está presente en 72 departamentos franceses, exponiendo a más del 40 % de la población a riesgos relacionados con esta enfermedad (HCC RANNC, 2023).

Por otro lado, a nivel ecológico, la sequía y el calor extremo afectaron la biodiversidad, especialmente en áreas húmedas del litoral atlántico, donde hubo una reducción anómala en la reproducción de aves acuáticas y anfibios (HCC RANNC, 2023).

En términos más amplios, el aumento de la temperatura promedio en Francia (+1,9 °C durante 2013-2022) supera el promedio global (+1,15 °C), lo que subraya la particular vulnerabilidad del país a los efectos del cambio climático (HCC RANNC, 2023). De hecho, las proyecciones climáticas indican que para 2030 Francia enfrentará un calentamiento cercano a los 2,0 °C, con extremos que podrían alcanzar los 3,0 °C en años particularmente cálidos, como 2022. Sin embargo, las previsiones a largo plazo son aún más preocupantes: si no se intensifican las políticas globales de

mitigación, el calentamiento promedio en Francia podría alcanzar los 4,0 °C para finales del siglo XXI (HCC RANNC, 2023).

Sin embargo, a pesar de los avances en la planificación estratégica, la implementación de medidas concretas sigue siendo insuficiente. Los planes existentes a menudo carecen de mecanismos de seguimiento y evaluación adecuados, lo que dificulta garantizar el logro de los objetivos climáticos (HCC RANNC, 2023).

Por otro lado, las políticas económicas relacionadas con el cambio climático demandan una transformación significativa. En 2022, los gastos desfavorables para el clima aumentaron considerablemente debido al «escudo tarifario», que representó ochenta mil millones de euros en gasto público acumulado entre 2021 y 2023. Este tipo de medidas pone de manifiesto el insuficiente apoyo para la transición energética y la reducción de emisiones (HCC RANNC, 2023).

A nivel legislativo, la Ley de Planificación Energética y Climática (LPEC), revisada cada cinco años, representa una oportunidad clave para alinear los objetivos nacionales con los compromisos europeos e internacionales. Sin embargo, su implementación depende de la rápida adopción de la Estrategia Francesa de Energía y Clima (SFEC), que debe incluir metas específicas para reducir las emisiones de metano y fomentar la acción climática en todos los sectores y regiones (HCC RANNC, 2023).

Asimismo, la creación de la Secretaría General de Planificación Ecológica (SGPE) en 2022 marcó un avance significativo en la coordinación de las políticas climáticas del Gobierno. No obstante, su efectividad dependerá de los recursos asignados y de su capacidad para articularse con otros proyectos gubernamentales (HCC RANNC, 2023).

En el ámbito internacional, las negociaciones climáticas siguen enfrentando desafíos importantes. Aunque la COP27 avanzó en la creación de un fondo para pérdidas y daños a petición de los países en desarrollo, no logró fortalecer los compromisos de reducción de emisiones. Este estancamiento resalta la necesidad de liderazgo político para revitalizar el impulso global hacia la COP28 (HCC RANNC, 2023).

Por su parte, el paquete «Fit for 55» de la Unión Europea ofrece un marco regulatorio sólido para reducir las emisiones netas en un 55 % para 2030. Sin embargo, la implementación de estas políticas en los Estados miembros, incluido Francia, enfrenta

retos significativos, lo que pone en riesgo el cumplimiento de los objetivos a largo plazo (HCC RANNC, 2023).

En conclusión, el cambio climático representa una amenaza multifacética para Francia, afectando su biodiversidad, economía, infraestructura y salud pública. Para abordar estos desafíos, es imprescindible adoptar un enfoque transformador que integre conocimientos científicos, fortalezca las políticas económicas y amplíe la cooperación internacional. Solo mediante una acción coordinada y ambiciosa será posible garantizar la resiliencia de Francia frente a un futuro climático cada vez más incierto (HCC RANNC, 2023).

3.3 Alineación con las teorías contemporáneas de Simon Dalby el paradigma del Antropoceno

La RNE mantiene un enfoque prioritariamente tradicional de seguridad, aun cuando las evidencias del impacto climático en el territorio francés son claras y alarmantes. A pesar de los desafíos concretos que el cambio climático está generando en Francia; sequías severas, incendios forestales recurrentes, olas de calor extremas y pérdida de biodiversidad, el documento no refleja un alineamiento con el paradigma de seguridad propuesto en el contexto del Antropoceno por Simon Dalby.

Francia enfrentó en 2022 fenómenos extremos relacionados con el cambio climático que han tenido impactos profundos en su economía, sociedad y medio ambiente. Las temperaturas alcanzaron niveles récord, con un aumento de +2,9 °C respecto al periodo de referencia (1900-1930), acompañadas por una sequía superficial que afectó a más del 75 % del territorio nacional. Además, la reducción de precipitaciones y los incendios forestales devastaron sectores clave como la agricultura y la generación hidroeléctrica, lo que expuso la vulnerabilidad del sistema hídrico y energético del país (HCC RANNC, 2023).

A pesar de estas evidencias, que sitúan al cambio climático como una amenaza inmediata y profunda para la estabilidad del país, la RNE no integra este fenómeno como un eje estructural de su estrategia de seguridad. El tratamiento del cambio climático se limita a medidas reactivas y técnicas, como la mejora de la resiliencia interna, sin abordar sus implicaciones sistémicas (HCC RANNC, 2023).

El contenido de la RNE se alinea principalmente con el paradigma clásico de seguridad, donde el Estado y la defensa militar son el centro de atención. Las principales amenazas identificadas incluyen la invasión rusa de Ucrania, las tensiones geopolíticas con potencias como China y el uso de herramientas híbridas como ciberataques (RNE, 2022). Estas prioridades reflejan una continuidad con las teorías tradicionales de seguridad, como las formuladas por Kenneth Waltz y John Herz, que enfocan sus esfuerzos en el equilibrio de poder y la disuasión militar.

En este contexto, la disuasión nuclear ocupa un lugar destacado como elemento esencial de la autonomía estratégica de Francia. El mantenimiento y modernización de su arsenal nuclear subrayan la importancia que se le otorga a esta herramienta como garantía frente a amenazas interestatales (RNE, 2022). Sin embargo, este énfasis refuerza la percepción de que la estrategia francesa sigue orientada hacia respuestas tradicionales, ignorando las amenazas sistémicas como el cambio climático (COLUCCI EUFEMIA, 2022).

El enfoque estratégico francés permanece anclado en este marco de estado, donde las soluciones al cambio climático se ven como parte de políticas ambientales o económicas, pero no como cuestiones centrales de seguridad. Este posicionamiento contrasta marcadamente con el paradigma del Antropoceno, que identifica el cambio climático y las alteraciones ecológicas como amenazas existenciales que reconfiguran el concepto de seguridad.

A pesar de que Francia experimenta una crisis climática tangible, como la sequía que en 2022 afectó el suministro de agua potable en más de dos mil municipios y los incendios forestales que quemaron 72 000 hectáreas, la estrategia nacional no aborda el cambio climático desde una perspectiva transformadora. (HCC RANNC, 2023). Francia parece abordar estas crisis como eventos aislados, más que como manifestaciones de una nueva realidad sistémica que redefine el panorama de amenazas y requiere un replanteamiento estratégico.

El paradigma de seguridad del Antropoceno, según Dalby, implica reconocer que las amenazas climáticas y ecológicas son inseparables de la seguridad nacional e internacional. Sin embargo, en la RNE no se encuentra esta integración. Por ejemplo, aunque menciona el impacto de las tensiones climáticas, estas no se traducen en acciones concretas para mitigar el problema globalmente ni para liderar un cambio estructural hacia la descarbonización.

En conclusión, Francia, a pesar de estar profundamente afectada por el cambio climático (HCC RANNC, 2023), mantiene un enfoque de seguridad centrado en amenazas tradicionales, priorizando la defensa militar y las rivalidades interestatales (RNE, 2022). La disuasión nuclear, aunque relevante en un contexto de tensiones geopolíticas, demuestra la dependencia de un paradigma de seguridad estatalista clásico, que ignora las amenazas sistémicas del cambio climático. Esto muestra una desconexión entre las realidades del Antropoceno y su estrategia de seguridad, evidenciando que el país no adopta el paradigma propuesto por Simon Dalby.

La ausencia de un enfoque sistémico que vincule el cambio climático con la seguridad nacional refuerza que la estrategia francesa sigue siendo esencialmente clásica, ignorando los desafíos de un mundo en transformación.

4 Convergencias y divergencias

El análisis de las convergencias y divergencias entre la Estrategia de Seguridad Nacional 2021 de España y la Revisión Nacional Estratégica 2022 de Francia permite comprender cómo cada país responde a un contexto global y cómo adaptan sus políticas de seguridad para enfrentar los desafíos contemporáneos. Este enfoque comparativo no solo destaca las similitudes en sus percepciones de las amenazas globales, sino que también pone de manifiesto sus diferencias fundamentales.

En primer lugar, se identificarán las convergencias entre ambas estrategias, como su reconocimiento compartido del impacto de las amenazas híbridas, la importancia de la resiliencia nacional y la necesidad de reforzar la autonomía estratégica europea. Ambas coinciden también en considerar el cambio climático como un multiplicador de riesgos, aunque cada una lo aborda con distinta intensidad, reconociendo su capacidad para agravar vulnerabilidades preexistentes y desencadenar crisis sistémicas. Estas similitudes surgen en un contexto marcado por la competencia entre grandes potencias y tensiones geopolíticas crecientes.

En segundo lugar, se analizarán las divergencias, que revelan enfoques distintos en áreas fundamentales como la priorización del cambio climático, la disuasión nuclear, las prioridades regionales y globales, la modernización militar y la capacidad operativa, así como la integración de objetivos de desarrollo sostenible en sus estrategias de seguridad.

Estas diferencias evidencian no solo las tradiciones históricas y políticas específicas de cada país, sino también sus distintas proyecciones estratégicas en el ámbito internacional, incluyendo las prioridades geográficas diferenciadas: mientras España se enfoca en el Magreb y África Subsahariana debido a su proximidad y los riesgos asociados al cambio climático y la migración, Francia prioriza el Indo-Pacífico y Europa del Este, alineándose con su papel de potencia global y sus intereses geopolíticos en estas regiones.

Este análisis y la tabla comparativa permitirán extraer conclusiones relevantes sobre cómo las estrategias de seguridad nacional de España y Francia abordan los retos del siglo XXI, evaluando tanto los puntos de encuentro como las discrepancias que marcan su posicionamiento frente a un orden mundial en constante evolución.

4.1 Convergencias entre la ESN 2021 y la RNE 2022

4.1.1 Adaptación a un contexto de inestabilidad geopolítica global

Ambas estrategias coinciden en que el escenario internacional actual está marcado por la fractura del orden mundial. Tanto España (ESN 2021) como Francia (RNE, 2022) reconocen la intensificación de rivalidades entre grandes potencias (China, Rusia y EE. UU.) y el retorno de conflictos interestatales de alta intensidad.

Por ejemplo, la invasión de Ucrania en 2022 se convierte en un punto de inflexión para Francia, marcando un cambio importante en su estrategia de seguridad (RNE, 2022). En el caso de España, su Estrategia de Seguridad Nacional fue publicada en 2021, antes de que comenzara la guerra en Ucrania, lo que explica que no haga énfasis en este conflicto, aunque ya se identificaba la competencia geopolítica (RNE, 2022).

4.1.2 Amenazas híbridas y desinformación

Las dos estrategias destacan el impacto creciente de las amenazas híbridas, que incluyen ciberataques, campañas de desinformación y el uso estratégico de recursos críticos (RNE, 2022). Francia subraya cómo estas tácticas buscan debilitar a las democracias modernas, mientras que España incorpora la desinformación por primera vez como un desafío específico y transversal (ESN 2021).

4.1.3 Importancia de la resiliencia nacional

España y Francia consideran la resiliencia un pilar estratégico fundamental. La ESN 2021 define la resiliencia nacional como la capacidad del conjunto de la sociedad para resistir, recuperarse y transformarse frente a crisis y amenazas de diversa índole (ESN 2021).

Desde esta perspectiva, propone fortalecer la resiliencia ante crisis mediante la detección temprana y la gestión eficiente de emergencias (ESN 2021). Por su parte, la RNE 2022 introduce el concepto de «economía de guerra» (RNE, 2022), orientado a movilizar recursos industriales y humanos en situaciones críticas.

4.1.4 Cambio climático como multiplicador de riesgos

Aunque con distinta intensidad, ambas estrategias reconocen el papel desestabilizador del cambio climático. En la ESN 2021, el cambio climático ocupa un lugar central y se aborda como una amenaza transversal con impactos directos en la seguridad energética, las crisis humanitarias y los conflictos (ESN 2021). Francia, aunque menciona el cambio climático, lo considera un multiplicador de tensiones que incrementan vulnerabilidades existentes, como la escasez de recursos hídricos o la migración (RNE, 2022).

4.1.5 Reforzar la autonomía estratégica europea

España y Francia coinciden en la necesidad de fortalecer la autonomía estratégica de Europa. Francia, como potencia de equilibrio, lidera esta iniciativa promoviendo la reducción de la dependencia de aliados externos, especialmente en materia de defensa y energía (RNE, 2022). España también respalda esta idea, alineándola con su interés en reforzar las políticas de la UE y colaborar con socios clave como la OTAN (ESN 2021).

4.2 Divergencias entre la ESN 2021 y la RNE 2022

4.2.1 Enfoque prioritario en el cambio climático

La diferencia más significativa radica en la priorización del cambio climático. La ESN 2021 sitúa el cambio climático como un pilar central, vinculándolo con la transición ecológica, la seguridad

energética y la resiliencia global (ESN 2021). España entiende que este fenómeno no solo es ambiental, sino que actúa como multiplicador de amenazas, especialmente en regiones como el el Magreb, Sahel y África Occidental (ESN 2021).

En contraste, la RNE 2022 reconoce el impacto del cambio climático, pero lo aborda de manera secundaria. Se menciona como un factor agravante de conflictos y tensiones, pero no se integra de manera transversal en los ejes estratégicos del documento. La RNE continúa priorizando la disuasión militar, la modernización de capacidades defensivas y la soberanía nacional (RNE, 2022).

4.2.2 Énfasis en la disuasión nuclear

Francia sitúa la disuasión nuclear como la piedra angular de su estrategia de defensa, considerándola esencial para proteger sus intereses vitales y garantizar su autonomía estratégica (RNE, 2022).

En la ESN 2021, este tipo de capacidades no se mencionan, ya que la estrategia española se enfoca en amenazas híbridas (ESN 2021) y en la cooperación internacional para resolver desafíos emergentes (ESN 2021).

4.2.3 Prioridades regionales y globales

España pone un énfasis considerable en regiones clave como el Magreb, el Sahel y el África Subsahariana (ESN 2021), donde el cambio climático y la fragilidad estructural generan inestabilidad con consecuencias directas en la seguridad europea.

En cambio, Francia adopta una visión más global y estratégica, centrándose en desafíos en el Indo-Pacífico, la competencia con China y las tensiones derivadas del conflicto en Europa del Este (RNE, 2022).

4.2.4 Modernización militar y capacidad operativa

La RNE 2022 otorga un peso importante a la modernización de las Fuerzas Armadas y al desarrollo de nuevas capacidades tecnológicas, como armas hipersónicas, ciberdefensa y protección de infraestructuras críticas (RNE, 2022).

Aunque la ESN 2021 menciona la necesidad de fortalecer capacidades tecnológicas y estratégicas, el enfoque de España se cen-

tra más en la resiliencia civil y la seguridad multidimensional, sin priorizar grandes capacidades militares (ESN 2021).

4.2.5 Visión del desarrollo sostenible y la Agenda 2030

La ESN 2021 integra de forma activa los objetivos de la Agenda 2030, especialmente en sus Líneas de Acción 32 y 33, donde se promueve la cooperación internacional para fortalecer la resiliencia de los países más vulnerables al cambio climático (ESN 2021).

Francia, aunque menciona su papel en la sostenibilidad, no desarrolla estos compromisos como un eje central, reflejando una continuidad en su enfoque más tradicional de seguridad (RNE, 2022).

4.3 Una visión contrapuesta de la seguridad nacional

La Estrategia de Seguridad Nacional de España (2021) y la Revisión Nacional Estratégica de Francia (2022) muestran enfoques diferenciados respecto a los retos globales.

Mientras que España coloca el cambio climático, la transición ecológica y la resiliencia multidimensional en el centro de su estrategia, Francia prioriza la disuasión militar, la modernización tecnológica y la autonomía estratégica como herramientas clave frente a un escenario geopolítico cada vez más volátil.

Estas diferencias reflejan las prioridades e identidades estratégicas de ambos países. España, como actor europeo enfocado en su entorno inmediato, adopta un enfoque más sostenible y preventivo ante amenazas emergentes como el cambio climático. Francia, en su papel de potencia global, combina su liderazgo europeo con una apuesta por el poder militar y tecnológico, manteniendo su estatus en un orden internacional en transformación.

En definitiva, aunque ambas estrategias comparten ciertos elementos, como la necesidad de reforzar la autonomía estratégica europea y abordar las amenazas híbridas, divergen en sus prioridades estructurales y en la integración del cambio climático como eje central o secundario de la seguridad nacional. Estas diferencias, sin embargo, reflejan las realidades estratégicas, políticas y geográficas propias de cada país.

El análisis de la Estrategia de Seguridad Nacional de España (2021) y la Revisión Nacional Estratégica de Francia (2022)

demuestra cómo cada estrategia ha estado influenciada por el contexto en el que fue elaborada: la crisis del COVID-19 en el caso español y la guerra de Ucrania en el francés. Esto sugiere que futuras estrategias nacionales seguirán reflejando los acontecimientos geopolíticos y las crisis que marquen cada momento.

Una cuestión clave es si estas estrategias continuarán basándose en el enfoque clásico de seguridad, centrado en la disuasión y la defensa militar o si evolucionarán hacia un modelo más integrador, que incorpore con mayor énfasis desafíos como el cambio climático, la resiliencia y la seguridad multidimensional.

5 Conclusiones

El análisis comparado de la Estrategia de Seguridad Nacional de España (2021) y la Revisión Nacional Estratégica de Francia (2022) evidencia que ambas incorporan, en distinta medida, los desafíos característicos del Antropoceno, esto es, los riesgos globales derivados del impacto humano sobre el planeta, aunque lo hacen con alcances, prioridades y niveles de integración claramente divergentes. En términos generales, las dos estrategias reconocen la dimensión ambiental como un factor con potencial desestabilizador, pero difieren de forma sustantiva en la centralidad que le otorgan y en su traducción estratégica.

En el caso español, la ESN 2021 integra de manera explícita el cambio climático y las amenazas ecológicas como elementos estructurales de su visión de seguridad. El documento no se limita a describir el clima como un problema ambiental, sino que lo conceptualiza como un multiplicador de riesgos capaz de intensificar fenómenos ya presentes en el entorno estratégico: conflictividad, migraciones, inseguridad alimentaria, tensiones sociales o degradación de la estabilidad regional. Este enfoque supone una ampliación del concepto de seguridad, más coherente con la complejidad sistémica del Antropoceno, y se acompaña de una orientación preventiva que incorpora referencias y compromisos vinculados a la sostenibilidad y al desarrollo, como la Agenda 2030 o el cumplimiento de los Acuerdos de París.

Frente a ello, la RNE 2022 de Francia reconoce el cambio climático y la degradación ambiental, pero lo hace de un modo más lateral y condicionado. La referencia aparece principalmente como un factor que puede agravar crisis o tensiones, sin que alcance un papel vertebrador dentro de la planificación de defensa. En

consecuencia, el componente ecológico queda subordinado a un marco de seguridad de corte más tradicional, donde predominan la disuasión, la protección de la soberanía, la preparación militar y la lógica de competición entre potencias. La estrategia francesa, aunque consciente de los nuevos retos, no reordena sus prioridades estratégicas en torno a ellos.

Este contraste permite afirmar que España muestra una aproximación más cercana a la reconceptualización de la seguridad propia del paradigma del Antropoceno desarrollado por Simon Dalby, centrado en la sostenibilidad ecológica, la resiliencia y la gestión de amenazas globales de carácter sistémico. La ESN 2021 refleja, al menos en el plano doctrinal, una comprensión de la interdependencia entre seguridad humana, estabilidad política y salud del planeta, e incorpora medidas preventivas y cooperativas; transición energética, reducción de vulnerabilidades, preparación ante desastres y cooperación internacional, que se alinean con esa lógica. Francia, en cambio, se mantiene mayoritariamente anclada en un entendimiento estatal-clásico de la seguridad, en el que los riesgos ecológicos no alcanzan el estatus de amenaza estructural ni desplazan el peso de las prioridades tradicionales.

Desde una perspectiva crítica y orientada al futuro, la diferencia más relevante no reside únicamente en el reconocimiento retórico de la amenaza climática, sino en la capacidad real de transformar esa conciencia en arquitectura estratégica e instrumentos sostenidos de política pública. España ha dado un paso significativo al situar el cambio climático dentro del núcleo de la seguridad nacional, pero el valor de esa evolución dependerá de la implementación: transversalización efectiva del enfoque ecológico en los sectores de defensa, protección civil, inteligencia y diplomacia preventiva; dotación estable de recursos; coordinación interministerial y continuidad política en el largo plazo. El principal desafío español no es conceptual, sino de ejecución: convertir el enfoque ampliado en capacidades, procedimientos y prioridades operativas comparables, en rigor y consistencia, a las que tradicionalmente se han dedicado a amenazas militares.

Francia, por su parte, presenta una menor disposición a reconfigurar su paradigma estratégico. La primacía de la disuasión y la lógica de soberanía, junto con una lectura más convencional del entorno internacional, puede limitar la anticipación de amenazas características del Antropoceno que no se manifiestan como agresiones directas, pero que desestabilizan regiones enteras y generan efectos estratégicos indirectos con impacto euro-

peo. Confiar en que los instrumentos clásicos absorberán estas presiones o permitirán responder de forma reactiva entraña un riesgo: en un contexto de cambios ambientales abruptos, basar la seguridad casi exclusivamente en Fuerzas Armadas, alianzas y herramientas tradicionales puede dejar flancos abiertos en términos de resiliencia social, estabilidad regional y gestión de crisis complejas.

En suma, el estudio pone de relieve un panorama dispar entre dos países europeos ante un cambio de época en materia de seguridad. España evidencia una mayor receptividad a una seguridad ampliada y ecológicamente informada, mientras que Francia mantiene una orientación más conservadora y continuista. La adaptación plena al paradigma del Antropoceno dependerá, en ambos casos, de su capacidad para actualizar prioridades estratégicas en los próximos años conforme se intensifiquen las crisis ambientales globales.

Finalmente, cabe subrayar que la seguridad en el Antropoceno exige una reconceptualización que trasciende el marco nacional. Los Estados deberán complementar sus instrumentos tradicionales; disuasión, fronteras, preparación militar, con estrategias orientadas a la sostenibilidad planetaria, la reducción de riesgos sistémicos y la cooperación multilateral. Solo mediante esta adaptación estructural, tal como plantea Dalby, será posible avanzar hacia una seguridad duradera, compartida y coherente con la nueva realidad ecológica que define el siglo XXI.

Bibliografía

Angus, I. (2020a). ¿Cuándo comenzó el Antropoceno... y por qué es importante? [en línea]. La Alianza Global Jus Semper. [Consulta: 2026]. Disponible en: https://jussemper.org/Inicio/Recursos/Info.%20econ/Resources/IanAngus-CuandoComenzoAntropoceno.pdf

—. (2020b). Enfrentando el Antropoceno

Una actualización [en línea]. La Alianza Global Jus Semper. [Consulta: 2026]. Disponible en: https://jussemper.org/Inicio/Recursos/Info.%20econ/Resources/IanAngus-EnfrentandoAlAntropoceno.pdf

Briggs, C. M. (2017). Foresight tools & early warning systems: Vulnerability assessments for abrupt and non-linear climate risks. En: Werrell, C. E. y Femia, F. (eds.). *Epicenters of Cli-*

mate and Security: The New Geostrategic Landscape of the Anthropocene.

Calatrava, A. (2022). La transformación del sistema de seguridad europeo tras la Guerra Fría: de 1991 a la crisis de Ucrania. *Historia Actual Online*. N.º 59, pp. 155-170. DOI: 10.36132/hao.v3i59.2293

Calduch Cervera, R. (2014). Métodos y técnicas de investigación internacional. 2.ª ed. Madrid, Universidad Complutense de Madrid (UCM).

—. (2021). *Curso de métodos y técnicas de investigación*. Universidad Complutense de Madrid.

Callahan, C. W. y Mankin, J. S. (2022). National attribution of historical climate damages. *Climatic Change*. 172(3). DOI: 10.1007/s10584-022-03387-y

Castañeda, M. G. y Merino, S. K. (2015). Evolución y condicionantes de las nociones de seguridad y defensa [en línea]. En: Tema de Investigación Central de la Academia. Academia de Guerra Ejército de Chile, CEE, pp. 25-44. [Consulta: 2026]. Disponible en: https://publicacionesacague.cl

Colucci, E. (2022). Proteger a Europa: la estrategia de defensa de Francia en medio del creciente crecimiento de la industria europea y de su preparación para la defensa [en línea]. Centro de Estudio Grl Mosconi. [Consulta: 2026]. Disponible en: https://www.fie.undef.edu.ar/ceptm/?p=14807

Dalby, S. (2016). Geopolitics in the Anthropocene [en línea]. Draft paper for presentation to the "Return of Geopolitics" conference. Tucson, Arizona. [Consulta: 2026]. Disponible en: http://www.geopoliticsconference.org/

—. (2023a). La destrucción asegurada: la potencia de fuego, el cambio climático y los dilemas de seguridad. *Geopolítica(s)*. 14(1), pp. 15-26. DOI: 10.5209/geop.88813

—. (2023b). Una nueva geopolítica para el Antropoceno. *La Alianza Global Jus Semper*.

Departamento de Seguridad Nacional (DSN). (2021). Estrategia de Seguridad Nacional 2021 [en línea]. DSN, Presidencia del Gobierno. [Consulta: 2026]. Disponible en: https://www.dsn.gob.es/sites/default/files/documents/ESN2021%20Accesible_1.pdf

—. (2023). *Informe Anual de Seguridad Nacional 2023*. DSN. [Consulta: 2026]. Disponible en: https://www.dsn.gob.es/es/publicaciones/informes-anuales/IASN2023

Haut Conseil pour le Climat (HCC). (2023). Rapport annuel 2023: «Acter l'urgence, engager les moyens» [en línea]. HCC. [Consulta: 2026]. Disponible en: https://www.hautconseilclimat.fr/publications/rapport-annuel-2023-acter-lurgence-engager-les-moyens/

Herz, J. H. (1950). Idealist internationalism and the security dilemma. *World Politics*. 2(2), pp. 157-180. DOI: 10.2307/2009187

Issberner, L. R. y Léna, P. (2023). Antropoceno: la problemática vital de un debate científico [en línea]. UNESCO Courier. [Consulta: 2026]. Disponible en: https://courier.unesco.org/es/articles/antropoceno-la-problematica-vital-de-un-debate-cientifico

Kuhn, T. (1962). *La estructura de las revoluciones científicas*.

Marsh, D. y Stoker, G. (2010). *Theory and Methods in Political Science*. 3.ª ed. Palgrave Macmillan.

McCreary, T. (2019). Human Planet: How We Created the Anthropocene by Simon L. Lewis and Mark A. Maslin [en línea]. The New Zealand Geographer. [Consulta: 2026]. Disponible en: https://www.academia.edu/40143054/Human_Planet_How_We_Created_the_Anthropocene_by_Simon_L_Lewis_and_Mark_A_Maslin

Mourad, B. y Luers, A. (2017). Tools for understanding systemic risks like climate change. En: Werrell, C. E. y Femia, F. (eds.). *Epicenters of Climate and Security: The New Geostrategic Landscape of the Anthropocene*.

Moure, L. (2009). La teoría de la política internacional treinta años después en línea]. Revista Electrónica de Estudios Internacionales. [Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3033204.pdf

Pyne, S. J. (2019). Welcome to the Pyrocene [en línea]. *Natural History*. [Consulta: 2026]. Disponible en: https://www.infobae.com/cultura/2025/01/30/the-pyrocene-una-historia-del-fuego-y-por-que-es-necesario-replantear-nuestra-relacion-con-las-llamas/

République Française. (2022). Revue nationale stratégique 2022 [en línea]. République Française. [Consulta: 2026]. Disponible en: https://www.sgdsn.gouv.fr/files/files/Revue%20nationale%20strat%C3%A9gique%20-%20Espagnol.pdf

Sampieri, R. H., Collado, C. F. y Baptista, M. P. L. (2014). *Metodología de la investigación*. 6.ª ed. McGraw-Hill.

Terradas, N. (2009). El dilema de seguridad y su importancia para el estudio de las relaciones internacionales [en línea]. Letras Internacionales. 88(3). [Consulta: 2026]. Disponible en: https://revistas.ort.edu.uy/letras-internacionales/article/view/1627

United Nations. (2022). 2022 Special Report on Human Security [en línea]. Human Development Reports. [Consulta: 2026]. Disponible en: https://hdr.undp.org/content/2022-special-report-human-security

University of Victoria (UVic). (2025). Simon Dalby – Senior Research Fellow [en línea]. [Consulta: 2026]. Disponible en: https://www.uvic.ca/research/centres/globalstudies/people/fellows/dalbysimon.php

Waltz, K. N. (1959). *Man, the state, and war: A theoretical analysis*. Columbia University Press.

—. (1979). *Theory of international politics*. Addison-Wesley.

—. (1988). The origins of war in neorealist theory. *Journal of Interdisciplinary History*. 18(4), pp. 615-628.

—. (2000). Structural realism after the Cold War. *International Security*. 25(1), pp. 5-41.

Vimeo. (2023). Welcome to the Anthropocene [vídeo]. [Consulta: 2026]. Disponible en: https://player.vimeo.com/video/39048998

Werrell, C. E. y Femia, F. (2017). *Epicenters of Climate and Security: The New Geostrategic Landscape of the Anthropocene*. The Center for Climate and Security.

Werrell, C. E. *et al*. (2017). *A responsibility to prepare: governing in an age of unprecedented risk and unprecedented foresight*. Global Policy.

Capítulo quinto

La polarización social en EE. UU. durante el siglo XXI y su repercusión geopolítica sobre el vínculo transatlántico

Miguel Requeno Soler

Resumen

Este trabajo analiza cómo la polarización ideológica en Estados Unidos, aun siendo un fenómeno interno, puede repercutir en el vínculo transatlántico al introducir dudas sobre la continuidad del compromiso estadounidense con sus aliados europeos. A lo largo del siglo XXI, la política exterior de Washington ha mostrado oscilaciones que no siempre responden solo al entorno internacional: también influyen los costes internos, el bloqueo político y la disputa partidista, que pueden convertir la acción exterior en un terreno de confrontación y dificultar líneas estables entre administraciones.

Desde la perspectiva europea, lo decisivo no es únicamente lo que EE. UU. hace en un momento concreto, sino qué expectativas razonables puede mantener la Unión Europea a medio plazo sobre su fiabilidad como garante de seguridad. En ese contexto, la autonomía estratégica aparece aquí no como una ruptura con la OTAN, sino como una adaptación gradual: un intento de reducir vulnerabilidades y ampliar márgenes de acción ante escenarios en los que el respaldo estadounidense pueda volverse más condicionado o menos previsible. La conclusión es deliberadamente

prudente: la polarización no explica por sí sola la evolución del vínculo, pero puede amplificar la incertidumbre que empuja a Europa a reforzar capacidades propias.

Palabras clave

OTAN, Estados Unidos, Unión Europea, Polarización ideológica, Autonomía estratégica.

Social Polarization in the United States in the 21st Century and Its Geopolitical Impact on the Transatlantic Relationship

Abstract

This study examines how ideological polarization in the United States, while primarily a domestic phenomenon, can reverberate across the transatlantic relationship by raising doubts about the continuity of the U.S. commitment to its European allies. Throughout the twenty-first century, Washington's foreign policy has displayed shifts that cannot be explained solely by the international environment: domestic political costs, legislative gridlock, and partisan conflict also shape external action, turning foreign policy into a field of confrontation and making it harder to sustain stable lines of policy across administrations.

From a European perspective, what matters is not only what the United States does at a given moment, but what reasonable expectations the European Union can hold over the medium-term regarding Washington's reliability as a security guarantor. In that context, strategic autonomy is framed here not as a rupture with NATO, but as a gradual adaptation: an effort to reduce vulnerabilities and widen room for manoeuvre in scenarios where U.S. support may become more conditional or less predictable. The conclusion is deliberately cautious: polarization does not by itself determine the evolution of the transatlantic bond, but it can amplify uncertainty in ways that push Europe to strengthen its own capabilities.

Key words

NATO, United States, European Union, Ideological polarization, Strategic autonomy.

1 Introducción

En mayo de 2017, durante la cumbre de la OTAN en Bruselas, el entonces presidente de EE. UU., Donald Trump, evitó reafirmar explícitamente el Artículo 5 y centró su intervención en reprochar a varios aliados que no asumían suficiente gasto en defensa (Trump, 2017). En Europa, esa señal fue percibida como un síntoma de mayor condicionalidad política del compromiso estadounidense: poco después, la canciller alemana Angela Merkel afirmó que «Europa debe tomar su destino en sus propias manos» (Merkel, 2017).

Ese punto de partida permite formular el problema que recorre este capítulo: hasta qué punto las tensiones domésticas de una gran potencia se reflejan en su política exterior, y cómo se reacomoda Europa cuando el socio principal proyecta señales menos estables. En estas páginas, la polarización se entiende en sentido político-social: el aumento de la distancia y la desconfianza entre identidades políticas, con efectos sobre la capacidad de sostener consensos y orientaciones duraderas. Aunque es un fenómeno interno, su persistencia puede dificultar la coherencia estratégica y la previsibilidad ante aliados y rivales. En ese contexto, la autonomía estratégica europea se plantea como una respuesta gradual orientada a reducir vulnerabilidades ante escenarios de mayor incertidumbre, más que como una alternativa a la OTAN o un giro de ruptura (Friedrichs y Tama, 2022; Borg, 2024). El significado del concepto y sus implicaciones se desarrollan con más detalle en el apartado teórico.

1.1 Delimitación y justificación de la investigación

Desde el inicio del siglo xxi, el sistema internacional ha atravesado transformaciones profundas que han puesto a prueba la cohesión de las alianzas tradicionales. En ese contexto, el vínculo transatlántico entre Estados Unidos y Europa —sostenido históricamente por valores compartidos, intereses estratégicos y estructuras institucionales como la OTAN— ha experimentado tensiones crecientes. Parte de esas fricciones se explican por desafíos externos (cambios en el equilibrio de poder, guerras, crisis económicas, presión rusa, impacto global de la pandemia), pero también por dinámicas internas estadounidenses que afectan a la consistencia del liderazgo y a la continuidad de sus compromisos.

Una de esas dinámicas es el aumento sostenido de la polarización social en Estados Unidos. Aunque suele analizarse como un fenómeno doméstico, su intensidad puede tener efectos que traspasan fronteras: condiciona el margen de maniobra del Ejecutivo, complica la estabilidad de las coaliciones políticas y eleva el coste interno de determinadas decisiones estratégicas. En términos prácticos, esto puede traducirse en señales de menor previsibilidad, cambios abruptos de prioridades entre administraciones y disputas internas que se proyectan hacia el exterior.

Este trabajo se centra en esa zona de contacto entre lo interno y lo externo: cómo la polarización social en Estados Unidos puede haber condicionado decisiones estratégicas que afectan al espacio euroatlántico y, con ello, a la estabilidad, continuidad y credibilidad del vínculo transatlántico. La delimitación es importante por dos motivos. Primero, porque se acota la polarización como fenómeno político-social, evitando convertir el análisis en una explicación total que lo atribuya todo a una sola causa. Segundo, porque el foco se fija en la relación con Europa y en el ámbito euroatlántico; cuando se alude a otras regiones, se hace como marco de contexto para entender prioridades, desplazamientos de atención y tensiones de recursos de la política exterior estadounidense, no como objeto central del trabajo.

El interés del tema es doble. En el plano académico, existe literatura sobre los efectos de la polarización en el funcionamiento institucional estadounidense y, paralelamente, sobre la transformación del vínculo transatlántico; sin embargo, son menos frecuentes los estudios que conectan de forma sistemática ambas dimensiones y se preguntan si hay una relación significativa entre ellas. En el plano estratégico, la evolución reciente de la Unión Europea en defensa y seguridad —con iniciativas orientadas a ampliar su autonomía estratégica— invita a considerar si parte de ese impulso responde a una percepción de incertidumbre sobre el compromiso estadounidense. El argumento que se explora aquí es prudente: la polarización podría operar como un factor que incrementa la incertidumbre sobre la continuidad estratégica, y esa incertidumbre podría haber influido en la consolidación de aspiraciones europeas de mayor autonomía.

El marco temporal 2001-2024 permite observar, a lo largo de distintas administraciones, tanto la trayectoria ascendente de la polarización como una secuencia de hitos que han exigido coordinación transatlántica: el 11-S y las guerras en Afganistán e Irak; la crisis financiera global; la anexión de Crimea; el auge de movimientos populistas; la pandemia de COVID-19 y la invasión rusa de Ucrania en 2022. Cada uno de estos episodios ha tensionado, de manera

distinta, el reparto de cargas, las prioridades y el discurso del compromiso mutuo. En conjunto, ofrecen una base temporal amplia para examinar si tensiones internas de la principal potencia occidental han repercutido en su papel como garante —o, al menos, como pilar— de la seguridad euroatlántica.

1.2 Eje del análisis y alcance de la discusión

El hilo conductor de la obra es sencillo de enunciar, aunque complejo de desplegar: si la polarización social se intensifica, ¿qué ocurre con la capacidad de Estados Unidos para sostener políticas exteriores estables hacia Europa, y cómo se interpreta esa evolución desde el lado europeo? Esta cuestión se sitúa en un terreno donde importan tanto las decisiones materiales (presupuestos, despliegues, acuerdos, prioridades estratégicas) como la dimensión perceptiva (credibilidad, confianza, previsibilidad).

A lo largo del trabajo, la atención se distribuye en dos planos complementarios. Por un lado, el plano doméstico estadounidense: la polarización puede traducirse en bloqueo legislativo, confrontación permanente, incentivos a políticas simbólicas y oscilaciones en la orientación estratégica, especialmente cuando la política exterior se convierte en un campo de disputa interna. Por otro, el plano europeo: las instituciones y gobiernos europeos no solo reaccionan a hechos, sino también a expectativas sobre el futuro del compromiso estadounidense, particularmente en momentos de cambio de administración, crisis internacionales o rupturas discursivas con el orden multilateral.

Este enfoque permite tratar la autonomía estratégica europea no como un «acto de divorcio» inevitable, sino como una respuesta gradual a un entorno percibido como más incierto. Si se erosiona la expectativa de continuidad resulta razonable que los aliados busquen reducir vulnerabilidades mediante capacidades propias, mecanismos institucionales o instrumentos de coordinación que complementen, o amortigüen, las fluctuaciones del socio principal.

1.3 Propuesta interpretativa: de la polarización doméstica a la incertidumbre estratégica

Este trabajo parte de una propuesta interpretativa prudente: la polarización social en Estados Unidos puede haber dejado de ser un fenómeno estrictamente interno para convertirse en una variable

que afecta, de forma indirecta pero relevante, a la política exterior hacia Europa. El mecanismo no se plantea como una relación automática, sino como un proceso en el que intervienen instituciones, incentivos políticos y lecturas estratégicas.

La polarización puede limitar la coherencia de la acción exterior por varias vías: reduce el espacio para consensos duraderos, facilita el uso partidista de la política exterior, dificulta la continuidad entre administraciones y puede amplificar decisiones que, aun siendo reversibles, son leídas por los aliados como señales de compromiso más condicionado. Desde el lado europeo, lo decisivo no es solo lo que Estados Unidos hace en un momento dado, sino si ese curso de acción parece estable, sostenido y políticamente viable en el tiempo. Ese componente perceptivo importa porque condiciona expectativas y, con ellas, decisiones institucionales y de planificación.

De ahí que ciertas iniciativas europeas de defensa y seguridad puedan interpretarse, al menos en parte, como una respuesta a la percepción de debilitamiento o volatilidad del compromiso estadounidense con la seguridad europea. Esta lectura conecta con una sensibilidad constructivista: los discursos y las señales moldean expectativas, y en momentos de tensión o cambios bruscos la interpretación puede inclinarse hacia la cautela: si el garante puede fluctuar, conviene ampliar márgenes propios.

Tras esta introducción, el capítulo se desarrolla en tres apartados y se cierra con unas conclusiones. El primero reúne las claves conceptuales para interpretar la relación entre polarización interna y política exterior. El segundo recorre la evolución de la política exterior estadounidense hacia el espacio euroatlántico a lo largo del siglo XXI. El tercero se detiene en los periodos en los que la polarización alcanza niveles especialmente altos y explora cómo esos momentos pueden haber afectado al vínculo transatlántico y al debate europeo sobre autonomía estratégica.

2 Marco teórico

2.1 Teorías de las relaciones internacionales

2.1.1 Perspectiva neorrealista

El neorrealismo (realismo estructural) explica el comportamiento de los Estados a partir de cómo está organizado el sistema inter-

nacional: un entorno marcado por la ausencia de una autoridad central efectiva. En esa anarquía, los Estados suelen actuar bajo una lógica de autoayuda: deben garantizar su seguridad por sus propios medios y, por ello, compiten por poder y supervivencia (Waltz, 2001). Para comprender las causas del conflicto, este enfoque distingue tres niveles de análisis. La primera imagen mira a factores individuales (naturaleza humana o decisiones de líderes). La segunda se centra en rasgos internos del Estado, como el régimen político o sus divisiones sociales. La tercera pone el foco en la estructura del sistema, especialmente en la distribución de poder y en cómo la anarquía condiciona la conducta estatal (Waltz, 2001). El neorrealismo considera que la tercera imagen ofrece la explicación más sólida: la estructura empuja a los Estados a buscar equilibrios de poder para evitar desbalances que puedan poner en riesgo su seguridad (Waltz, 2001).

En esta lógica, anticipar importa tanto como reaccionar. Waltz habla de la «sombra del futuro» como el temor a que otros Estados se conviertan en amenazas potenciales: como nadie puede estar seguro de las intenciones ajenas a largo plazo, los Estados tienden a prever escenarios de conflicto y a ajustar sus estrategias de forma continua (Waltz, 2001). Por eso, incluso sin agresiones inmediatas, el sistema incentiva cautela y competición.

Dentro de ese marco, la percepción de amenaza ayuda a explicar por qué Estados distintos responden de manera diferente ante presiones parecidas. No basta con medir la distribución de poder: también importan la proximidad, las capacidades ofensivas y las intenciones atribuidas al otro. El concepto de equilibrio de amenaza capta esta idea: los Estados valoran qué consideran amenazante y, en función de ello, buscan alianzas o refuerzan sus defensas (Walt, 1985). Esto implica que un actor con poder limitado puede percibirse como muy peligroso si sus acciones parecen expansionistas. Se ha señalado, por ejemplo, el caso de Libia bajo Gadafi: pese a sus recursos militares modestos, sus actividades desestabilizadoras provocaron respuestas coordinadas de sus vecinos por la amenaza que proyectaba su conducta (Kirdin, 2017).

Esta importancia de la percepción se conecta con un problema clásico: la incertidumbre y la dificultad de distinguir entre medidas ofensivas y defensivas generan el «dilema de seguridad». Acciones que un Estado adopta como defensivas pueden interpretarse como agresivas por otros, alimentando una espiral de desconfianza que dificulta la cooperación y favorece la compe-

tición (Jervis, 1978). El riesgo crece cuando se malinterpretan señales. La crisis de los misiles de Cuba lo ilustra: aunque la Unión Soviética no pretendía atacar a Estados Unidos, existía el peligro de que sus movimientos se leyeran como preparativos ofensivos. Jervis destaca que Khrushchev subrayó que «Moscú no podía lanzar un ataque exitoso y que no había motivo para que Washington adoptara una respuesta preventiva» (Jervis, 1978: 180). El episodio muestra cómo percepciones subjetivas pueden afectar directamente a la estabilidad internacional.

Aun así, el neorrealismo no presupone que las respuestas a las presiones externas sean siempre automáticas. Aquí entra el realismo neoclásico, que añade un nivel intermedio: las presiones estructurales influyen, pero su traducción en política exterior pasa por filtros internos, como la percepción de las élites y la capacidad del Estado para movilizar recursos (Rose, 1998). Desde esta perspectiva, variables domésticas —equilibrios institucionales, cohesión política o capacidad de coordinación— pueden condicionar el grado de consistencia con el que un Estado define prioridades y sostiene compromisos.

Además, no todos los Estados reaccionan igual ante amenazas similares. En ciertos contextos, la falta de consenso y las disputas internas pueden derivar en *underbalancing*: aun percibiendo una amenaza externa, el Estado no moviliza recursos suficientes o adopta estrategias insuficientes o poco consistentes (Schweller, 2004). El apaciguamiento británico frente a la Alemania nazi suele presentarse como un ejemplo clásico de cómo restricciones y divisiones internas pueden contribuir a respuestas por debajo de lo esperable, pese al deterioro del entorno estratégico (Schweller, 2004).

En el plano de las alianzas, el realismo estructural entiende organizaciones como la OTAN como instrumentos para gestionar el equilibrio de poder en un sistema competitivo (Waltz, 2001). El realismo neoclásico mantiene ese marco, pero subraya que el grado de compromiso y la continuidad de las prioridades también están mediados por condiciones internas —costes políticos, equilibrios entre instituciones y capacidad de sostener consensos— que influyen en la credibilidad y en la sostenibilidad de los compromisos hacia los aliados (Rose, 1998; Schweller, 2004).

2.1.2 Enfoque constructivista en las relaciones internacionales

El constructivismo parte de una idea simple: la estructura internacional no «programa» automáticamente lo que hacen los

Estados. Su conducta depende, en buena medida, de los significados que construyen en la interacción y de los procesos sociales que se acumulan con el tiempo (Wendt, 2005). Desde esta óptica, la anarquía —la ausencia de una autoridad central— no tiene un efecto único: puede vivirse como rivalidad o como cooperación según las prácticas y expectativas que se vayan asentando. Por eso, intereses e identidades no se dan por supuestos desde el inicio; se forman y cambian a medida que los Estados aprenden, se relacionan y reinterpretan su entorno (Wendt, 2005).

De ahí se sigue que un mismo entorno anárquico puede producir dinámicas muy distintas, dependiendo de marcos compartidos de interpretación y percepciones que se consoliden entre los actores. Incluso algo tan «material» como el poder militar no se interpreta de manera automática: una capacidad puede leerse como amenaza o como oportunidad según el contexto histórico y la relación previa entre quienes interactúan (Katzenstein, 1996; Wendt, 2005). En ese proceso, las normas internacionales y las instituciones sirven como marcos de sentido: orientan qué se considera legítimo, qué resulta aceptable y cómo se definen ciertos intereses (Finnemore y Sikkink, 1998).

Aplicado al vínculo transatlántico, esta perspectiva sugiere que la OTAN se entiende peor si se reduce a una alianza militar pensada solo para contener amenazas externas. Su continuidad también descansa en valores compartidos y en expectativas mutuas sobre seguridad, liderazgo y responsabilidad, que han sostenido su legitimidad con el paso del tiempo (Adler y Barnett, 1998). Además, esa legitimidad se apoyó en una narrativa más amplia de cooperación tras la Guerra Fría, que dio a la Alianza un sentido renovado dentro del orden posterior.

En ese marco cobra especial relevancia el concepto de comunidades de seguridad. Para Adler y Barnett (1998), no basta con cooperar por conveniencia: existe una comunidad de seguridad cuando se asienta un sentido de comunidad y unas expectativas compartidas y fiables de cambio pacífico, de modo que sus miembros dan por supuesto que resolverán sus disputas sin recurrir a la guerra ni al uso de la fuerza entre ellos. Ese suelo de confianza se alimenta de aprendizaje social, hábitos de cooperación y significados compartidos. En el caso transatlántico, esta lógica ayuda a entender por qué la relación puede aguantar tensiones puntuales sin romperse, aunque esas tensiones pongan a prueba la cohesión.

Katzenstein (1996) añade un matiz importante: las percepciones de amenaza y las políticas de seguridad están atravesadas por tradiciones culturales y normas internas. Por eso, la política exterior no es solo respuesta a presiones externas; también expresa valores y narrativas nacionales que moldean la manera de leer el entorno internacional.

En consecuencia, normas e identidades no se forman únicamente dentro de los Estados: también se construyen en el propio sistema internacional, donde alianzas y comunidades de seguridad actúan como espacios de socialización. Esto permite observar cómo las narrativas internas en Estados Unidos pueden chocar —o encajar— con normas compartidas y percepciones de amenaza, generando tensiones sobre el significado de liderazgo o compromiso en el exterior.

Aunque el constructivismo se aleja del realismo estructural en el énfasis, ambos reconocen la importancia del nivel estructural. La diferencia es que, para el constructivismo, esa estructura incluye una dimensión ideacional: identidades colectivas y normas transnacionales condicionan cómo se interpretan las presiones externas y, en consecuencia, cómo se responde a ellas.

2.1.3 Convergencia entre neorrealismo y constructivismo

Neorrealismo y constructivismo parten de supuestos distintos, pero pueden combinarse sin forzarlos si se usan para responder a preguntas diferentes. El neorrealismo fija las presiones estructurales que empujan a los Estados a priorizar seguridad y equilibrio (Waltz, 2001). El constructivismo ayuda a entender por qué, ante presiones parecidas, las respuestas no son idénticas: porque los Estados interpretan amenazas y compromisos a través de identidades, percepciones y significados compartidos (Wendt, 2005). Este cruce resulta útil para analizar cómo la polarización interna en Estados Unidos puede terminar influyendo en su política exterior y en la relación con Europa.

El punto de contacto está en la amenaza: la estructura impone límites, pero la política concreta depende de cómo se leen señales e intenciones. Las percepciones erróneas pueden escalar tensiones y disparar respuestas desproporcionadas (Jervis, 1978), mientras que una historia de cooperación y un lenguaje común pueden facilitar acuerdos (Wendt, 2005).

También importan normas e instituciones, no solo como reglas, sino como marcos que legitiman acciones y estabilizan expectativas (Finnemore y Sikkink, 1998). Por eso, la OTAN puede entenderse a la vez como instrumento estratégico y como comunidad de valores; su continuidad tras la Guerra Fría se explica no solo por cálculo material, sino también por su reinterpretación en un contexto más cooperativo (Adler y Barnett, 1998; Kaminski, 2019).

Cuando entra el factor doméstico, la combinación cobra más sentido: el equilibrio de poder puede ser una necesidad, pero definir qué es amenaza, qué costes son aceptables y qué compromisos se sostienen depende de narrativas internas (Jervis, 1978). Eso puede afectar a la credibilidad de los compromisos estadounidenses y alimentar en Europa el debate sobre autonomía estratégica (Martin y Sinkkonen, 2021). En paralelo, iniciativas europeas de seguridad pueden leerse como respuesta material y como intento de reforzar una identidad propia de actor (Adler y Barnett, 1998).

En suma, el neorrealismo aclara restricciones y presiones del entorno, pero se queda corto si no explica cómo se interpretan. El constructivismo ilumina significados y normas, pero necesita recordar que no actúan en el vacío: hay capacidades y distribución de poder que ponen límites. Usarlos de forma complementaria ayuda a evitar dos reduccionismos: materialismo sin ideas e ideas sin límites materiales.

2.2 Concepto de polarización

2.2.1 Definición y tipos de polarización

La polarización puede entenderse como el proceso por el que opiniones, actitudes e intereses se van separando hasta agruparse en dos polos enfrentados (Friedrichs y Tama, 2022; Borg, 2024). En los últimos años ha ganado peso también en el análisis de la política internacional, porque sus efectos no se quedan dentro de las fronteras estatales y pueden proyectarse hacia el exterior. Para trabajar con el concepto con cierta precisión conviene distinguir entre polarización ideológica y polarización afectiva, dos dimensiones que interactúan y pueden condicionarse mutuamente.

La polarización ideológica alude a la distancia creciente en posiciones sobre cuestiones políticas concretas: desde el papel del

Estado hasta cómo se entiende el orden internacional o el valor del multilateralismo. La polarización afectiva, en cambio, tiene más que ver con la identificación emocional y partidista: el desacuerdo deja de ser solo sobre políticas y pasa a vivirse como una cuestión de identidad, donde el adversario se percibe como alguien moralmente inaceptable (Iyengar *et al.*, 2012). Ambas dimensiones pueden reforzarse: la ideológica estructura preferencias y prioridades, mientras la afectiva dificulta la cooperación con el adversario.

En política exterior, la polarización ideológica puede notarse en los cambios de orientación entre administraciones. Cuando crece la distancia, aparecen posturas más enfrentadas sobre cooperación internacional, multilateralismo o compromisos con aliados, lo que complica sostener una línea reconocible y aumenta la incertidumbre para sus socios (Friedrichs y Tama, 2022). En el vínculo transatlántico, las diferencias entre demócratas y republicanos influyen también en la manera de leer amenazas y en el enfoque hacia la seguridad colectiva (Smeltz, 2022). En la práctica, esto se traduce en oscilaciones en compromisos internacionales y enfoques más unilaterales, mermando la capacidad de liderazgo de Estados Unidos (Bloethe, 2021).

La polarización afectiva, por su parte, se asocia a mayores dificultades para construir acuerdos. Cuando el rechazo hacia el adversario domina, el margen para el consenso se reduce y puede aumentar la dependencia de decisiones unilaterales del Ejecutivo (Colomer, 2023). En política exterior, esa falta de acuerdos internos puede traducirse en respuestas menos consistentes y en una erosión de la confianza de los aliados, que perciben un compromiso más inestable (Borg, 2024).

La literatura revisada sugiere, además, un patrón: momentos de polarización interna intensa coinciden con etapas de mayor variación en la política exterior estadounidense, lo que apunta a una relación estrecha entre división interna y pérdida de influencia (Colomer, 2023). Esto no implica un efecto automático ni inmediato, pero sí indica que, en crisis internacionales, el consenso interno facilita proyectar fortaleza y coherencia (Friedrichs y Tama, 2022).

En ese marco, la dinámica institucional importa. El bipartidismo y la separación de poderes han contribuido a un entorno de confrontación sostenida en el que las instituciones pueden reforzar el conflicto al reducir incentivos para el consenso (Colomer, 2023).

En política exterior, esto puede debilitar el papel del Congreso como contrapeso efectivo y favorecer un uso más frecuente de competencias ejecutivas. Friedrichs y Tama (2022) señalan que esta tendencia ha restado coherencia y previsibilidad al compromiso internacional de EE. UU., haciendo su liderazgo más dependiente de ciclos presidenciales.

La comparación internacional ayuda a situar el caso. Bernaerts *et al.* (2023) muestran que democracias más consensuales —como las escandinavas— tienden a contener mejor la polarización gracias a estructuras institucionales más representativas. En contraste, sistemas mayoritarios como el estadounidense presentan mayores niveles de polarización ideológica y afectiva, lo que dificulta políticas sostenidas y coherentes.

Aun así, no todo el análisis termina en una lectura solo negativa. Algunos trabajos sugieren que choques externos fuertes —crisis económicas o conflictos— pueden reducir temporalmente las divisiones internas al crear un foco común, siempre que lleguen antes de que se consoliden bloques extremos (McCarthy *et al.*, 2006; Axelrod *et al.*, 2021). Para la política exterior estadounidense, este matiz es relevante porque ayuda a explicar por qué, en ciertos momentos, una crisis puede generar unidad transitoria y facilitar acuerdos.

En conjunto, aunque ambas dimensiones importan, aquí se considera que la polarización ideológica pesa especialmente para entender la política exterior, porque estructura prioridades y orientaciones entre administraciones. La polarización afectiva puede actuar como elemento amplificador, al dificultar la construcción de acuerdos duraderos (Axelrod *et al*., 2021).

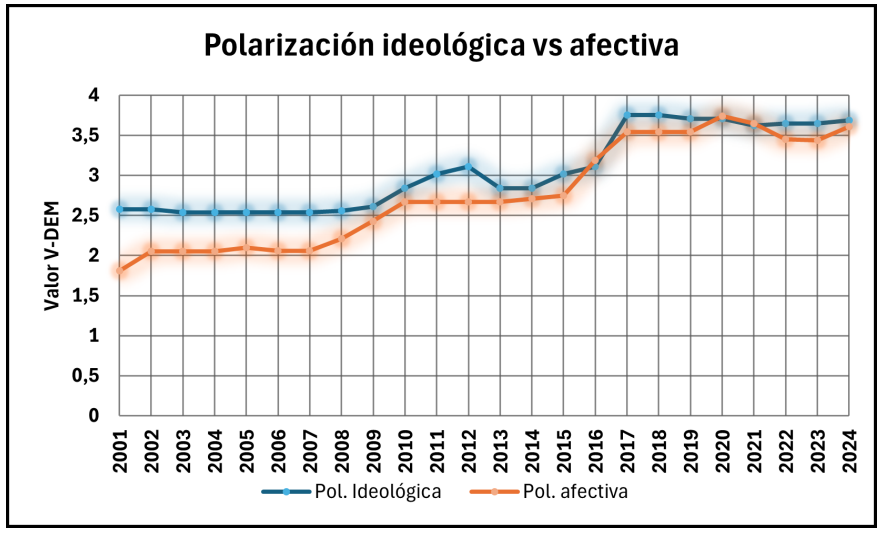
2.2.2 ¿Cómo medir la polarización?

Para este trabajo se utiliza el proyecto V-DEM[1] como referencia para seguir la evolución de la polarización en Estados Unidos a lo largo del tiempo. Su utilidad aquí es operativa: ayuda a identificar momentos de intensificación de las fracturas internas y, por tanto, periodos en los que resulta razonable examinar con más

[1] El proyecto Varieties of Democracy (V-DEM) está diseñado para comparar sistemas políticos a lo largo del tiempo. Se apoya en evaluaciones de expertos por país y en modelos estadísticos orientados a mejorar la fiabilidad y la comparabilidad de los indicadores (Coppedge *et al.*, 2021). Entre sus dimensiones incluye variables relacionadas con polarización.

detalle su posible relación con la política exterior hacia Europa (McCoy *et al*., 2022; Bernaerts *et al*., 2023). Como complemento, los datos del *Chicago Council on Global Affairs* permiten observar cambios en la opinión pública estadounidense sobre el vínculo transatlántico.

Se emplean dos indicadores de V-DEM: *polarization of society* y *political polarization*. Siguiendo a Bernaerts *et al*. (2023), el primero se aproxima a la polarización ideológica y el segundo a la polarización afectiva. Para facilitar la lectura, ambos se presentan en una escala de 0 a 4, donde los valores altos indican mayores divisiones y deterioro de la convivencia política.



La figura 1 recoge la evolución de estas dos vertientes durante el período de estudio y se utilizará como apoyo para orientar el análisis en apartados posteriores.

2.2.3 Evolución de la polarización en EE. UU.

La polarización en Estados Unidos no se explica solo por cambios en actitudes sociales; también se vincula a un diseño institucional que puede dificultar la cooperación partidista. La separación estricta de poderes nació para evitar la concentración de autoridad, pero en escenarios de antagonismo elevado tiende a favorecer la confrontación (Colomer, 2023). A ello se suma la combinación de elecciones presidenciales separadas y un sistema

legislativo basado en distritos de mayoría relativa, que reduce la representatividad y empuja a una dinámica de «bloque contra bloque» (Colomer, 2023).

En ese marco, un Ejecutivo elegido de forma independiente y un Congreso bicameral con equilibrios propios generan incentivos para el bloqueo: con frecuencia, un partido controla la Presidencia, mientras el otro domina al menos una de las cámaras, lo que eleva el coste político de cooperar (Colomer, 2023). Cuando el Legislativo no produce acuerdos estables, la iniciativa tiende a desplazarse hacia la Presidencia, un patrón que se vuelve especialmente visible cuando el entorno internacional presiona para actuar con rapidez (Friedrichs y Tama, 2022).

El bloqueo se aprecia con claridad en el Senado. La disciplina partidista y las reglas de supermayorías facilitan que iniciativas relevantes se estanquen, alimentando la percepción de ineficacia del sistema (Colomer, 2023). En la práctica, el filibusterismo[2] eleva el umbral para avanzar legislación y hace más frecuente el recurso a mociones de clausura (*cloture*) para terminar el debate, que Colomer señala como indicador directo del bloqueo en contextos de polarización (Colomer, 2023).

Esta transformación importa cuando se mira hacia fuera. La polarización interna puede dificultar consensos estratégicos y hacer que las prioridades cambien con mayor brusquedad entre administraciones (Friedrichs y Tama, 2022; Smeltz, 2022). Esto no implica que toda variación se explique por la polarización, pero sí sugiere que sostener líneas coherentes en el tiempo resulta más complicado cuando el desacuerdo interno es intenso.

En paralelo, la menor colaboración del Congreso favorece que los presidentes actúen con mayor autonomía, recurriendo a órdenes ejecutivas o a acuerdos con respaldo legislativo limitado para avanzar agendas exteriores (Bloethe, 2021). Esta vía puede ser eficaz a corto plazo, pero reduce la continuidad y proyecta una señal de imprevisibilidad hacia aliados que dependen de compromisos duraderos.

Desde una mirada constructivista, el problema no es solo institucional, sino también narrativo: las disputas internas sobre el

[2] En el Senado de EE. UU., el *filibuster* es una táctica para prolongar el debate y retrasar o impedir una votación; la *cloture* es el mecanismo para limitar el debate y superar esa obstrucción. Introducida en 1917 y reformada en 1975, la *cloture* requiere tres quintos del Senado (sesenta votos) (United States Senate, 2025c, 2025a).

papel global de Estados Unidos o sobre qué amenazas se consideran prioritarias influyen en cómo se interpretan costes y objetivos de la acción exterior (Borg, 2024). En Europa, esas oscilaciones alimentan dudas sobre la fiabilidad del compromiso estadounidense con la seguridad europea, incluso dentro de la OTAN, y refuerzan los debates sobre autonomía estratégica e iniciativas para desarrollar capacidades propias (Pesu y Sinkkonen, 2024). En conjunto, la polarización puede dificultar políticas exteriores consistentes y erosionar la imagen de Estados Unidos como actor previsible y fiable (Friedrichs y Tama, 2022).

2.3 Relación entre polarización y teorías de relaciones internacionales

2.3.1 Articulación entre polarización y política exterior desde el neorrealismo

En el neorrealismo, la intuición de partida es conocida: en un sistema anárquico, los Estados tienden a priorizar su seguridad y a vigilar el equilibrio de poder (Waltz, 2001). Lo relevante aquí es que esa respuesta no se sostiene igual cuando dentro del país falta un acuerdo mínimo sobre prioridades. Con una polarización ideológica intensa, se vuelve más difícil mantener una línea exterior estable: no solo cambian objetivos entre administraciones, también se discute de forma más aguda el coste de los compromisos, lo que reduce la consistencia de la política exterior a ojos de aliados y adversarios (Friedrichs y Tama, 2022; Colomer, 2023).

El realismo neoclásico permite concretar el mecanismo: las presiones externas influyen, pero se traducen en decisiones a través de filtros internos, como la interpretación de las élites y la capacidad del Estado para coordinarse y movilizar recursos (Rose, 1998). En ese marco, la polarización puede elevar el riesgo de respuestas incompletas o difíciles de sostener en el tiempo. Schweller conceptualiza este tipo de desviación como *underbalancing*: aun percibiendo una amenaza, el Estado no responde con la coherencia o intensidad esperable porque las disputas internas dificultan la movilización política necesaria (Schweller, 2004).

Esta lógica también afecta a cómo se definen y priorizan amenazas. Walt recuerda que la percepción de amenaza no depende solo del poder material: influyen la proximidad, las intenciones

atribuidas y la lectura política del adversario (Walt, 1985). En un contexto polarizado, esas lecturas pueden volverse menos compartidas y más sensibles a la disputa partidista. Borg (2024), por ejemplo, apunta a una convergencia relativa ante el ascenso de China, mientras que en el caso de Ucrania el desacuerdo interno puede dificultar sostener una postura estable.

El dilema de seguridad añade una advertencia útil: la incertidumbre y la interpretación de señales pueden escalar tensiones incluso entre actores racionales (Jervis, 1978). Trasladado a la política exterior en contextos polarizados, el punto no es que el sistema «obligue» a un resultado, sino que las divergencias internas pueden trasladarse a la forma de valorar riesgos, costes y compromisos, haciendo más probable una línea cambiante o contradictoria en el tiempo (Jervis, 1978).

Por último, si la OTAN encaja con la lógica del equilibrio en Europa, la polarización estadounidense introduce una duda práctica sobre la continuidad del compromiso. Esa incertidumbre puede reforzar, entre los aliados europeos, el incentivo a cubrir riesgos mediante más inversión y planificación propia y, en el marco de la Unión Europea, alimentar el debate sobre capacidades autónomas como forma de reducir vulnerabilidades ante posibles virajes (Pesu y Sinkkonen, 2024). En conjunto, esta lectura permite tratar la polarización no como un asunto meramente doméstico, sino como un factor que podría afectar a la estabilidad del papel estadounidense en el espacio euroatlántico.

2.3.2 Papel del constructivismo en el análisis de la percepción transatlántica

Desde un enfoque constructivista, la polarización importa porque puede alterar los marcos desde los que Estados Unidos interpreta su papel internacional y legitima sus compromisos. Cuando el conflicto interno se intensifica, no solo se discuten políticas concretas: también se tensionan ideas sobre identidad, amenaza y responsabilidad exterior, lo que puede dificultar sostener una política exterior reconocible y estable. En términos de Wendt (2005), intereses e identidades no son fijos: se construyen socialmente y pueden variar cuando cambia el contexto interno y las normas que organizan el debate público.

En ese plano, la OTAN es un ejemplo útil porque su cohesión no depende únicamente de capacidades. Adler y Barnett recuerdan que una comunidad de seguridad se sostiene sobre expectati-

vas compartidas y fiables de cambio pacífico, además de hábitos de cooperación y confianza acumulada (Adler y Barnett, 1998). Si esas expectativas se ven sometidas a cuestionamiento recurrente —aunque no cambien de inmediato los despliegues o las capacidades— la relación puede resentirse en el terreno de la credibilidad. Algo parecido ocurre con las normas: Finnemore y Sikkink (1998) explican que se difunden, se interiorizan y también se disputan, pudiendo transformarse con el tiempo. En un clima polarizado, esa disputa puede intensificarse y afectar a ideas que parecían asentadas, como el valor del multilateralismo o el sentido del compromiso transatlántico.

El efecto tiende a ser doble. Hacia dentro, cuesta más construir una base común que legitime una política exterior sostenida; hacia fuera, se proyecta una imagen menos predecible, lo que puede erosionar la confianza aliada. En el caso del vínculo transatlántico, Pesu y Sinkkonen (2024) señalan que la percepción europea de fiabilidad se ve afectada por la inestabilidad interna estadounidense. En conjunto, el constructivismo ayuda a captar cómo la polarización puede alterar expectativas y marcos de interpretación que sostienen decisiones estratégicas, y por qué esos cambios pueden ser relevantes incluso cuando los intereses materiales de seguridad siguen presentes (Wendt, 2005).

3 La política exterior de Estados Unidos (2001–2024)

3.1 La política exterior de EE. UU. en la administración Bush (2001-2008)

Al final de la Guerra Fría, la política exterior de Estados Unidos tendía a apoyarse en el multilateralismo y en la gestión de crisis mediante marcos institucionales. Durante la presidencia de Bill Clinton (1993-2001), pese a la primacía adquirida tras la caída de la URSS, la estrategia exterior no se presentó como un proyecto de dominación total del sistema, y el recurso a coaliciones siguió siendo una pauta habitual (Ryan, 2017). Ese marco empezó a tensionarse con la llegada de George W. Bush en 2001, asociada por parte de la literatura a un enfoque más asertivo y unilateral (Daalder y Lindsay, 2003).

El 11 de septiembre de 2001 reordenó las prioridades estratégicas estadounidenses y reforzó la idea de que la seguridad exigía actuar con rapidez, incluso bajo una lógica preventiva. La res-

puesta se articuló como la «Guerra contra el Terror», que habilitó intervenciones militares y reforzó un liderazgo dispuesto a sostener el orden global mediante el uso de la fuerza (Ryan, 2017). En ese marco se invadió Afganistán en octubre de 2001, con respaldo internacional y apoyo de la OTAN, aunque la ocupación evidenció pronto problemas en la reconstrucción y la estabilización, contribuyendo a una guerra prolongada y al resurgimiento talibán (Bogren, 2007).

La gran fractura transatlántica llegó con Irak en 2003: la intervención no contó con autorización del Consejo de Seguridad de la ONU y se justificó, entre otros argumentos, por las supuestas armas de destrucción masiva, cuya falta de evidencias terminó erosionando la legitimidad de la operación (Ryan, 2017). La división europea fue clara —apoyos como Reino Unido y España frente a rechazos como Francia y Alemania— y Washington optó por una coalición *ad hoc*, lo que reforzó la percepción de unilateralismo (Sazo Muñoz, 2009). En paralelo, Europa ya venía impulsando esfuerzos para reforzar capacidades propias en el marco de la Política Europea de Seguridad y Defensa (PESD), sin plantearlos como una ruptura con la OTAN (Hunter, 2002). En conjunto, la etapa Bush dejó una política exterior cuestionada por sus costes de legitimidad y por el desgaste acumulado en Irak y Afganistán (Bogren, 2007).

3.2 La política exterior de EE. UU. en la administración Obama (2009-2016)

Cuando Obama llegó a la presidencia en 2009, heredó dos guerras difíciles de cerrar, una crisis económica y una reputación exterior dañada. Su intención fue recuperar margen político con un tono más conciliador y una preferencia explícita por la diplomacia y la cooperación, presentando el liderazgo estadounidense como algo que debía ejercerse con más cautela en el uso de la fuerza (Lieberman, 2009). En su discurso de El Cairo resumió esa idea con una frase que buscaba marcar distancia con el intervencionismo más duro: «Ninguna nación puede ni debe imponer a otra un sistema de gobierno» (Obama, 2009). Ese cambio de tono, sin embargo, no eliminó los dilemas estratégicos: en varios frentes, su administración optó por ajustar instrumentos y prioridades más que por retirarse del escenario global (Powell, 2015).

En Irak, la retirada de las tropas en 2011 respondió a una presión interna evidente por reducir costes y exposición, pero no aseguró

un marco de seguridad estable. Según Rupérez (2013), el país quedó institucionalmente frágil, lo que facilitó la aparición de un vacío aprovechado más tarde por el Estado Islámico y obligó a Washington a implicarse de nuevo en 2014 con un perfil distinto: ataques aéreos y apoyo a fuerzas locales, sin volver a una ocupación masiva. En Afganistán, el recorrido fue más ambiguo: un refuerzo temporal en 2009 para contener a los talibanes y, después, una retirada gradual que no se tradujo en una pacificación definitiva.

Ese patrón ayuda a entender su enfoque general: evitar guerras de ocupación, pero sin renunciar a actuar cuando lo consideraba necesario. En la práctica, el antiterrorismo cedió un mayor peso al empleo de drones y operaciones especiales, reduciendo costes políticos frente a despliegues prolongados, aunque abrió controversias sobre sus implicaciones y eficacia a largo plazo (García, 2012). La retórica era de prudencia y alianzas; el resultado fue una política exterior que trató de mantener capacidad de intervención sin repetir el modelo de Irak (Powell, 2015).

La Primavera Árabe llevó esa lógica al límite. En Libia (2011), la fórmula de *leading from behind* —apoyo estadounidense con protagonismo europeo— buscó contener la exposición directa de EE. UU., pero también mostró los riesgos de intervenir sin una salida política clara: tras la caída de Gadafi, el país entró en una fase de inestabilidad prolongada y debilidad estatal (Whitmore y Deni, 2013). Siria, por su parte, se convirtió en un episodio especialmente delicado para la percepción del liderazgo estadounidense. Tras el uso de armas químicas en 2013, la administración evitó una intervención militar directa y optó por una vía diplomática con Rusia orientada a un desarme químico parcial. La decisión se interpretó de forma divergente: para algunos, dañó la credibilidad disuasoria (Deni, 2015); para otros, fue coherente con una contención deliberada (Powell, 2015). En cualquier caso, el episodio alimentó una pregunta incómoda también en Europa: hasta qué punto Washington estaba dispuesto a asumir costes altos en crisis complejas.

En el plano geopolítico, Obama impulsó el *Pivot to Asia*, priorizando el Indo-Pacífico ante el ascenso de China y tratando de reforzar alianzas regionales y su presencia estratégica (Hillison, 2018). En Europa, ese giro se leyó con inquietud: no como ruptura, sino como una señal de que el continente dejaba de ser el centro de gravedad en la agenda estadounidense (Powell, 2015). Aun así, la anexión rusa de Crimea en 2014 reactivó la centra-

lidad de la seguridad europea. La respuesta estadounidense se basó en sanciones y refuerzo del flanco oriental de la OTAN, sin una intervención militar directa, y reforzó la expectativa de que los aliados europeos asumieran más carga en defensa (Guinea, 2018).

Ese reajuste se notó en el debate sobre el reparto de responsabilidades: se reafirmó el valor de la Alianza, pero se insistió en el aumento del gasto europeo, alineado con el objetivo del 2 % acordado en Gales (García, 2016). Persistieron, además, fricciones puntuales, como en la defensa antimisiles, donde el impulso estadounidense no siempre encontró el mismo entusiasmo en París o Berlín, preocupados por el efecto sobre la relación con Rusia (Whitmore y Deni, 2013). En conjunto, la etapa Obama dejó un vínculo transatlántico funcional, pero con una tendencia que se fue normalizando: cooperación estrecha, sí y, al mismo tiempo, una Unión Europea más consciente de sus dependencias y más atenta a reforzar capacidades propias.

3.3 La política exterior de EE. UU. en la primera administración Trump (2017-2020)

Con Donald Trump, la política exterior de Estados Unidos se volvió menos institucional y más transaccional: alianzas y compromisos se presentaban como acuerdos en los que cada socio debía justificar su valor en dinero, seguridad y resultados. La relación con la OTAN fue el ejemplo más visible. Trump la criticó con dureza, llegó a cuestionar su utilidad y presionó públicamente a los aliados para que aumentaran el gasto en defensa, aunque sin traducir esa retórica en una retirada real de Europa; de hecho, mantuvo e incluso reforzó ciertos elementos de la presencia militar estadounidense y logró que varios países elevaran su inversión (Benedicto Solsona, 2018). El mensaje de fondo no era nuevo, pero el modo de plantearlo —como un reproche directo y casi contable— sí deterioró el clima político.

Ese enfoque también se trasladó al terreno económico. En 2018, Washington impuso aranceles a productos europeos como el acero y el aluminio, invocando razones de seguridad nacional. La Unión Europea respondió con medidas de represalia y, según Benedicto Solsona (2018), el episodio alimentó la percepción de que Estados Unidos estaba dispuesto a tratar a sus socios como rivales cuando lo consideraba conveniente. No fue solo una dis-

puta comercial: afectó a la confianza en la previsibilidad del socio estadounidense.

En paralelo, la Estrategia de Seguridad Nacional de 2017 devolvió al primer plano la competencia entre grandes potencias, señalando a China y Rusia como actores revisionistas que desafiaban el orden internacional (The White House, 2017). Sin embargo, la aplicación de esa visión no siempre fue lineal. Con China, la administración endureció el pulso económico y reforzó un marco de rivalidad, aunque Trump alternó esa línea con una diplomacia muy personalista con Xi Jinping. Con Rusia ocurrió algo parecido: pese a una retórica a veces conciliadora, Washington mantuvo sanciones y reforzó su presencia en el flanco oriental de la OTAN, lo que alimentó la sensación europea de que el tono y la política concreta podían ir por carriles distintos (Schuette, 2023). Para varios aliados, el problema no era solo la dureza o suavidad de la postura, sino la impresión de que el rumbo podía cambiar con rapidez.

En Oriente Medio, Trump optó por un alineamiento especialmente estrecho con Israel y por una política de «máxima presión» sobre Irán. En 2018, Estados Unidos reconoció Jerusalén como capital de Israel y trasladó su embajada desde Tel Aviv (The White House, 2018), una decisión que provocó un rechazo amplio en la comunidad internacional. Ese mismo año abandonó el acuerdo nuclear con Irán y restableció sanciones para forzar una renegociación en términos más favorables para Washington (Benedicto Solsona, 2018). Según diversos análisis, el efecto fue más bien un aumento de la tensión regional que una moderación clara del comportamiento iraní.

En el plano militar, el gasto en defensa aumentó[3] y la disuasión ocupó un lugar central en el discurso estratégico (Benedicto Solsona, 2018). A la vez, Trump combinó promesas de reducir intervenciones con acciones puntuales, como los bombardeos en Siria en 2017 y 2018 tras el uso de armas químicas por el régimen de Bashar al-Assad (Dombrowski y Reich, 2017). Esa mezcla mostró una tensión constante entre el mensaje de «menos guerras» y la disposición a usar la fuerza cuando Washington quería marcar un límite.

[3] Según datos de SIPRI (2024), el gasto en defensa de EE. UU. aumentó de 639 856 millones de dólares en 2016 a 778 397 millones de dólares en 2020.

Finalmente, a nivel comunicativo, Trump practicó una diplomacia de corte populista: anuncios en redes sociales, mensajes dirigidos a su audiencia doméstica y choques frecuentes con organismos internacionales como la ONU o la OMC (Löfflmann, 2022). En términos interpretativos, puede leerse como una etapa orientada a maximizar ventajas nacionales y a competir abiertamente, pero que, por su estilo confrontativo y cambiante, aumentó la incertidumbre estratégica y empujó a la UE a tomarse más en serio la necesidad de prepararse para actuar con mayor autonomía (Benedicto Solsona, 2018; Löfflmann, 2022).

3.4 La política exterior de EE. UU. durante la administración Biden (2021-2024)

La llegada de Biden a la Casa Blanca se interpretó como un intento de devolver previsibilidad a la política exterior tras la etapa Trump: menos fricción con los aliados, más coordinación y un lenguaje multilateral. Ese giro de estilo, sin embargo, convivió con un contexto exigente: rivalidad sostenida con China, presión de Rusia sobre Europa y una política interna cada vez más polarizada. En su marco estratégico, la administración presentó el liderazgo estadounidense como una combinación de instrumentos militares, económicos y diplomáticos para mantener influencia en un entorno más competitivo (The White House, 2022). En paralelo, el énfasis en democracia y cooperación funcionó también como una forma de recomponer legitimidad y cohesión entre socios (Lacatus y Blanc, 2023).

Uno de los focos centrales fue recomponer la relación transatlántica. Biden buscó reducir la fricción política y reafirmar el compromiso con la OTAN, pero esa recuperación no implicó un retorno automático a la dependencia tradicional. La Unión Europea siguió avanzando en iniciativas para reforzar capacidades y coordinación propias, presentadas como complementarias a la Alianza, pero orientadas a ganar margen de acción en un entorno más incierto (Romano, 2024). En muchas capitales europeas, fue calando una idea simple: seguir de la mano de Washington era imprescindible, pero sin dar por garantizada su implicación.

La sintonía en seguridad, además, no eliminó fricciones económicas. La Ley de Reducción de la Inflación (IRA) impulsó producción nacional y transición energética, pero en Europa se percibió como una medida con efectos proteccionistas que podía perjudicar a la industria europea (von Daniels, 2024). El resultado fue una

relación más cooperativa que durante Trump, aunque no necesariamente más cómoda en todos los frentes.

El gran eje del periodo fue Ucrania. Tras la invasión rusa de febrero de 2022, EE. UU. lideró la respuesta occidental con sanciones y apoyo militar a Kiev (Demczuk, 2023). En 2023, Biden presentó la guerra como una prueba de resistencia democrática frente a la política del miedo y la fuerza, una formulación que refuerza una lectura ideacional del conflicto, aunque también puede entenderse como una estrategia de contención y equilibrio frente a Rusia (Biden, 2023). La guerra reforzó la cohesión aliada: más atención al flanco oriental, mayor urgencia inversora y la entrada de Finlandia y Suecia. Las cumbres de Madrid (2022) y Vilna (2023) consolidaron ese giro con énfasis en disuasión y gasto en defensa (Arteaga y Simón, 2023). Al mismo tiempo, la prolongación del conflicto sin un horizonte claro convirtió el apoyo occidental en una variable crítica: una reducción importante podría alterar la capacidad ucraniana de sostener el esfuerzo y reconfigurar el equilibrio europeo (Demczuk, 2023).

En el Indo-Pacífico, Biden mantuvo la contención hacia China, pero con un enfoque más coordinado. Impulsó marcos como AUKUS y QUAD[4] y endureció controles tecnológicos en ámbitos sensibles como el de los semiconductores (Contreras Peralta, 2023). Aun así, la interdependencia económica limitó el desacoplamiento y, en el caso europeo, se consolidó una estrategia de *de-risking*: reducir dependencias críticas sin romper vínculos comerciales (von Daniels, 2024).

En Oriente Medio, la administración combinó continuidad y reajuste. La retirada de Afganistán en 2021 quedó marcada por la caída rápida de Kabul y una evacuación difícil, dañando la percepción de control y planificación (Tovar Ruiz, 2022). En Irán, el intento de reactivar el JCPOA no prosperó (Soare, 2021). Y, respecto a Israel, el apoyo tradicional se mantuvo, pero la guerra en Gaza desde 2023 expuso un dilema persistente entre respaldo a un aliado y coherencia con el discurso sobre derechos humanos, con costes reputacionales y tensiones políticas (Aguirre y Morales Bertrand, 2024).

En suma, Biden trató de ejercer una política de «poder inteligente», reforzando alianzas y legitimidad sin renunciar a ins-

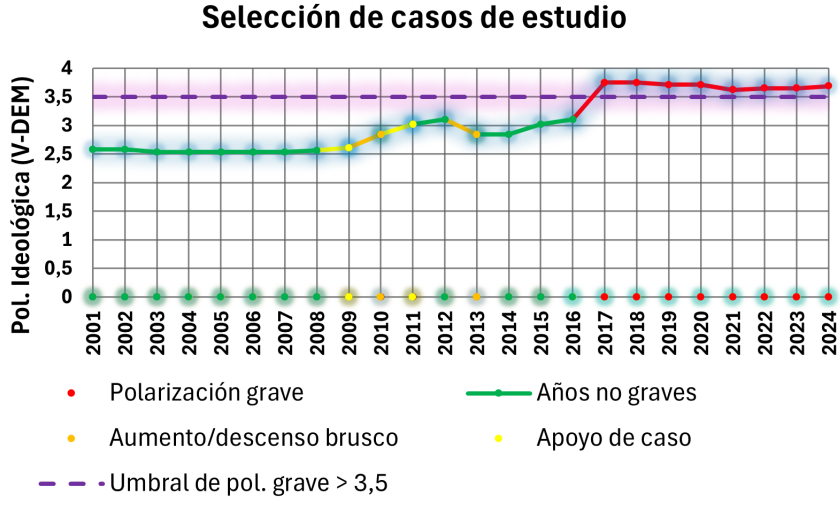
[4] AUKUS es una alianza estratégica entre Australia, Reino Unido y Estados Unidos. El QUAD responde a una estrategia informal conformada por Estados Unidos, Japón, India y Australia para contrarrestar la influencia china en el Indo-Pacífico.

trumentos coercitivos cuando lo consideró necesario (Contreras Peralta, 2023). Su margen, sin embargo, estuvo condicionado por la redistribución del poder global y por la polarización interna estadounidense, que dificulta proyectar una línea exterior estable y previsible (Romano, 2024). El resultado fue una relación transatlántica más cooperativa y una respuesta occidental más coordinada frente a Rusia, pero también una cautela europea más asentada respecto a la dependencia de EE. UU.

4 Análisis de la repercusión de la polarización en EE. UU. en el vínculo transatlántico

4.1 Evolución de la polarización en EE. UU. según V-DEM (2001-2024)

Para seguir la polarización ideológica en Estados Unidos de manera comparable a lo largo del tiempo, este capítulo utiliza el indicador de V-DEM, que la sitúa en una escala de 0 (sin polarización) a 4 (polarización grave) (Coppedge *et al*., 2021). El uso de esta medida aquí es sobre todo práctico: sirve para ubicar cuándo la polarización se mantiene en niveles muy altos y cuándo cambia con especial rapidez, porque esos momentos son los que, si existe un vínculo con la política exterior, tendrían más probabilidades de dejar señales visibles en el discurso estratégico de Washington y en la manera en que Europa interpreta la consistencia del socio estadounidense.



La figura 2 permite observar de manera gráfica, el criterio de selección de casos. En ese sentido, el primer foco se pone en los años en los que el indicador se mueve ya en la parte alta de la escala. En este trabajo, se toma como referencia el valor de 3,5 para identificar los años cercanos a «polarización grave», y con ese criterio el tramo que más destaca es 2017-2024, que coincide con las administraciones de Trump (2017-2020) y Biden (2021-2024). Este recorte no pretende demostrar por sí solo ninguna relación causal: simplemente ayuda a acotar el periodo en el que la polarización aparece de forma más intensa y sostenida.

El segundo foco no se fija tanto en el nivel como en la velocidad del cambio. Además de mirar si la polarización es alta, interesa detectar años en los que aumenta abruptamente respecto al anterior. Con ese criterio, 2010 y 2017 resaltan por incrementos especialmente pronunciados, mientras que 2013 sobresale por un descenso poco habitual. Esta combinación permite priorizar aquellos puntos del periodo 2001-2024 donde resulta más razonable investigar si se producen ajustes relevantes en el marco estratégico estadounidense y si, en paralelo, se intensifican respuestas europeas orientadas a ganar margen de autonomía.

Por la misma lógica, la etapa de Bush queda en un segundo plano en este apartado: durante esos años el indicador se mantiene en niveles moderados y sin variaciones especialmente marcadas, lo que ofrece menos contraste para explorar la relación que plantea el trabajo. En cambio, alrededor del repunte de 2010 se incorporan también 2009 y 2011 como años de contexto inmediato, no porque sean máximos por sí mismos, sino porque ayudan a entender mejor qué ocurre antes y después del salto.

4.2 Período 2009-2011

Cuando Barack Obama llegó a la Casa Blanca en 2009, Estados Unidos seguía marcado por el desgaste de las guerras y por una economía aún vulnerable. En torno a 2010 se percibe un repunte brusco de polarización, que coincidió con dos hitos que concentraron la confrontación partidista: la aprobación de la *Affordable Care Act* y las elecciones de medio término, que devolvieron a los republicanos el control de la Cámara de Representantes (Jacobson, 2011). El efecto fue un clima de mayor bloqueo y negociación más difícil, que condicionó el margen político del Ejecutivo en el plano doméstico.

Desde una lectura neorrealista, la conflictividad interna importa porque estrecha la capacidad de sostener compromisos exteriores largos y costosos: aumenta el incentivo a priorizar frentes, limitar objetivos y reclamar mayor reparto de cargas. Desde una lectura constructivista, la polarización importa también porque disputa el relato sobre qué papel debe jugar EE. UU. en el mundo y, con él, la confianza que proyecta hacia sus socios. Por eso, se ha señalado que el estancamiento legislativo tiende a empujar a la presidencia a apoyarse más en la política exterior, donde dispone de más margen operativo que en la legislación interna (Carmines y Fowler, 2017; Colomer, 2023). Ese trasfondo se reflejaba, además, en actitudes sociales más prudentes respecto a intervenciones prolongadas y en diferencias partidistas visibles sobre multilateralismo y globalización (Bouton *et al*., 2010).

El cambio de tono se aprecia en el contraste entre las estrategias de seguridad nacional de la administración Bush y la de Obama. La *National Security Strategy* de 2006 explicitaba una lógica más unilateral y preventiva (The White House, 2006). La estrategia de 2010, en cambio, reencuadró el liderazgo en términos cooperativos: «Ninguna nación puede afrontar sola los retos del siglo xxi, ni dictar sus términos al mundo» (The White House, 2010: 40). Leída en clave constructivista, esa formulación busca recomponer la legitimidad estadounidense tras Irak y reconstruir la confianza con sus aliados. Leída en clave neorrealista, facilita coaliciones y justifica un reparto de cargas más exigente. El documento, además, dejaba entrever una atención creciente hacia Asia-Pacífico (The White House, 2010), lo que no implicaba abandonar Europa, pero sí repartir prioridades de forma más visible.

En paralelo, la Unión Europea reforzaba su arquitectura exterior. La entrada en vigor del Tratado de Lisboa impulsó el Servicio Europeo de Acción Exterior y consolidó el marco de la Política Común de Seguridad y Defensa, incluida la posibilidad de avanzar hacia una defensa común si hubiera unanimidad (Unión Europea, 2007). Grevi *et al.* (2009) describen este momento como un paso hacia una acción exterior más integrada, aunque todavía apoyada en la OTAN y en capacidades nacionales. En términos constructivistas, este tipo de reformas busca construir la idea de una UE con voz propia; en términos neorrealistas, sin embargo, el límite seguía siendo material: la dependencia en términos de seguridad resultaba incuestionable.

Dos decisiones estadounidenses dieron contenido práctico a esa ambivalencia europea. Primero, la retirada de Irak respondió a

fatiga social, costes y prioridades, reforzando la impresión de que Washington necesitaba cerrar ciclos de implicación prolongada. Segundo, la intervención en Libia en 2011 se convirtió en una señal especialmente nítida: Estados Unidos optó por un papel de apoyo mientras Francia y Reino Unido asumían el liderazgo operativo. Xuereb (2021) subraya que el episodio expuso a la vez límites europeos para articular una respuesta cohesionada y la disposición estadounidense a no liderar automáticamente. Ese patrón es compatible con la idea de *underbalancing*: una respuesta más contenida de lo esperable ante una crisis, en parte porque el liderazgo directo elevaba el coste político (Schweller, 2004). En una lectura constructivista, lo relevante es el efecto de señal: la implicación estadounidense aparece como contingente, no garantizada.

Esa dimensión simbólica se hizo explícita con el discurso de despedida del secretario de Defensa Robert Gates en Bruselas (2011), cuando advirtió que futuros líderes estadounidenses podrían «no considerar que la inversión de América en la OTAN merece la pena» si Europa no revertía el declive de sus capacidades (Dowdall, 2011: 5). Más que una reprimenda técnica, el mensaje reordenaba expectativas sobre responsabilidad compartida: desde el constructivismo, porque tensiona la narrativa de compromiso incondicional; desde el neorrealismo, puesto que vuelve a poner en primer plano la relación entre capacidades, reparto de cargas y credibilidad de la disuasión.

En conjunto, 2009-2011 no produce todavía una autonomía estratégica europea en sentido fuerte. Pero es compatible con un cambio de atmósfera: una política interna estadounidense más áspera, una política exterior más selectiva y una UE que empezaba a dotarse de instrumentos para actuar con mayor coherencia, en un entorno donde el liderazgo de Washington podía percibirse menos automático.

4.3 Despolarización: el caso de 2013

En 2013, se aprecia una despolarización relativa en Estados Unidos respecto al año anterior. Pero ese alivio no se tradujo en un sistema político fluido: el Congreso de los Estados Unidos siguió dividido —demócratas en el Senado y republicanos en la Cámara— y el año estuvo atravesado por episodios de confrontación institucional, como el cierre de gobierno de octubre y la crisis del techo de deuda. Los datos del Senado sobre el recurso a

mociones de clausura reflejan, además, que la dinámica de obstrucción siguió presente (United States Senate, 2014).

Ese doble plano se ve bien en el lanzamiento de las negociaciones del Acuerdo Transatlántico de Comercio e Inversiones (TTIP). El acuerdo no se entendió únicamente como un tratado comercial: se presentó como una apuesta por fijar estándares y reforzar la posición occidental en un entorno de competencia global más compleja. Hamilton (2015)[5] lo describió ante el Congreso como un instrumento para reposicionar a Estados Unidos y a los europeos en esa competencia «difusa». Desde Europa, el TTIP también se leyó como una vía para recuperar centralidad geopolítica en un momento en que Washington mostraba más atención hacia Asia (Meto, 2019). Leído desde el neorrealismo, el TTIP buscaba sostener influencia fijando estándares en un entorno competitivo; desde el constructivismo, pretendía reforzar la identidad transatlántica mediante reglas compartidas que legitimaran la cooperación.

Pero 2013 fue también el año en que ese terreno normativo sufrió una sacudida. El caso Edward Snowden y las filtraciones sobre vigilancia masiva de la NSA dañaron la confianza política y social en Europa, especialmente por el espionaje a líderes como Angela Merkel. La reacción no se limitó a indignación: instituciones europeas como el Parlamento Europeo y la Comisión Europea revisaron marcos de transferencia de datos y reabrieron el debate sobre autonomía regulatoria. Parte de la literatura interpreta que este clima aceleró la afirmación europea de soberanía en privacidad digital, cristalizada en el Reglamento General de Protección de Datos (GDPR) como un giro hacia mayor control normativo frente al enfoque estadounidense (Svantesson y Kloza, 2017). Obama trató de contener el deterioro con un discurso en enero de 2014 apelando a una relación entre aliados basada en respeto mutuo (Obama, 2014), pero en países como Alemania el daño dejó una huella más duradera, consolidando una mirada más crítica hacia el liderazgo estadounidense (Makeschin, 2015).

La crisis de Siria se leyó en Europa como una prueba de la credibilidad de Washington. Tras el ataque químico en Ghouta y la «línea roja» anunciada un año antes, Washington optó por una salida diplomática con Rusia que encauzó la adhesión siria a la Convención sobre Armas Químicas y el inicio del desmantela-

[5] Daniel Hamilton era el director de Centro para Relaciones Transatlánticas de la Universidad John Hopkins de Washington (Hamilton, 2015).

miento del arsenal (Rupérez, 2013; Powell, 2015). Para varios aliados europeos, la solución evitaba otra campaña militar, pero dejó una señal ambivalente: mostraba prudencia y aversión al coste, a la vez que alimentaba dudas sobre hasta qué punto EE. UU. asumiría el liderazgo cuando el apoyo interno fuese frágil (Deni, 2015). En ese sentido, el episodio es compatible con el concepto de *underbalancing* (Schweller, 2004) entendida como contención del liderazgo bajo restricciones domésticas, más que como una renuncia forzada ante una amenaza directa.

Por último, el acuerdo interino con Irán[6] (JPOA) en noviembre reforzó el lado cooperativo del vínculo transatlántico. Negociado con el P5+1 y con participación directa de Catherine Ashton, el pacto limitó temporalmente el programa nuclear iraní a cambio de alivio parcial de sanciones y proyectó una imagen de liderazgo diplomático coordinado con europeos (Powell, 2015).

En conjunto, 2013 sugiere que una despolarización relativa fue compatible con iniciativas que buscaban afianzar la relación con Europa (TTIP) y con episodios de cooperación diplomática (Irán), pero no evitó choques en el plano normativo (Snowden) ni eliminó la fricción interna. Leído con prudencia, 2013 sugiere que la política doméstica condiciona el margen de acción, pero el vínculo transatlántico también depende de cómo se combinan intereses y costes con confianza y reglas.

4.4 2017: récord de polarización durante el primer año de presidencia de Trump

El primer año de Donald Trump coincidió con el mayor clima de polarización en Estados Unidos hasta entonces, dificultando sostener reglas compartidas y consensos duraderos y proyectando esa tensión hacia fuera. Aunque el apoyo social a la OTAN seguía siendo mayoritario, la opinión pública estadounidense mostraba diferencias claras por electorados y mayor tibieza entre quienes se identificaban con Trump, haciendo la alianza más discutible políticamente (Smeltz *et al.*, 2017). En ese marco, el discurso «America First» se tradujo en un enfoque más transaccional: en su primera gran cita con la OTAN en Bruselas, Trump evitó rea-

[6] El *Joint Plan of Action* (JPOA), firmado en noviembre de 2013, fue el acuerdo interino que estableció los principios básicos de negociación con Irán. Este sirvió como base para el posterior *Joint Comprehensive Plan of Action* (JCPOA), firmado en julio de 2015 (Cronberg, 2017).

firmar con claridad el compromiso colectivo de defensa y exigió mayor esfuerzo financiero a los aliados (Trump, 2017), hasta el punto de que el Senado de Estados Unidos se vio empujado a respaldar públicamente la defensa colectiva, un gesto inusual cuando la continuidad del compromiso no está en duda (Graham, 2017).

La *National Security Strategy* (2017) consolidó ese cambio de marco. El documento adoptó una lectura competitiva del orden internacional, defendió revisar alianzas bajo criterios de reciprocidad e insistió en que Europa debía aumentar su contribución a la defensa —con referencia al objetivo del 2 %— y definió a Rusia y China como potencias «revisionistas» (The White House, 2017). En términos neorrealistas, la lógica dominante era de competitividad y reparto de cargas; en términos constructivistas, el efecto fue desplazar el lenguaje de comunidad hacia una relación fundamentalmente transaccional.

Varias decisiones de 2017 reforzaron en Europa la idea de imprevisibilidad. La retirada del Acuerdo de París simbolizó un alejamiento del multilateralismo climático y chocó con una UE donde el clima ya formaba parte de su identidad regulatoria y de proyección internacional (Chestnoy y Gersinkova, 2017). En paralelo, el endurecimiento del tono estadounidense sobre el acuerdo nuclear con Irán —pese a evaluaciones internacionales favorables— abrió una brecha con las principales capitales europeas (Thompson y Thränert, 2017). Y, en el terreno económico, las negociaciones del TTIP, ya debilitadas, terminaron de quedar aparcadas con el cambio de administración (Schneider-Petsinger, 2019). Cada episodio era gestionable por separado; juntos, alimentaron una percepción de volatilidad.

La respuesta europea combinó malestar diplomático y señales de ajuste. Angela Merkel lo resumió tras una cumbre aliada con una frase que se convirtió en referencia: los europeos debían «tomar su destino en sus propias manos» (Merkel, 2017). Y ante los movimientos de Washington respecto al acuerdo con Irán, Federica Mogherini defendió que no correspondía a un solo país terminar unilateralmente un acuerdo respaldado por el Consejo de Seguridad (EEAS, 2017b). Sin hablar de distanciamiento, el año dejó a una UE más vigilante y más dispuesta a proteger márgenes propios cuando percibiese vulnerabilidad.

En ese clima, se produjo un hito institucional con efectos duraderos: el lanzamiento de PESCO en noviembre de 2017, un ins-

trumento previsto desde Lisboa pero no activado hasta entonces (Consejo de la Unión Europea, 2017). Sería exagerado atribuirlo a un único factor —también pesaron el *Brexit* y un entorno de seguridad más exigente—, pero es razonable plantear que las señales procedentes de Washington (condicionalidad, énfasis en el reparto de cargas y menor previsibilidad) contribuyeron a abrir una ventana política para dar el paso (Martí Sempere, 2024). Así, 2017 no solo refleja un giro estadounidense: ayuda a entender por qué, desde Europa, la inquietud empezó a traducirse en herramientas concretas.

4.5 Polarización, unilateralismo y tensión transatlántica. El trienio 2018-2020

Entre 2018 y 2020, la política estadounidense siguió marcada por una polarización alta y por una dinámica institucional poco propicia al compromiso. En ese entorno, el Congreso tuvo dificultades para producir consensos sostenidos y el Ejecutivo tendió a apoyarse más en márgenes presidenciales, mientras el Senado recurría de forma intensiva a instrumentos para desbloquear obstrucciones (United States Senate, 2021). Este contexto no basta para explicar la política exterior, pero sí ayuda a entender por qué decisiones con fuerte impacto transatlántico se tomaron con escasa coordinación previa con los aliados.

Más que una suma de fricciones, 2018-2020 prolongó el giro transaccional abierto en 2017: en clave neorrealista, alianzas, comercio y despliegues se trataron como palancas para redistribuir costes y exigir reciprocidad; en clave constructivista, el vínculo perdió parte de su lógica de comunidad y pasó a percibirse como más condicional, con compromisos menos previsibles.

La salida unilateral de Estados Unidos del acuerdo nuclear con Irán (JCPOA) en 2018 condensó ambos planos. La decisión se adoptó sin alineamiento con socios europeos y provocó una reacción pública coordinada: Emmanuel Macron, Angela Merkel y Theresa May expresaron su «pesar» y reiteraron su compromiso con el acuerdo (UK Prime's Minister Office, 2018). Materialmente, el episodio reabrió un problema de proliferación y sanciones; políticamente, alimentó dudas sobre la fiabilidad de los compromisos estadounidenses, un coste sobre todo dañino cuando la cooperación depende de credibilidad y continuidad (Tovar Ruiz, 2020).

En paralelo, las fricciones comerciales reforzaron la lectura de una relación más transaccional. Los aranceles al acero y aluminio europeos en 2018 y nuevas tensiones en 2020 llevaron a la UE a responder con contramedidas, gestionando el conflicto en clave de reciprocidad (Comisión Europea, 2025). Y el TTIP, ya debilitado, quedó en la práctica congelado, cerrando la vía más ambiciosa para anclar el vínculo mediante un marco económico común (Schneider-Petsinger, 2019). Desde una óptica material, el recurso a aranceles ilustra el uso de instrumentos económicos como presión; desde una óptica normativa, reforzó la impresión de que incluso entre aliados el marco preferente de cooperación podía sustituirse por la lógica de presión-respuesta.

En 2020, el anuncio de retirar en torno a doce mil tropas estadounidenses de Alemania añadió una dimensión de seguridad a esa percepción de incertidumbre. Trump lo justificó como reacción a la falta de cumplimiento alemán en gasto de defensa, con una retórica de reproche hacia un aliado central (Alcaro, 2020). Más allá de su ejecución final, el episodio importó por la señal: si el despliegue se presenta como moneda de intercambio, el compromiso adquiere un carácter condicional. En términos constructivistas, eso erosiona confianza dentro de una comunidad de seguridad; en términos materiales, introduce dudas sobre la disponibilidad estadounidense cuando el apoyo doméstico o el cálculo político cambian (Tovar Ruiz, 2020).

La respuesta europea fue más que retórica. Durante el trienio se afianzó la idea de que Europa debía ampliar su margen de maniobra y reducir dependencias, sin plantearlo como sustitución de la OTAN (Tovar Ruiz, 2020). Ese diagnóstico se articuló en torno a la autonomía estratégica, entendida como refuerzo de capacidades y reducción de vulnerabilidades ante incertidumbres externas (Borrell, 2020).

Entre 2019 y 2020, ese impulso empezó a institucionalizarse. El primer ciclo de CARD[7] (2019-2020) buscó identificar cooperaciones y reducir duplicidades en capacidades (EDA, 2024). El Fondo Europeo de Defensa (EDF) asentó bases para financiar proyectos conjuntos y reforzar la base industrial y tecnológica (EDA, 2022).

[7] La *Coordinated Annual Review on Defence* (CARD) fue lanzada oficialmente en noviembre de 2017 con el objetivo de identificar carencias y oportunidades de cooperación entre los Estados miembros en materia de defensa, promoviendo la convergencia estratégica y una planificación más coherente a nivel europeo (EEAS, 2017a).

Y a finales de 2020, la UE reguló la participación de terceros en proyectos individuales de PESCO, abriendo una cooperación limitada bajo condiciones estrictas: una forma de equilibrar eficacia operativa y control europeo (Cózar Murillo, 2022). Leído desde un realismo pragmático, esa apertura permite sumar capacidades sin perder gobernanza; leído desde el constructivismo, delimita quién puede participar y bajo qué normas, reforzando una identidad europea definida por reglas.

En conjunto, el trienio 2018-2020 sugiere que la polarización y el bloqueo internos en Estados Unidos hicieron más probable una política exterior menos predecible y más unilateral y esa experiencia contribuyó a que en Europa la inquietud pasara de diagnóstico a diseño institucional. No fue el único motor —también pesaron el *Brexit* y el deterioro del entorno de seguridad—, pero estos años ayudan a explicar por qué la UE empezó a traducir dudas sobre fiabilidad en instrumentos concretos para sostener su autonomía de acción.

4.6 Polarización en la administración Biden (2021-2024)

El periodo 2021-2024 combinó dos rasgos que, juntos, ayudan a explicar la evolución del vínculo transatlántico: por un lado, una polarización interna estadounidense persistentemente alta; por otro, el intento de la nueva administración de reconstruir credibilidad exterior mediante un retorno al multilateralismo. En el plano institucional, la dinámica de obstrucción legislativa siguió siendo relevante, y el recurso a herramientas parlamentarias para sortear bloqueos sugiere un contexto político poco propicio a consensos estables (United States Senate, 2023, 2025b). En el plano social, varios sondeos mostraron una brecha partidista estable en apoyo a alianzas y a la defensa de aliados (Smeltz *et al.*, 2023).

Sobre ese telón de fondo, Biden apostó desde el inicio por señales claras de continuidad con los aliados: reingresó en el Acuerdo de París y trató de reactivar un lenguaje de compromiso con Europa (Ayuso, 2021). En la cumbre de la OTAN de junio de 2021, llegó a calificar el Artículo 5 como una «obligación sagrada», una formulación pensada para cerrar dudas sobre la garantía colectiva (Biden, 2021b). En términos constructivistas, estas señales importan porque buscan restaurar confianza y expectativas compartidas; en términos más materiales, pretenden reducir la incertidumbre estratégica que la etapa anterior había reintroducido.

Sin embargo, el mismo año mostró límites visibles. La retirada de Afganistán en agosto de 2021 —justificada por Biden como el cierre de una guerra demasiado larga— se ejecutó de forma caótica y con coordinación aliada percibida como insuficiente, lo que provocó críticas en Europa, especialmente desde Reino Unido y Alemania, y reabrió dudas sobre la fiabilidad práctica del liderazgo estadounidense (Biden, 2021a; Tovar Ruiz, 2022). Para los aliados europeos, la retirada erosionó la confianza en la coordinación transatlántica y reavivó una preocupación más estructural: depender de un garante cuya disposición puede variar con el tiempo y con la política interna, esa incertidumbre que Waltz asocia a la «sombra del futuro» (Waltz, 2001).

La invasión rusa de Ucrania en febrero de 2022 reordenó el panorama. La respuesta occidental reforzó de forma inmediata la coordinación transatlántica y, en el plano doctrinal, el nuevo Concepto Estratégico de la OTAN aprobado en Madrid definía Rusia como principal amenaza y, por primera vez, incluyó a China como desafío sistémico, alineándose con prioridades estratégicas que Washington venía enfatizando (NATO, 2022). En paralelo, líderes europeos insistieron en una idea que se volvería recurrente: una defensa europea más fuerte no compite con la OTAN, sino que la refuerza (Scholz, 2022; von der Leyen, 2022; Macron, 2023). Esa formulación es relevante porque permite sostener, a la vez, cohesión aliada y margen de iniciativa europea.

Pese al discurso de unidad, los datos sugieren una Alianza desigual: en 2024, 18 de 32 miembros alcanzaron el 2 % del PIB en defensa, y solo una parte de ellos se encuentra en la primera línea fronteriza con Rusia (SIPRI, 2024). Esto ayuda a explicar por qué, incluso en un contexto de refuerzo atlántico, la UE aceleró instrumentos propios. El Fondo Europeo de Defensa operó como palanca para financiar proyectos conjuntos y reducir dependencias tecnológicas (EDA, 2022); la Brújula Estratégica fijó una hoja de ruta para capacidad de acción y lectura común de amenazas (Consejo de la Unión Europea, 2022) y la misión EUMAM Ucrania tradujo el apoyo político en entrenamiento y sostenimiento militar (EEAS, 2022).

El periodo deja, así, una imagen mixta pero coherente: la administración Biden buscó reconstruir previsibilidad y confianza con Europa, y la guerra de Ucrania reforzó de hecho la alianza. Al mismo tiempo, la persistencia de polarización y la memoria reciente de episodios como Afganistán mantuvieron viva la percepción europea de vulnerabilidad ante futuros giros en Washington. Desde

una lente neorrealista, eso favorece inversiones en capacidades propias como forma de reducir dependencia; desde una lente constructivista, consolida una narrativa europea de responsabilidad y autonomía compatible —al menos en el discurso— con la pertenencia a la OTAN.

5 Conclusiones

Este capítulo ha explorado una intuición sencilla, pero difícil de medir con precisión: cuando la polarización política y social aumenta en Estados Unidos, su capacidad para sostener una política exterior estable y previsible hacia Europa puede verse sometida a más presión y, ante esa incertidumbre, la Unión Europea tiende a pensar con más seriedad en cómo reducir dependencias sin romper el vínculo transatlántico. El recorrido 2001-2024 sugiere que la polarización no actúa como un «motor único» de la relación transatlántica, pero sí puede operar como un factor que amplifica oscilaciones y hace más costosa la continuidad estratégica entre administraciones, especialmente cuando la política exterior se convierte en un terreno de disputa interna.

Una primera conclusión es que el efecto más relevante de la polarización no siempre se observa en decisiones aisladas, sino en la percepción de continuidad. Incluso cuando Estados Unidos mantiene compromisos materiales con Europa, la previsibilidad depende de si esos compromisos parecen políticamente sostenibles en el tiempo. Cuando el debate interno se vuelve más confrontativo, aumentan los incentivos a utilizar la política exterior como señal doméstica, y eso puede traducirse en mensajes contradictorios, cambios de énfasis o decisiones más fácilmente reversibles. Para Europa, que basa buena parte de su seguridad en expectativas de respaldo a medio y largo plazo, el problema no es solo qué hace Washington hoy, sino qué es razonable esperar que mantenga mañana.

La segunda conclusión es que esta dinámica opera en dos planos complementarios. En el plano estadounidense, la polarización puede estrechar márgenes de consenso y dificultar políticas exteriores con vocación de permanencia. En el plano europeo, lo decisivo es cómo se interpretan esas señales: la confianza aliada se apoya tanto en capacidades como en expectativas, y las expectativas se alteran cuando el compromiso se percibe como más contingente, más sujeto al ciclo político interno o a giros entre administraciones. Por eso, el análisis no apunta tanto a un dete-

rioro lineal del vínculo como a una relación que se vuelve más sensible a cambios de tono, prioridades y credibilidad.

La tercera conclusión es que las iniciativas europeas asociadas a la autonomía estratégica encajan mejor si se entienden como adaptación y no como ruptura. A lo largo del periodo analizado, Europa no ha buscado una sustitución del paraguas atlántico; más bien ha tratado de ampliar márgenes propios para responder a escenarios en los que el respaldo estadounidense pueda volverse menos claro, más condicionado o más variable. En esa lógica, instrumentos como PESCO, el Fondo Europeo de Defensa o la Brújula Estratégica pueden leerse como intentos de reforzar capacidades, coordinación e industria, sin asumir que eso implique un «divorcio» transatlántico. El matiz es importante: la autonomía aparece como un seguro ante incertidumbre, no como una declaración de independencia.

La cuarta conclusión introduce un límite necesario: la polarización, por sí sola, no determina el estado del vínculo. El contexto internacional puede reforzar la cohesión aliada incluso cuando la polarización es elevada. La invasión rusa de Ucrania en 2022 mostró que, ante una amenaza directa, la coordinación transatlántica puede intensificarse y recuperar reflejos de cooperación, lo que obliga a leer con cuidado cualquier explicación mono causal. En ese sentido, el efecto de la polarización parece depender de condiciones mediadoras: el tipo de crisis, la urgencia percibida, el liderazgo político disponible y la capacidad institucional para sostener un curso de acción más allá de una administración concreta.

Esta idea conecta con la evolución 2021-2024: el vínculo se recompone en el discurso y se fortalece frente a la amenaza rusa, pero convive con dudas sobre la previsibilidad a largo plazo. La polarización interna no bloqueó la acción exterior de la administración Joe Biden, pero podría haber limitado la sensación de continuidad estratégica que Europa necesita para confiar sin reservas. La respuesta europea, como sugiere el cierre del apartado anterior, ha sido dual: apoyarse en Estados Unidos cuando la urgencia lo exige y, al mismo tiempo, seguir construyendo capacidades y mecanismos propios para no depender por completo de la estabilidad política de Washington.

En conjunto, el capítulo no «cierra» una relación causal definitiva, pero sí ofrece una lectura plausible: cuando aumenta la incertidumbre sobre la continuidad del compromiso estadounidense

—y la polarización es una de las condiciones que pueden alimentarla— se refuerzan los incentivos europeos a reducir vulnerabilidades. Esto no elimina la centralidad del vínculo transatlántico, pero ayuda a entender por qué el debate sobre autonomía estratégica ha ganado espacio en la agenda europea y por qué es probable que no desaparezca, aunque varíen las circunstancias inmediatas. La cuestión de fondo, en última instancia, no es si Europa deja de contar con Estados Unidos, sino cómo ajusta su seguridad para que esa dependencia sea más gestionable en un entorno donde la política doméstica del socio principal puede introducir más incertidumbre que en etapas anteriores.

Bibliografía

Adler, E. y Barnett, M. (1998). *Security Communities*. Cambridge, Cambridge University Press.

Aguirre, M. y Morales Bertrand, C. (2024). El incierto «día después» de la guerra en Gaza [en línea]. afkar/ideas. N.º 71, pp. 16-19. [Consulta: 2025]. Disponible en: https://www.politicaexterior.com/wp-content/uploads/2024/04/5Aguirreesp.pdf

Alcaro, R. (2020). Ideology, Not Strategy, Explains the US Troop Withdrawal from Germany [en línea]. IAI Commentaries. 20(56). [Consulta: 2025]. Disponible en: https://www.iai.it/sites/default/files/iaicom2056.pdf

Arteaga, F. y Simón, L. (2023). La OTAN tras la Cumbre de Vilna [en línea]. ARI 74/2023. Real Instituto Elcano. [Consulta: 2025]. Disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2023/07/ari74-arteaga-simon-la-otan-tras-la-cumbre-de-vilna-1.pdf

Axelrod, R., Daymude, J. J. y Forrest, S. (2021). Preventing extreme polarization of political attitudes [en línea]. Proceedings of the National Academy of Sciences. 118(50). [Consulta: 2024]. Disponible en: https://pnas.org/doi/full/10.1073/pnas.2102139118

Ayuso, A. (2021). La agenda exterior de Biden y sus implicaciones para la Unión Europea y América Latina [en línea]. Relaciones Internacionales. 30(60), pp. 265-274. [Consulta: 2026]. Disponible en: https://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S2314-27662021000100265

Benedicto Solsona, M. Á. (2018). Trump y su Estrategia de Seguridad Nacional una «contradictio in terminis» [en línea]. Boletín del Instituto Español de Estudios estratégicos. N.º 9, pp. 403-413. [Consulta: 2025]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6467945

Bernaerts, K., Blanckaert, B. y Caluwaerts, D. (2023). Institutional design and polarization. Do consensus democracies fare better in fighting polarization than majoritarian democracies? [en línea]. Democratization. 30(2), pp. 153-172. [Consulta: 2024]. Disponible en: https://www.tandfonline.com/doi/full/10.1080/13510347.2022.2117300

Biden, J. R. (2021a). Remarks by President Biden on the Way Forward in Afghanistan [en línea]. The White House. [Consulta: 2025]. Disponible en: https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2021/04/14/remarks-by-president-biden-on-the-way-forward-in-afghanistan/

—. (2021b). Remarks by US President Joe Biden and NATO Secretary General Jens Stoltenberg at their meeting in the Oval Office [en línea]. NATO. [Consulta: 2025]. Disponible en: http://www.nato.int/cps/en/natohq/opinions_184847.htm

—. (2023). Remarks by President Biden Ahead of the One-Year Anniversary of Russia's Brutal and Unprovoked Invasion of Ukraine [en línea]. The White House. [Consulta: 2025]. Disponible en: https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2023/02/21/remarks-by-president-biden-ahead-of-the-one-year-anniversary-of-russias-brutal-and-unprovoked-invasion-of-ukraine/

Bloethe, D. W. (2021). The effects of political polarization on american foreign policy [trabajo fin de máster] [en línea]. Johns Hopkins University. [Consulta: 2024]. Disponible en: https://jscholarship.library.jhu.edu/server/api/core/bitstreams/2044a47f-ad0c-4cf9-93f1-389e502c9cea/content

Bogren, K. (2007). Fighting evil or evil fighting? : a constructive analysis of the Bush administrations "war on terror" [trabajo fin de grado] [en línea]. Lunds University. [Consulta: 2025]. Disponible en: https://lup.lub.lu.se/student-papers/search/publication/1320955

Borg, S. (2024). "A Battle for the Soul of This Nation": How Domestic Polarization Affects US Foreign Policy in Post-Trump America [en línea]. International Journal: Canada's Journal of Global Policy Analysis. 79(1), pp. 22-39. [Consul-

ta: 2024]. Disponible en: https://journals.sagepub.com/doi/10.1177/00207020241232986

Borrell, J. (2020). Por qué es importante la autonomía estratégica europea [en línea]. Servicio Europeo de Acción Exterior. [Consula: 2025]. Disponible en: https://www.eeas.europa.eu/eeas/por-qu%C3%A9-es-importante-la-autonom%C3%A-Da-estrat%C3%A9gica-europea_es

Bouton, M. M. et al. (2010). Constrained Internationalism: Adapting to New Realities. Results of a 2010 National Survey of American Public Opinion. Global Views 2010 [en línea]. The Chicago Council on Global Affairs. [Consulta: 2025]. Disponible en: https://globalaffairs.org/sites/default/files/2020-11/Global%20Views%202010.pdf

Carmines, E. G. y Fowler, M. (2017). The Temptation of Executive Authority: How Increased Polarization and the Decline in Legislative Capacity Have Contributed to the Expansion of Presidential Power [en línea]. Indiana Journal of Global Legal Studies. 24(2), pp. 369-397. [Consulta: 2025]. Disponible en: https://muse.jhu.edu/article/678118

Chestnoy, S. y Gersinkova, D. (2017). USA Withdrawal from Paris Agreement – What Next? [en línea]. International Organisations Research Journal. 12(4), pp. 215-225. [Consulta: 2025]. Disponible en: https://iorj.hse.ru/en/2017-12-4/212736131.html

Colomer Calsina, J. M. (2023). La polarización política en Estados Unidos. Barcelona, DEBATE.

Comisión Europea. (2025). EU countermeasures on US steel and aluminium tariffs explained [en línea]. [Consulta: 2025]. Disponible en: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_25_750/QANDA_25_750_EN.pdf

Consejo de la Unión Europea. (2022). A Strategic Compass for Security and Defence [en línea]. [Consulta: 2024]. Disponible en: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

Contreras Peralta, J. (2023). La política exterior de Joe Biden: el poder inteligente en la competencia de las grandes potencias [en línea]. Revista de Relaciones Internacionales de la UNAM. N.º 147, pp. 79-107. [Consulta: 2026]. Disponible en:

https://investigacion.politicas.unam.mx/rri/wp-content/uploads/articulos/147/rri147.pdf

Coppedge, M. et al. (2021). V-DEM Dataset v11.1 [en línea]. V-DEM Working Paper forthcoming. SSRN. [Consulta: 2025]. Disponible en: https://ssrn.com/abstract=3831905

Cózar Murillo, B. (2022). PESCO as a Game-Changer for Differentiated Integration in CSDP after Brexit [en línea]. European Papers. 7(3), pp. 1303-1324. [Consulta: 2025]. Disponible en: https://www.europeanpapers.eu/en/e-journal/pesco-game-changer-differentiated-integration-csdp-after-brexit

Cronberg, T. (2017). No EU, no Iran deal: the EU's choice between multilateralism and the transatlantic link [en línea]. The Nonproliferation Review. 24(3-4), pp. 243-259. [Consulta: 2025]. Disponible en: https://www.tandfonline.com/doi/full/10.1080/10736700.2018.1432321

Daniels, L. von (2024). Economy and national security: US foreign economic policy under Trump and Biden [en línea]. SWP Research Paper. Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs. [Consulta: 2025]. Disponible en: https://www.swp-berlin.org/10.18449/2024RP11/

Demczuk, A. M. (2023). Biden's Soft Power vs. Coercive Diplomacy and Responding to Russia's Invasion of Ukraine [en línea]. Teka Komisji Politologii i Stosunków Międzynarodowych. 17(1), pp. 7-21. [Consulta: 2025]. Disponible en: https://journals.umcs.pl/teka/article/view/13570

Deni, J. R. (2015). The Real Rebalancing: American Diplomacy and The Tragedy of President Obama's Foreign Policy [en línea]. US Army War College Press. [Consulta: 2025]. Disponible en: https://press.armywarcollege.edu/monographs/440

Dombrowski, P. y Reich, S. (2017). Does Donald Trump have a grand strategy? [en línea]. International Affairs. 93(5), pp. 1013-1037. [Consulta: 2025]. Disponible en: http://academic.oup.com/ia/article/93/5/1013/4098313

Dowdall, J. (2011). Reflections on the Status and Future of the Transatlantic Alliance [en línea]. Security & Defence Agenda. [Consulta: 2025]. Disponible en: https://www.files.ethz.ch/isn/130842/GATES_Report_final.pdf

EDA. (2022). European Defence Fund (EDF) [en línea]. [Consulta: 2025]. Disponible en: https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf)

— (2024). Coordinated Annual Review on Defence (CARD) [en línea]. [Consulta: 2025]. Disponible en: https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card)

EEAS. (2017a). Coordinated Annual Review on Defence [en línea]. [Consulta: 2025]. Disponible en: https://www.eeas.europa.eu/sites/default/files/coordinated_annual_review_on_defence_card_factsheet.pdf

— (2017b). Remarks by High Representative/Vice-President Federica Mogherini following the Ministerial Meeting of the E3/EU + 3 and Iran [en línea]. [Consulta: 2025]. Disponible en: https://www.eeas.europa.eu/node/32546

—. (2022). EU Military Assistance Mission in support of Ukraine [en línea]. [Consulta: 2025]. Disponible en: https://www.eeas.europa.eu/eumam-ukraine_en?s=410260

Finnemore, M. y Sikkink, K. (1998). International Norm Dynamics and Political Change [en línea]. International Organization. 52(4), pp. 887-917. [Consulta: 2025]. Disponible en: https://www.cambridge.org/core/product/identifier/S0020818398440608/type/journal_article

Friedrichs, G. M. y Tama, J. (2022). Polarization and US foreign policy: key debates and new findings [en línea]. International Politics. 59(5), pp. 767-785. [Consulta: 2024]. Disponible en: https://link.springer.com/10.1057/s41311-022-00381-0

García, D. (2012). La «Doctrina Obama», la teoría de la «Guerra Limitada» y la nueva política exterior de EEUU: ¿hacia una política neo-Nixoniana? [en línea]. UNISCI Discussion Papers. N.º 28, pp. 145-153. [Consulta: 2025]. Disponible en: https://www.redalyc.org/pdf/767/76724473012.pdf

García, J. (2016). La Unión Europea y la OTAN en el marco de la nueva Estrategia Global de Seguridad de la Unión Europea [en línea]. Revista UNISCI. N.º 42, pp. 217-239. [Consulta: 2025]. Disponible en: http://revistas.ucm.es/index.php/RUNI/article/view/53794

Graham, L. (2017). Historic Moment For U.S.-NATO Relationship [en línea]. Lindsey Graham Press Releases. [Consulta: 2025]. Disponible en: https://www.lgraham.senate.gov/public/index.cfm/2017/6/historic-moment-for-u-s-nato-relationship

Grevi, G., Helly, D. y Keohane, D. (2009). European security and defence policy: the first ten years (1999-2009) [en línea]. París, European Union Institute for Security Studies. [Consul-

ta: 2025]. Disponible en: https://www.iss.europa.eu/sites/default/files/EUISSFiles/ESDP_10-web.pdf

Guinea, M. (2018). La política exterior de Estados Unidos hacia Europa. Cambios y continuidades de Obama a Trump [en línea]. UNISCI Journal. 16(48), pp. 61-90. [Consulta: 2025]. Disponible en: http://www.unisci.es/la-politica-exterior-de-estados-unidos-hacia-europa-cambios-y-continuidades-de-obama-a-trump/

Hamilton, D. (2015). TTIP's Geostrategic Implications [en línea]. National Security Benefits of Trade Agreements with Asia and Europe. Washington D.C., Johns Hopkins University, School of Advanced International Studies. [Consulta: 2025]. Disponible en: https://docs.house.gov/meetings/FA/FA18/20150317/103161/HHRG-114-FA18-Wstate-HamiltonD-20150317.pdf

Hillison, J. R. (2018). The Relevance of the European Union and the North Atlantic Treaty Organization for the United States in the 21st Century [en línea]. US Army War College Press. [Consulta: 2025]. Disponible en: https://press.armywarcollege.edu/monographs/392

Hunter, R. E. (2002). The European Security and Defense Policy: NATO's Companion - or Competitor? [en línea]. Santa Monica, RAND Corporation. [Consulta: 2025]. Disponible en: https://www.rand.org/pubs/monograph_reports/MR1463.html

Igwe, A. U. y Ugwuja, A. A. (2015). The United States and Global Agenda-Setting on Security- An Assessment of the Impact of the 'Bush Doctrine' on the International System 2002 – 2012 [en línea]. *International Journal of Research*, 02(05). [Consulta: 2025].

Iyengar, S., Sood, G. y Lelkes, Y. (2012). Affect, Not Ideology [en línea]. Public Opinion Quarterly. 76(3), pp. 405-431. [Consulta: 2025]. Disponible en: https://academic.oup.com/poq/article-abstract/76/3/405/1894274?redirectedFrom=fulltext

Jacobson, G. C. (2011). The Republican Resurgence in 2010 [en línea]. Political Science Quarterly. The Academy of Political Science. 126(1), pp. 27-52. [Consulta: 2025]. Disponible en: https://www.jstor.org/stable/23056913

Jervis, R. (1978). Cooperation Under the Security Dilemma [en línea]. World Politics. 30(2), pp. 167-214. [Consulta: 2025]. Disponible en: https://www.jstor.org/stable/2009958

Kaminski, J. J. (2019). Rethinking Realism and Constructivism Through the Lenses of Themes and Ontological Primacy [en línea]. Croatian International Relations Review. 25(85), pp. 6-29. [Consulta: 2025]. Disponible https://www.researchgate.net/publication/337480816_Rethinking_Realism_and_Constructivism_Through_the_Lenses_of_Themes_and_Ontological_Primacy_-_Introduction-Integrative_Pluralism_and_21st_Century_International_Relations_Theorising

Katzenstein, P. J. (ed.). (1996). *The culture of national security: norms and identity in world politics*. Nueva York, Columbia Univ. Press.

Kirdin, Ş. E. (2017). A Neo-Realist Case Study of U.N.-Authorized Humanitarian Interventions in The Post Cold War World [en línea]. Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. 2(19), pp. 615-632. [Consulta: 2025]. Disponible en: https://dergipark.org.tr/en/download/article-file/459328

Lacatus, C. y Blanc, E. (2023). Diplomacy of Hope: Transatlantic Relations in the Transition from Trump to Biden [en línea]. Foreign Policy Analysis. 19(4). [Consulta: 2025]. Disponible en: https://academic.oup.com/fpa/article/19/4/orad026/7264757

Leyen, U. von der (2022). State of the Union Address by President von der Leyen [en línea]. European Commission. [Consultado: 2025]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_5493

Lieberman, R. C. (2009). The Politics of United States Foreign policy under Barack Obama [en línea]. Revista de Ciencia Política. 29(3), pp. 829-845. [Consulta: 2025]. Disponible en: https://scispace.com/pdf/the-politics-of-united-states-foreign-policy-under-barack-1f1sf0ff17.pdf

Löfflmann, G. (2022). 'Enemies of the people': Donald Trump and the security imaginary of America First [en línea]. The British Journal of Politics and International Relations. 24(3), pp. 543-560. [Consulta: 2025]. Disponible en: 'Enemies of the people': Donald Trump and the security imaginary of America First - Georg Löfflmann, 2022

Macron, E. (2023). Conferencia anual de los embajadores - Discurso del Presidente Emmanuel Macron. La France au Salvador [en línea]. République Fraçaise. [Consulta: 2025]. Disponible en: https://sv.ambafrance.org/Conferencia-anual-de-los-embajadores-Discurso-del-Presidente-Emmanuel-Macron

Makeschin, S. (2015). Barack Obama, Europe and the Transatlantic Relationship: From the World's White Knight to the Spy that Came in from the Cold? A German Perspective [en línea]. COPAS-Current Objectives of Postgraduate American Studies. 16(1). [Consulta: 2025]. Disponible en: https://copas.uni-regensburg.de/index.php/copas/article/view/222

Market, D., Daalder, I. H. y Lindsay, J. M. (2003). America Unbound: The Bush Revolution in Foreign Policy [en línea]. Naval War College Review. 57(2). [Consulta: 2025]. Disponible en: https://digital-commons.usnwc.edu/nwc-review/vol57/iss2/12

Martí Sempere, C. (2024). Una revisión de la Colaboración Estructurada Permanente [en línea]. Real Instituto Elcano. [Consulta: 2025]. Disponible en: https://www.realinstitutoelcano.org/analisis/una-revision-de-la-colaboracion-estructurada-permanente/

Martin, G. J. y Sinkkonen, V. (2021). Transatlantic relations and European strategic autonomy in the Biden era: neglect, primacy or reform? [en línea]. FIIA briefing paper. N.º 301. [Consulta: 2025]. Disponible en: https://fiia.fi/wp-content/uploads/2021/02/bp301_us-and-european-strategic-autonomy_ville-sinkkonen-and-garret-martin.pdf

McCarthy, N. M., Rosenthal, H. y Poole, K. T. (2006). Polarized America: The Dance of Ideology and Unequal Riches [en línea]. Cambridge, MIT Press [Consulta: 2024]. Disponible en: https://www.researchgate.net/profile/Nolan-Mccarty/publication/23573640_Polarized_America_The_Dance_of_Ideology_and_Unequal_Riches/links/0deec5183c5fbdbeb6000000/Polarized-America-The-Dance-of-Ideology-and-Unequal-Riches.pdf

McCoy, J. et al. (2022). Reducing Pernicious Polarization: A Comparative Historical Analysis of Depolarization [en línea]. Carnegie Endowment for International Peace. [Consulta: 2025]. Disponible en: https://carnegie-production-assets.s3.amazonaws.com/static/files/McCoy_et_al_-_Polarization_final_3.pdf

Merkel, A. D. (2017). Angela Merkel warns Europe can no longer rely on old allies, US and Britain [en línea]. ABC. [Consulta: 2025]. Disponible en: https://www.abc.net.au/listen/programs/worldtoday/angela-merkel-warns-europe-can-no-longer-rely-on/8568690

Meto, S. (2019). Geo-political reasons behind the Transatlantic Trade and Investment Partnership (TTIP) from the viewpoint of the European Union [en línea]. Middle East Technical University. [Consulta: 2025]. Disponible en: https://www.proquest.com/openview/1506cb755a749d33200ded3c57298d1d/1?cbl=2026366&diss=y&pq-origsite=gscholar

NATO. (2022). NATO 2022 Strategic Concept [en línea]. [Consulta: 2026]. Disponible en: https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

Obama, B. (2009). Remarks by the President at Cairo University, 6-04-09 [en línea]. [Consulta: 2025]. Disponible en: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-Cairo-university-6-04-09

—. (2014). Remarks by the President on Review of Signals Intelligence [en línea]. [Consulta: 2025]. Disponible en: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

Pesu, M. y Sinkkonen, V. (2024). Trans-atlantic (mis)trust in perspective: asymmetry, abandonment and alliance cohesion [en línea]. Cambridge Review of International Affairs. 37(2), pp. 206-225. [Consulta: 2025]. Disponible en: https://www.tandfonline.com/doi/full/10.1080/09557571.2023.2225650

Powell, C. T. (2015). La política exterior y de seguridad de Barack Obama: ¿hacia un nuevo paradigma geopolítico estadounidense? [en línea]. Cuadernos de Estrategia. N.º 177, pp. 181-212. [Consulta: 2025]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5255548

Romano, S. (2024). Estados Unidos de América: cambios y continuidades de su política exterior. Breve análisis histórico y reflexiones sobre los gobiernos de Trump y Biden [en línea]. En: Arenal, L. et al. (eds.). Relaciones internacionales y geopolítica en tiempos de policrisis. Sevilla, Universidad Internacional de Andalucía. [Consulta: 2026]. Disponible en: https://dspace.unia.es/entities/publication/6b8d3c7a-866f-4b0b-a6f9-9d153dec3695

Rose, G. (1998). Neoclassical Realism and Theories of Foreign Policy [en línea]. World Politics. 51(1), pp. 144-172. [Consulta: 2025]. Disponible en: https://muse.jhu.edu/article/36415

Rupérez, J. (2013). La política exterior de los Estados Unidos bajo Barack Obama: análisis y prospección [en línea]. Panorama Estratégico 2013. Ministerio de Defensa, IEEE, pp. 39-73. [Consulta: 2025]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4184251

Ryan, M. (2017). Bush the transnationalist: a reappraisal of the unilateralist impulse in US foreign policy, 2001–2009 [en línea]. International Politics. 54(5), pp. 561-582. [Consulta: 2025]. Disponible en: http://link.springer.com/10.1057/s41311-017-0054-8

Sazo Muñoz, D. (2009). Provocando el desequilibrio de poder: Crítica a la política exterior de George W. Bush desde la realpolitik [en línea]. Revista Enfoques, 7(10), pp. 293-311. [Consulta: 2025]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3020092

Schneider-Petsinger, M. (2019). US–EU Trade Relations in the Trump Era Which Way Forward? [en línea]. Chatham House. (US and the Americas Programme). [Consulta: 2025]. Disponible en: https://www.chathamhouse.org/sites/default/files/publications/research/2019-03-08US-EUTradeRelations2.pdf

Scholz, O. (2022). Policy statement by Olaf Scholz, Chancellor of the Federal Republic of Germany and Member of the German Bundestag, 27 February 2022 in Berlin, Website of the Federal Government [en línea]. Bundesregierung. [Consulta: 2025]. Disponible en: https://www.bundesregierung.de/breg-en/news/policy-statement-by-olaf-scholz-chancellor-of-the-federal-republic-of-germany-and-member-of-the-german-bundestag-27-february-2022-in-berlin-2008378

Schuette, L. A. (2023). Shaping institutional overlap: NATO's responses to EU security and defence initiatives since 2014 [en línea]. The British Journal of Politics and International Relations. 25(3), pp. 423-443. [Consulta: 2025]. Disponible en: https://journals.sagepub.com/doi/10.1177/13691481221079188?__cf_chl_f_tk=COP0Z_jK51yLXWTe3mYBOaXnSmX9ihZW.elLQxYd7_8-1782902960-1.0.1.1-NnRT7s1EXt.z_bVyaUrNpVzv030f7aVUWJVQYko3ZGA

Schweller, R. L. (2004). Unanswered Threats: A Neoclassical Realist Theory of Underbalancing [en línea]. International Security. 29(2), pp. 159-201. [Consulta: 2025]. Disponible en: https://direct.mit.edu/isec/article/29/2/159-201/11809

SIPRI. (2024). SIPRI Military Expenditure Database [en línea]. [Consulta: 2026]. Disponible en: https://www.sipri.org/databases/milex

Smeltz, D. (2022). Are we drowning at the water's edge? Foreign policy polarization among the US Public [en línea]. International Politics. 59(5), pp. 786-801. [Consulta: 2024]. Disponible en: https://link.springer.com/10.1057/s41311-022-00376-x

Smeltz, D. et al. (2017). Results of the 2017 Chicago Council Survey of American public opinion and US foreign policy [en línea]. The Chicago Cuncil on Global Affairs. [Consulta: 2025]. Disponible en: https://globalaffairs.org/research/public-opinion-survey/2020-chicago-council-survey

Smeltz, D. et al. (2023). A Cost of Conflict Americans Turn Inward. Results of the 2023 Chicago Council Survey of American Public Opinion and US Foreign Policy [en línea]. The Chicago Council on Global Affairs. [Consulta: 2025]. Disponible en: https://globalaffairs.org/research/public-opinion-survey/2023-survey-public-opinion-us-foreign-policy

Soare, S. R. (2021). Biden's Security Policy: Democratic Security or Democratic Exceptionalism? [en línea]. Intereconomics. 56(1), pp. 14-20. [Consulta: 2025]. Disponible en: http://link.springer.com/10.1007/s10272-021-0945-1

Svantesson, D. J. B. y Kloza, D. (eds.). (2017). Trans-Atlantic Data Privacy Relations as a Challenge for Democracy [en línea]. Cambridge, Intersentia. [Consulta: 2025]. Disponible en: https://www.cambridge.org/core/product/identifier/9781780685786/type/book

The White House. (2006). The National Security Strategy of the United States of America [en línea]. [Consulta: 2024]. Disponible en: https://history.defense.gov/Portals/70/Documents/nss/nss2006.pdf?ver=Hfo1-Y5B6CMl8yHpX4x-6IA%3d%3d

—. (2010). National Security Strategy [en línea]. [Consulta: 2024]. Disponible en: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

—. (2017). National Security Strategy [en línea]. [Consulta: 2024]. Disponible en: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

—. (2018). President Donald J. Trump Keeps His Promise To Open U.S. Embassy In Jerusalem, Israel [en línea]. [Consulta: 2025]. Disponible en: https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-keeps-promise-open-u-s-embassy-jerusalem-israel

—. (2022). National Security Strategy 2022 [en línea]. [Consulta: 2024]. Disponible en: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Thompson, K. y Thränert, O. (2017). Trump preparing to end Iran nuke deal [en línea]. Policy Perspectives. 5(4). [Consulta: 2025]. Disponible en: http://hdl.handle.net/20.500.11850/181637

Tovar Ruiz, J. (2020). La política europea de Trump y las relaciones transatlánticas [en línea]. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades. 22(45), pp. 474-498. [Consulta: 2025]. Disponible en: https://www.redalyc.org/journal/282/28268121021/html/

Tovar Ruiz, J. (2022). La paradoja de la política exterior de Joe Biden [en línea]. Revista CIDOB de Asuntos Internacionales N.º 132, pp. 195-220. [Consulta: 2025]. Disponible en: https://www.cidob.org/es/articulos/revista_cidob_d_afers_internacionals/132/la_paradoja_de_la_politica_exterior_de_joe_biden

Trump, D. J. (2017). Remarks by President Trump at NATO Unveiling of the Article 5 and Berlin Wall Memorials – Brussels, Belgium [en línea]. The White House. [Consulta: 2025]. Disponible en: https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-nato-unveiling-article-5-berlin-wall-memorials-brussels-belgium/

UK Prime's Minister Office. (2018). Joint statement from Prime Minister May, Chancellor Merkel and President Macron following President Trump's statement on Iran [en línea]. GOV.UK. [Consulta: 2025]. Disponible en: https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-chancellor-merkel-and-president-macron-following-president-trumps-statement-on-iran

Unión Europea. (2007). Tratado de Lisboa por el que se modifica el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea [en línea]. Diario Oficial de la Unión Europea. 17 de diciembre,C306/1. [Consulta: 2025].

Disponible en: https://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0008.01/DOC_19

—. (2017). Decisión (PESC) 2017/2315 del Consejo 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 [en línea]. Diario Oficial de la Unión Europea. 14 de diciembre, L331/57. [Consulta: 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017D2315

United States Senate. (2014). U.S. Senate: Cloture Motions - 113th Congress [en línea]. [Consulta: 2025]. Disponible en: https://www.senate.gov/legislative/cloture/113.htm

—. (2021). U.S. Senate: Cloture Motions - 116th Congress [en línea]. [Consulta: 2025]. Disponible en: https://www.senate.gov/legislative/cloture/116.htm

—. (2023). U.S. Senate: Cloture Motions - 117th Congress [en línea]. [Consulta: 2025]. Disponible en: https://www.senate.gov/legislative/cloture/117.htm

—. (2025a). U.S. Senate: About Filibusters and Cloture [en línea]. [Consulta: 2025]. Disponible en: https://www.senate.gov/about/powers-procedures/filibusters-cloture.htm

—. (2025b). U.S. Senate: Cloture Motions - 118th Congress [en línea]. [Consulta: 2025]. Disponible en: https://www.senate.gov/legislative/cloture/118.htm

—. (2025c). U.S. Senate: Glossary [en línea]. [Consulta: 2026]. Disponible en: https://www.senate.gov/about/research-tools/glossary.htm

Walt, S. M. (1985). Alliance Formation and the Balance of World Power [en línea] International Security. 9(4), pp. 3-43. [Consulta: 2025]. Disponible en: https://www.jstor.org/stable/2538540?origin=crossref

Waltz, K. N. (2001). *El hombre, el Estado y la guerra. Un análisis teórico*. Colección de Estudios Internacionales CIDE. CIDE.

Wendt, A. (2005). La anarquía es lo que los estados hacen de ella: la construcción social de la política de poder [en línea]. Relaciones Internacionales. N.º 1, pp. 1-47. [Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3155857

Whitmore, S. J. y Deni, J. R. (2013). NATO Missile Defense and the European Phased Adaptive Approach: The Implications of Burden Sharing and the Underappreciated Role of The U.S. Army [en línea]. US Army War College Press. [Consulta: 2025]. Disponible en: https://press.armywarcollege.edu/monographs/516

Xuereb, M. (2021). The Response of the EU to Major Shifts in US Foreign Policy in the Last Decade [trabajo fin de máster] [en línea]. Universidad de Malta, Instituto de Estudios Europeos. [Consulta: 2024]. Disponible en: https://www.um.edu.mt/library/oar/bitstream/123456789/90387/1/21MAPEL029.pdf

Capítulo sexto

Del *laissez faire* a la acción decidida.

La respuesta policial vasca al terrorismo etarra (1980-1993)

Diego Abel Redondo Olmedo

Resumen

Entre 1980 y 1993, la política pública antiterrorista del Gobierno Vasco experimentó una profunda transformación, especialmente en lo relativo al papel de la Policía Autónoma Vasca (Ertzaintza) como instrumento de seguridad autonómico en la lucha contra el terrorismo de ETA. Inicialmente, el Ejecutivo vasco adoptó una actitud de indiferencia hacia la organización terrorista, evitando el enfrentamiento directo en el delicado contexto de la Transición y priorizando la consolidación de su autogobierno. Sin embargo, diversos factores, desde los asesinatos de *ertzainas* y de ciudadanos vinculados al Partido Nacionalista Vasco (PNV), hasta los fracasos de sucesivos intentos de diálogo y un cambio en la postura de ETA respecto a la Ertzaintza, impulsaron un giro progresivo en la estrategia institucional.

A lo largo de cuatro legislaturas, la Ertzaintza pasó de ser un cuerpo incipiente, con funciones limitadas y frecuentemente al margen de la lucha contra el terrorismo, a desempeñar un papel operativo de cierta relevancia en la persecución de ETA, ganando legitimidad social y profesionalización.

Este artículo analiza dicha evolución entre 1980 y 1993, resaltando cómo se gestó una política pública en un entorno altamente complejo y polarizado y subrayando la importancia del contexto sociopolítico y de la interacción entre actores clave (Gobierno Vasco-PNV, Ertzaintza y la propia ETA) en la eficacia de la respuesta antiterrorista.

Palabras clave

Ertzaintza, ETA, Política pública, Policía Autónoma Vasca, Gobierno Vasco.

From laissez-faire to decisive action. The Basque police response to ETA terrorism (1980-1993)

Abstract

Between 1980 and 1993, the Basque Government changed its anti-terrorism policy a lot, especially about the role of the Basque Police (Ertzaintza) in the fight against ETA. At the beginning, the Basque Government didn't want to confront the terrorist group directly. During the Spanish Transition, it preferred to focus on building its own regional government. But many things made the government change its position: the killing of police officers (ertzainas), the murder of people from the Basque Nationalist Party (PNV), the failure of peace talks, and the change in ETA's attitude towards the Ertzaintza.

During four political periods, the Ertzaintza changed from a small police force with few responsibilities to an important part of the fight against ETA. It became more professional and gained more support from society.

This article looks at how the anti-terrorism policy changed between 1980 and 1993. It shows how difficult the situation was and how important the political and social context was. It also explains how the relationship between the Basque Government, the Ertzaintza, and ETA affected the success of the anti-terrorist actions.

Key words

Ertzaintza, ETA, Public policy, Basque Autonomous Police, Basque Government.

Lista de abreviaturas

AP	Alianza Popular
Art.	Artículo
ASK	Abertzale Sozialista Komiteak / Comités Socialistas Abertzales
AVCS	Adjuntos a la Viceconsejería de Seguridad
BBT Berroci	Berroci Berezi Taldea / Grupos Especiales de Berroci
BOE	Boletín Oficial del Estado
CDS	Centro Democrático y Social
EA	Eusko Alkartasuna / Solidaridad Vasca
EAJ-PNV	Euzko Alderdi Jeltzalea-Partido Nacionalista Vasco
EE	Euskadiko Eskerra / Izquierda del País Vasco
ErNE	Ertzainen Nazional Elkartasuna / Solidaridad Nacional de los Ertzainas
ETA	Euskadi Ta Askatasuna / Tierra Vasca y Libertad
ETA-pm	ETA-Político Militar
ETA-m	ETA-Militar
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
HB	Herri Batasuna / Unidad Popular
IA	Izquierda Abertzale
KAS	Koordinadora Abertzale Sozialista / Coordinadora Abertzale Socialista
LAB	Langile Abertzaleen Batzordeak / Comisiones de Obreros Abertzales
MLNV	Movimiento de Liberación Nacional Vasco
PAV	Policía Autónoma Vasca
PSE-PSOE	Partido Socialista de Euskadi-Partido Socialista Obrero Español
PSOE	Partido Socialista Obrero Español
SAS	Special Air Service / Servicio Aéreo Especial

STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
UCD	Unión de Centro Democrático

1 Introducción

El final de la dictadura franquista trajo consigo la recuperación de las instituciones vascas, las cuales se enfrentaron a un periodo de gran complejidad política e inseguridad en el País Vasco. Así, allá por 1980, se constituyó el primer Gobierno Vasco de la etapa autonómica, conformado por el Partido Nacionalista Vasco (PNV), y se dieron los primeros pasos para la reconstitución de la Policía Autónoma Vasca (PAV) como cuerpo policial propio de la comunidad.

La pervivencia de la organización terrorista *Euskadi ta Askatasuna* (ETA), activa desde 1958, se convirtió en uno de los mayores desafíos para las novísimas autoridades democráticas y, desde su inicio, la administración vasca se vio obligada a definir su política pública antiterrorista.

Desde esta manera, en 1980 comenzó una coexistencia ininterrumpida de ETA y la Ertzaintza, hasta la disolución de la organización terrorista en 2018. Estos dos «hermanos agnados», cuyos respectivos orígenes pueden situarse en el PNV, han moldeado la política antiterrorista en el País Vasco durante casi cuarenta años (Alfaro, 2022; El Correo, 1980; Sánchez y Simón, 2017).

Transcurridos casi ocho años desde la disolución oficial de ETA, resulta oportuno realizar una mirada retrospectiva que permita identificar y analizar los elementos clave de esa lucha, especialmente desde el ámbito de las políticas públicas.

A la vista de la situación planteada, el propósito de este artículo es, bajo el marco de la teoría de las políticas públicas, analizar cómo evolucionó la política antiterrorista del Gobierno Vasco contra ETA en el País Vasco, desde el ámbito policial, entre 1980, con los pasos previos para la reinstauración de la Ertzaintza en el periodo democrático, hasta finales de 1993, año en el que la organización terrorista asesinó al *ertzaina* Joseba Goikoetxea Asla. Esta acción puede considerarse como la primera en la que

ETA asesinaba, de manera premeditada, a un agente de la PAV, sin que existiera la «justificación» de la condición previa de la víctima como militar o miembro de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Analizar este periodo (1980-1993) permite valorar si las acciones del Gobierno Vasco atinentes a la aplicación de la política pública antiterrorista en su vertiente policial variaron en función del contexto político, social o legislativo de cada legislatura. Con este fin, es imprescindible examinar las relaciones entre los actores clave, identificados mediante el modelo del «triángulo de actores» propuesto por Knoepfel *et al.* (2007), adaptado según se observa en la figura 1. En el presente caso, se limita el estudio al Gobierno Vasco-PNV y a la Ertzaintza, en su rol de autoridades político-administrativas, y a ETA como el grupo-objetivo, excluyéndose los beneficiarios finales, esto es, la sociedad española en general y vasca en particular.

Metodológicamente, para analizar esta evolución de la política antiterrorista vasca se ha adoptado un enfoque cualitativo basado en un análisis exhaustivo de fuentes primarias apoyado por la triangulación de información para suplir la carencia de fuentes académicas.

Por último, se ha empleado la denominada triangulación temporal para estudiar el problema en diferentes momentos a lo largo del tiempo, concretamente las primeras cuatro legislaturas con ejecutivos peneuvistas en el Gobierno autonómico, con el objetivo de identificar los distintos cambios, tendencias y patrones temporales.

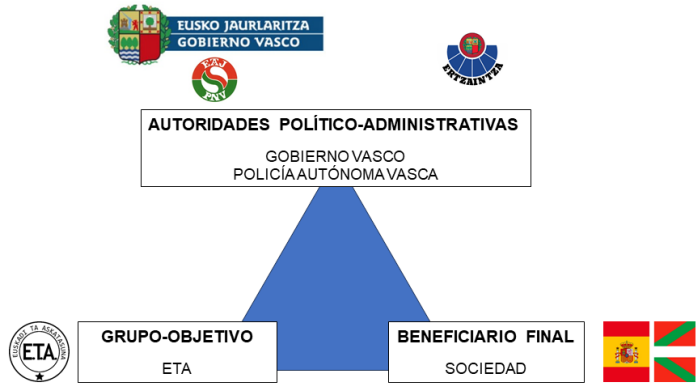
2 I Legislatura (1980-1984). Nacimiento de la Ertzaintza y pasividad inicial

2.1 El papel del PNV

A la hora de enfrentar la reconstitución de la Ertzaintza, el Gobierno Vasco apostó por modelos como el inglés o el canadiense (Arroyo, 2022; Rioja, 2022; Vasco Press 520, citado en Fernández *et al.*, 2021). Este modelo policial «amable» pudiera parecer improcedente en un tiempo convulso marcado por la violencia, especialmente en el País Vasco; no obstante, no se debe obviar que, en aquellos años, el Gobierno Vasco mostraba una concepción muy distorsionada de la violencia terrorista. El viceconsejero de Interior, Elí Galdós, llegó a decir en una entrevista en mayo de 1980 que ETA, y por ende su violencia, era una respon-

sabilidad de la política dictada desde «Madrid» para el País Vasco, primero durante la dictadura franquista y, en aquel momento, bajo el Gobierno de la Unión de Centro Democrático (UCD) del presidente Adolfo Suárez (Ere, 1980, citado en Fernández *et al.*, 2021: 537).

En consonancia con lo anterior, la política pública antiterrorista establecida por el Gobierno Vasco era clara y se resumía en evitar



cualquier actuación contra ETA. En palabras de Ángel Abásolo, director de Seguridad del Gobierno Vasco, en agosto de 1981, «nosotros [Gobierno Vasco] no vamos a hacer nada concreto contra ETA porque tenemos una misión distinta a cubrir» (Balantx, 1982: 11). En su idealismo, llegaban a creer que la pacificación del País Vasco se produciría de forma natural, llegando a ligar el fin de la violencia con la mejora de la situación económica, la reducción del paro y una mayor autonomía para la comunidad autónoma.

Asimismo, la forma de captación de las primeras promociones del cuerpo, entre los afines al partido, cuestión recurrentemente negada, permitió al Gobierno Vasco y al propio PNV conformar «una auténtica policía política al servicio del partido» (Fernández *et al.*, 2021: 533; Dávila, 2006). La mejor muestra de ello es que entre los primeros agentes, tanto *berrocis*[1] como de las promo-

[1] Denominación recibida al haberse adiestrado en la localidad alavesa del mismo nombre. El adiestramiento de esos primeros agentes la llevaron a cabo miembros del

ciones iniciales, salvo excepciones, muchos contaban con plena confianza de los mandos políticos (El Correo, 1980; Alfaro, 2022).

Sin embargo, a pesar de esa imagen pública ofrecida por el Gobierno Vasco, en su fuero interno era consciente del problema que podría suponer ETA. En el segundo semestre de 1982, publicaciones como *Punto y Hora de Euskal Herria* y *Tiempo* se hicieron eco de la filtración de un supuesto informe de la Consejería de Interior del Gobierno Vasco en el que se enumeraban como cometidos de los *ertzainas* la «lucha contra la droga, orden público y sobre todo ayudar a los berrocis en la lucha antiterrorista» (Tiempo, 1982, citado en Balantx, 1982: 12).

Este presunto informe mencionaría que, una vez suplidas las carencias de personal y material, la PAV podría enfrentarse a ETA y acabar con la organización terrorista sin ayuda de las FCSE, para lo que sería imprescindible el trabajo del «Gobierno Vasco, [de] la gente del PNV» (Balantx, 1982: 12).

Esta filtración generó una gran polémica, sobre todo por esa especial participación de la «gente del PNV» en la lucha contra ETA. Ante esa circunstancia, cargos de relevancia del PNV como el consejero de Interior José Luis Retolaza o el senador Joseba Azkarraga[2] realizaron diversas matizaciones, afirmando que sería la PAV quien debería llevar la responsabilidad de la lucha contra ETA, si bien apoyándose en toda la sociedad vasca, no solo en los militantes del PNV.

En consecuencia, la PAV sí tendría una labor contra ETA, y de ello era consciente el Gobierno Vasco desde 1980, cuando en una reunión con representantes del Gobierno estatal, Luis Retolaza, más explícito que en sus declaraciones de 1982, comentó que su idea de política antiterrorista se basaba en «combinar la acción psicológica y la acción disuasoria» (Vasco Press, 1992b: 10).

En esta legislatura, incluso se produjo la remisión del conocido como «dossier Arístegui[3]», recibido por el Ministerio del Interior desde la Consejería y que incluía datos concretos de la localiza-

ejército británico, en concreto el Special Air Force (SAS) (Alfaro, 2022; Rioja, 2022).

[2] El Consejero de Interior afirmó que «es ridículo pensar que sólo las bases del PNV deben colaborar […] con la Policía Autónoma para luchar contra ETA, porque es una labor que compete a todo el pueblo vasco»; mientras que el senador Azkarraga comentó que «debe ser la Policía Autónoma y no nuestros militantes los que realicen esa labor, aunque nosotros prestemos nuestra colaboración» (Balantx, 1982: 12).

[3] En referencia al gobernador civil en Gipuzkoa, Pedro Manuel de Arístegui, quien actuó como intermediario.

ción de diversos comandos en el País Vasco. En cualquier caso, no se trataba de un alarde de españolidad de Retolaza, sino de un intento para que ETA no les perjudicara su proyecto de «construcción nacional» (Díaz Herrera y Durán, 2002).

En definitiva, dejando al margen estas ambigüedades, el baño de realidad lo provocaron acontecimientos como el robo en las dependencias de la PAV en febrero de 1983, que se describirá en los siguientes apartados, que puso de manifiesto que ese modelo a semejanza de los *bobbies* era «inaplicable en un País Vasco, donde los terroristas estaban crecidos y robaban las armas a la Policía» (Domínguez, 2009). Esta acción provocó que miembros del Gobierno Vasco fuesen conscientes del grave problema que suponía ETA, afirmando que «se trataba del ataque más directo contra las instituciones vascas», en palabras del consejero de Interior Luis Retolaza; o que, con esta forma de actuar, «ETA-m[4] se enfrentaba al pueblo», según el *lehendakari* Carlos Garaikoetxea (El Correo, 1983c: 13; 1983d: 13).

2.2 El papel de la Ertzaintza

Tras su reconstitución, la Ertzaintza no asumió, entre sus competencias y funciones, la lucha contra el terrorismo. De esta manera, al menos al inicio, no se tuvo que dotar de estructuras específicas para luchar contra ETA.

Sin embargo, acciones terroristas como la perpetrada en febrero de 1983 contra las instalaciones de la PAV en la Diputación de Gipuzkoa permitieron constatar que en ningún caso ETA iba a mantener una displicencia total hacia la Ertzaintza.

En esta época, en torno al año 1983, la PAV se vio en la necesidad de establecer estructuras que, aun no reconocidas oficialmente, pudieran desarrollar ciertas investigaciones relacionadas con ETA. Así surgió el grupo Ekintza[5], el cual puede considerarse como el «embrión de un equipo especializado en la investigación y repre-

[4] En el presente artículo, todas las referencias que se realicen a ETA, siempre que se haga a hechos concretos perfectamente datados posteriores a 1982, deben entenderse realizadas a ETA-Militar (ETA-m).

[5] Palabra en vasco que significa «acción» y la cual era empleada igualmente por ETA para hacer referencia a sus acciones terroristas. En relación con el grupo creado dentro de la PAV, sus funciones también recibieron críticas, ya que se les acusó de investigar a todos los aspirantes para ingresar este cuerpo policial durante los primeros años (Vasco Press, 1992e).

sión del terrorismo», y que estaba formado por «unas docenas» de *ertzainas* encabezadas por Genaro García de Andoáin quien, en ese mismo momento, se encontraba ejerciendo funciones de interlocutor en las negociaciones ETA-PNV (Díaz Herrera y Durán, 2002; Méndez, 1986: 8).

Por otro lado, el asalto perpetrado contra la Diputación de Gipuzkoa sacó a la luz un grave problema al que se enfrentaba esa novísima Ertzaintza: la infiltración de miembros de ETA entre sus filas. Para materializar esta acción, el comando terrorista requirió la colaboración de un policía autonómico de la primera promoción, José Ignacio de Juana Chaos quien, tras huir, continuaría su militancia con una sangrienta trayectoria terrorista (M. P., 2008; Domínguez, 2009).

Este hecho no fue una excepción en esta época ya que, en estas primeras promociones, ETA logró introducir numerosos infiltrados en las filas de las Ertzaintza[6]. José María Lizarraga Goicoechea, Jesús María Bastarrica Munduate, Juan Manuel Pumar[7] Méndez, Federico Fernández de Jáuregui, José Miguel Sueskun, Jesús Guergue y Santos Berganza Cendegui son solo algunos ejemplos (Domínguez, 2022b; El Correo, 1983a; Yoldi, 1989).

2.3 El papel de ETA

La puesta en marcha de la PAV no supuso un cambio sustancial en la estrategia de ETA ya que, como se adelantó anteriormente, el nuevo cuerpo policial no desarrollaba cometidos relacionados con la lucha antiterrorista y, en aquel momento, los *ertzainas* no entraban dentro del proceso de *targeting*[8] de la organización terrorista.

[6] Entre estos infiltrados no se contabiliza a Pedro María Briones Goicoechea, ya que, tras colaborar con ETA desde 1979, conformando a partir de 1983 el comando *Bianditz* y participando en el asesinato de un policía nacional en San Sebastián, abandonó la organización terrorista e ingresó en la PAV. Briones fue detenido en 1986 (Domínguez, 2022b).

[7] En otras fuentes el apellido se escribe como «Pomar» o «Fumar».

[8] Empleando terminología militar, el término *targeting* puede traducirse como «selección de blancos» y debe centrarse exclusivamente en aquellos cuyo acometimiento proporcione ventaja en la campaña militar (Bueno Fernández, 2020). En el contexto de este artículo, debe entenderse este proceso de *targeting* como la selección de blancos que realizaba la organización terrorista y cuya neutralización coadyuvaba a cumplir los objetivos de la estrategia marcada en cada momento por la Dirección de ETA.

ETA lo reconocía de forma pública cuando, en enero de 1980[9], difundió un comunicado en el que enfatizó su compromiso de no atacar a la «Policía Autóctona», si bien en la medida en que este cuerpo respetase los intereses populares de *Euskadi*, lo que no puede sino interpretarse como los intereses de la propia organización terrorista. Asimismo, este comunicado finalizaba amenazando a todos aquellos supuestos infiltrados en las instituciones municipales o provinciales vascas (ETA, 1980).

A pesar de este aparentemente «tranquilizador» comunicado hacia la PAV, en agosto de 1981 la policía francesa incautó a la organización terrorista diversos documentos en los que se incluía, entre otras cuestiones, el nombre del, por aquel entonces, superintendente de la Ertzaintza, Díaz Arcocha (El Diario Vasco, 1985, citado en Fernández *et al.*, 2021). El *ertzaina*, antiguo militar, fue finalmente asesinado por ETA en marzo de 1985.

Asimismo, esta presunta inmunidad no implicaba que, para satisfacer sus necesidades operativas y, en sus propias palabras, realizar «abastecimiento y requisa de armamento» (ETA, 1983; El Correo, 1983b), ETA no pudiera incluir entre sus *targets* a instalaciones de la PAV. Así, durante la primera legislatura del recién estrenado Gobierno Vasco, ETA realizó una de sus acciones más audaces, cuando un comando asaltó el 28 de febrero de 1983 las dependencias de la Ertzaintza en la Diputación de Gipuzkoa y se apoderó de más de un centenar de pistolas, munición, uniformes, equipos de comunicaciones, etc. (M. P., 2008; Domínguez, 2009).

El asalto, aparte de poner en duda el modelo policial que propugnaba el Gobierno Vasco, mostraba un grave problema al que se iba a enfrentar la Ertzaintza, expuesto en el apartado anterior, esto es, los infiltrados de ETA.

2.4 Integración de datos de la legislatura

Una de las prioridades del PNV y, por ende, del Ejecutivo vasco era poner en marcha, al inicio de la legislatura, el proyecto para disponer de un cuerpo policial autonómico como un «instrumento indispensable» de la política de «construcción nacional», cuyos

[9] Este comunicado se publicó antes de la reconstitución de la *Ertzaintza*, tras el asesinato el 10 de enero de 1980 del comandante Jesús Velasco, jefe de Miñones de la Diputación de Álava. Si bien el mismo se encuentra fuera del periodo de estudio, se considera de especial interés su inclusión.

cimientos se habían colocado con la aprobación del Estatuto de Autonomía de 1979[10] (San Sebastián y Gurruchaga, 2000: 148).

Este empeño «personal» del PNV provocó que, desde su reconstitución oficial en 1982, aunque iniciada dos años antes, la Ertzaintza haya sido señalada por su íntima vinculación con el partido, llegando a ser calificada como la «policía del PNV», cuyos primeros componentes fueron incluso reclutados entre los afines a los *jeltzales*[11] (Dávila, 2006; Fernández *et al*., 2021; San Sebastián y Gurruchaga, 2000: 148).

En estos primeros años, el Gobierno Vasco consideraba ETA y su violencia una responsabilidad heredada por el Gobierno ucedista de la dictadura franquista, de ahí que la política antiterrorista oficial fuera no «hacer nada concreto contra ETA» (Balantx, 1982: 11; Ere, 1980, citado en Fernández *et al.*, 2021), máxime cuando en enero de 1980 la organización terrorista había trasladado, en un comunicado oficial, su compromiso de no atacar a la «Policía Autóctona»; eso sí, siempre que este Cuerpo respetara los intereses de *Euskadi* (ETA, 1980), lo que debe interpretarse como los intereses de la propia ETA.

No en vano, entre 1981-1982 se produjo la pactada disolución de ETA político-militar y su reconversión en agente político, por lo que no resulta extraño que para los representantes del Ejecutivo vasco se llegase a considerar que la pacificación del País Vasco podría producirse de forma natural con mejoras en la situación económica, la reducción del paro y una mayor autonomía, y por ello, era mejor «hacer nada» (Buesa, 2012; Sánchez y Simón, 2017). Así, la estrategia oficial pasaba por una suerte de inacción táctica, confiando en que las circunstancias sociopolíticas transformaran el escenario de violencia.

A pesar de esta línea oficial, el Gobierno Vasco era consciente de que la organización terrorista podría interferir en ese proyecto de «construcción nacional» del PNV, por lo que en esta legislatura se dieron ciertos pasos en lo que podría denominarse como una incipiente política antiterrorista: el informe Arístegui; la creación del grupo Ekintza; o el supuesto informe de la Consejería de

[10] En virtud de la Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco.

[11] Palabra en vasco traducida como «nacionalista» y que figura en la propia denominación oficial en vasco del PNV (*Eusko Alderdi Jeltzalea*). Según el traductor de la web del Gobierno Vasco, los términos *jeltzale* o *jelkide* hacen alusión al PNV o a sus seguidores (Gobierno Vasco, 2019).

Interior[12] (Díaz Herrera y Durán, 2002; Méndez, 1986; Tiempo, 1982, citado en Balantx: 12). Estas actuaciones iban en consonancia con los comentarios de Luis Retolaza en una reunión con representantes del Gobierno estatal, reconociendo que su política antiterrorista se basaría en «la acción psicológica y la acción disuasoria» (Vasco Press, 1992a).

ETA, por su parte, cumplió su compromiso de no agredir a la Ertzaintza durante esta etapa, aunque no dejó de considerar a la nueva policía como un actor relevante en su entorno. De hecho, en agosto de 1981, se incautaron en Francia documentos con referencias al entonces superintendente Carlos Díaz Arcocha, lo que evidenciaba que el seguimiento a la policía vasca formaba parte de los planes de la organización terrorista (El Diario Vasco, 1985, citado en Fernández *et al*., 2021).

No obstante, el punto de inflexión en este periodo fue el asalto perpetrado por ETA a las dependencias de la PAV en la Diputación de Gipuzkoa el 28 de febrero de 1983 bajo el pretexto de un «aprovisionamiento de armamento» (ETA, 1983; El Correo, 1983b). Esta acción, facilitada por la presencia de un miembro de ETA infiltrado en la Ertzaintza, encendió las alarmas en el seno del Ejecutivo vasco, que empezó a tomar mayor conciencia de la vulnerabilidad de su proyecto ante la actuación de la organización terrorista (Domínguez, 2009; El Correo, 1983; M. P., 2008).

3 II Legislatura (1984-1986). Primeros atentados y estrategia incipiente

3.1 El papel del PNV

Coincidiendo con la II Legislatura del Gobierno Vasco, el Gobierno de España, en el marco de su política antiterrorista, consiguió que Bélgica y Francia concedieran las extradiciones de los miembros de ETA que eran detenidos en sus territorios, al objeto de que fueran procesados por la Autoridad Judicial española.

Así, en julio de 1984, por primera vez en su historia, Bélgica concedió extradiciones por delitos de terrorismo, tratándose de dos ciudadanos españoles acusados de pertenecer a ETA o de parti-

[12] Este informe versaba sobre los cometidos de la *Ertzaintza*, entre ellos auxiliar a los *berrocis* en la luchar antiterrorista para acabar con ETA sin ayuda de las FCSE.

cipar en la perpetración de acciones terroristas, Joseba Artetxe y Gaizka Ormaza (Garrigó, 1984; Panisello, 2016).

Más complejo era el caso francés, ya que repetidamente denegaba las peticiones de extradición desde España, a pesar de estar motivadas en delitos análogos a otras concedidas a Alemania o Italia (Reventós, 1993). Fruto de un trabajo iniciado en octubre de 1982 para que Francia se metiese «de lleno en la lucha contra ETA», a lo que se sumaba el precedente belga, el Ejecutivo socialista consiguió en septiembre de 1984 que Francia, por primera vez para España, extraditara a miembros de ETA detenidos en el país galo (Panisello, 2016: 29).

A pesar de estos éxitos de la política estatal en la lucha antiterrorista, según Domínguez (2009), la postura del PNV fue totalmente antagonista: en el caso francés, se opuso a las extradiciones y, en el belga, llegó incluso a realizar gestiones para que ese país no entregara a Joseba Artetxe y Gaizka Ormaza.

No obstante, esta postura del PNV ante ETA cambió tras el asesinato del superintendente de la Ertzaintza Carlos Díaz Arcocha en marzo de 1985, apostando por la aplicación de medidas políticas y policiales y promoviendo la movilización social contra el terrorismo. No en vano, el *lehendakari* José Antonio Ardanza llegó a manifestar, buscando ese apoyo popular contra ETA, que la organización terrorista había atacado «una de las manifestaciones más genuinas de nuestras instituciones», en alusión a la PAV (Alfaro, 1985a: 17). Más hirientes fueron las declaraciones del presidente del PNV, Xabier Arzalluz, que imputaba a ETA la comisión de un grave error, ya que habían puesto más gente en su contra, toda vez que este asesinato no fue «asumido […] con la misma indiferencia», que los perpetrados, por ejemplo, contra militares, policías y guardias civiles (Diario Vasco, 1985, citado en Fernández *et al*., 2021: 543). Esta repulsa política se materializó con una declaración institucional del Parlamento Vasco condenando el terrorismo y rechazando la negociación política con ETA[13] y una Declaración contra la violencia por la Juntas Generales de Gipuzkoa (C. V., 1985; Moreno Bibiloni, 2021).

[13] Esta declaración fue posteriormente apoyada en el Congreso de los Diputados con la aprobación el 5 de noviembre de 1987 del *Acuerdo de Madrid sobre Terrorismo* o *Pacto de Madrid*, que suscribieron todos los partidos con representación salvo HB, incluyendo al PNV. Este acuerdo sirvió de base para el posterior *Pacto de Ajuria Enea* (González, 2018).

Por su parte, el Gobierno Vasco, como primera medida práctica, aunque de dudosa efectividad, encargó a una comisión internacional de expertos la redacción de un informe sobre la violencia en el País Vasco, cuyos resultados se hicieron parcialmente públicos en marzo de 1986. Este informe que, entre otras cuestiones, recogía diversas recomendaciones en materia de seguridad ciudadana, información, educación y concienciación ciudadana, sirvió «de coartada al PNV para aceptar la implicación de la Ertzaintza en la lucha contra ETA» (Ruiz de Azúa, 1986; Domínguez, 2009).

Fruto de esa nueva orientación, en mayo de 1986, en virtud de la Orden de 20 de mayo, surgieron los Adjuntos a la Viceconsejería de Seguridad (AVCS), que se convirtieron en el servicio de información de la Ertzaintza encargado de la lucha antiterrorista.

Estos cambios permitieron la realización de la primera operación de la PAV contra ETA, que favoreció la liberación de Lucio Aguinagalde el 1 de noviembre de 1986, si bien especialmente motivada por la antigua militancia *jeltzale* del secuestrado. Como reconoció el propio presidente del PNV, Xabier Arzalluz, el empresario era «carne propia de este partido», y, por tanto, en ese asunto volcaron todos sus esfuerzos, no solo policiales, sino también de movilización de masas (El Correo, 1986: 10).

No obstante, los pasos del Gobierno Vasco seguían siendo muy medidos. Al final del operativo, que se saldó con la trágica muerte del *ertzaina* Genaro García de Andoáin, también antiguo militante del partido, el Gobierno Vasco, a través del *lehendakari* Ardanza, alabó el papel de la Ertzaintza a pesar de sus recursos limitados, a la vez que exigía un traspaso pleno de competencias de orden público y el repliegue de las FCSE[14] (Fernández de Vallejo, 1986; Corcuera, 1986).

Igualmente, a pesar de la legislación nacional vigente, el Gobierno Vasco seguía manteniendo la negativa a reconocer la jurisdicción de la Audiencia Nacional para los casos de terrorismo[15], defen-

[14] A pesar de las reivindicaciones del Gobierno Vasco, el ministro del Interior del Gobierno de España, José Luis Barrionuevo, reconoció que no existía ningún impedimento legal para que la *Ertzaintza* no actuase contra cualquier forma de criminalidad (Corcuera, 1986).

[15] El Real Decreto-Ley 3/1977, de 4 de enero, sobre competencia jurisdiccional en materia de terrorismo, establecía, en su art. primero, que «la instrucción, conocimiento y fallo de las causas por los delitos de terrorismo corresponderá exclusivamente a los Juzgados Centrales de Instrucción y a la Audiencia Nacional».

diendo la idoneidad de las instancias judiciales del País Vasco. Los detenidos por el secuestro, en vez de ser trasladados a Madrid, fueron puestos a disposición del juzgado competente por razón del territorio, en este caso, el de Durango (Bizkaia) (EFE, 1986; Domínguez, 2009).

De forma paralela, durante el primer semestre de 1986, el PNV y *Herri Batasuna* (HB), brazo político de la organización terrorista ETA[16], iniciaron un proceso de negociación para intentar acabar con la violencia en el País Vasco, en el que el partido *jeltzale* era representado, precisamente, por Genaro García de Andoáin (Díaz Herrera y Durán, 2002). Esto provocó que la reacción de los *jelkides*[17] ante grandes atentados, como el producido el 23 de abril de 1986 en Madrid que se saldó con cinco víctimas mortales, fuera tibia, no solo contra la acción terrorista, sino con HB (Moreno Bilbiloni, 2021).

3.2 El papel de la Ertzaintza

A pesar de la creciente amenaza de ETA y de las acciones perpetradas contra la Ertzaintza, incluido el asesinato de Díaz Arcocha en marzo de 1985, la PAV no consideraba la lucha contra la organización terrorista como uno de sus cometidos.

A pesar de esta creencia, en este mismo periodo, en el año 1985 se puede establecer la creación del Berroci Berezi Taldea (BBT), conformado con base en el grupo de «berrocis» primigenio y que constituyó el Grupo Especial de Intervención, dedicado a actuar en las situaciones de mayor complejidad y peligrosidad, como es el caso del terrorismo (De Otálora y Calabor, 1995).

Sin embargo, a nivel de las bases del cuerpo, la mayor parte de los agentes de las primeras promociones consideraba la activi-

[16] Los partidos políticos HB, *Euskal Herritarrok* (EH) y *Batasuna* fueron ilegalizados mediante Sentencia del Tribunal Supremo (STS) de fecha 27 de marzo de 2003, ratificada mediante las Sentencias del Tribunal Constitucional (STC) 5/2004 y 6/2004 y, finalmente, mediante la Sentencia del Tribunal Europeo de Derechos Humanos (STEDH) de 30 de junio de 2009. La STS de 27 de marzo de 2003 establece que el partido político HB y las marcas que le sucedieron sirvieron para materializar la estrategia de «desdoblamiento» diseñada por ETA y «a asumir, inicialmente, el desarrollo de la función de la Unidad Popular como elemento clave para simultanear, en un mismo instrumento, la participación en los procesos electorales y la coordinación, control y estímulo de todos aquellos sectores sociales que pudieran coadyuvar al complemento político de la actividad terrorista».

[17] *Ibidem* nota 11.

dad de ETA y, por ende, la lucha antiterrorista, como algo ajeno a su ocupación policial, sin «influencia relevante en la agenda», descartando incluso la posibilidad de ser objeto de un ataque. En palabras de uno de los primeros «berrocis», la lucha contra ETA «no iba con nosotros [y] lo de Arcocha. "Bueno era militar"», reproduciendo el mismo argumento que esgrimía ETA como justificación del asesinato del superintendente (Dávila, 2006: 323-324).

A pesar de lo anterior, en el caso del asesinato de Díaz Arcocha, la propia PAV realizó una investigación interna para determinar la autoría del crimen que, «sorpresivamente», nunca fructificó. Los responsables de esas pesquisas fueron los agentes Jesús Guergue y Federico Fernández de Jáuregui, mencionados anteriormente, quienes, en septiembre de 1989, fueron detenidos por la Guardia Civil por su papel como colaboradores de ETA[18].

Ante la necesidad de disponer de una estructura más especializada, en virtud de la Orden de 20 de mayo de 1986, se crearon oficialmente los AVCS. Este grupo, compuesto por 33 agentes repartidos por las tres provincias vascas, tuvo como principal problema la captación de sus miembros debido la falta de voluntad de muchos *ertzainas* para intervenir en labores antiterroristas (Domínguez, 2009).

Esta Unidad, liderada por Genaro García de Andoáin, fue la responsable del dispositivo que facilitó la liberación del empresario guipuzcoano Lucio Aguinagalde en noviembre de 1986, si bien con un alto coste, esto es, el asesinato de su jefe. Esta actuación está rodeada de una gran polémica: falta de planificación y excesiva precipitación, posiblemente motivadas por las reiteradas críticas que recibía la Ertzaintza sobre su supuesta pasividad ante ETA; temeraria exposición del responsable del grupo; falta de comunicación con otras fuerzas de seguridad y, por último, el exiguo despliegue de recursos materiales y humanos (Arroyo, 1986; Fernández de Vallejo, 1986). Demasiados claroscuros para una actuación liderada por un *ertzaina* que en ese momento representaba al PNV y al Gobierno Vasco en unas negociaciones con ETA.

[18] Ambos fueron juzgados por su presunta participación en el asesinato de Arcocha y, finalmente, absueltos, en virtud de la Sentencia 48/2000 de la Audiencia Nacional de fecha 25 de septiembre.

3.3 El papel de ETA

Como se relató anteriormente, ETA realizó un salto cualitativo al planificar y ejecutar el asesinato del *ertzaina* Díaz Arcocha en marzo de 1985, de quien disponía de informaciones desde, al menos, 1981.

En su comunicado de reivindicación, ETA se justificó apelando al pasado militar del superintendente, evitando cualquier mención a su condición de *ertzaina* (ETA, 1985), en un claro intento de mitigar el rechazo social que este asesinato estaba provocando en una parte del nacionalismo vasco vinculado al PNV.

Tras el secuestro de Aguinalgalde en octubre de 1986, ETA, inmersa en ese salto cualitativo, acusó a la cúpula del PNV de la gravedad que supondría que la *Ertzaintza* colaborase con «las fuerzas de ocupación españolas» (ETA, 1986a). ETA le trasladaba de esta forma al PNV y, por ende, al Gobierno Vasco, que, si empleaba la PAV en labores antiterroristas, aunque fuera para liberar a un histórico militante *jeltzale* como Aguinagalde, la escalada de violencia se incrementaría.

De forma tristemente premonitoria, esta amenaza se transformó en un nuevo asesinato de un *ertzaina*, en este caso García de Andóain, en noviembre de 1986. ETA, en su comunicado, acusó al PNV de poner a la PAV al servicio de «los verdaderos enemigos del pueblo vasco», en alusión a las FCSE, calificándola, por primera vez, con el despectivo término «cipayo[19]» (ETA, 1986b), que acompaña a la Ertzaintza hasta nuestros días, compartida por el entorno de la Izquierda *Abertzale* (IA), con «sistemática finalidad de menosprecio, provocación o descalificación, presentando un ánimo tendencial de menospreciar conscientemente el principio de autoridad» (Juzgado de lo Penal número 2 de Vitoria, citado en González, 2024).

El uso de epítetos denigrantes, según Gómez Moral (2013: 44), era una forma de «despojar de su sustantividad de persona» a los *ertzainas* y, a través de esa «deshumanización verbal», preparar a la sociedad vasca «para digerir sin problemas cualquier desenlace por terrible que fuera», incluso hasta el asesinato.

[19] En alusión a los cipayos indios, esto es, los soldados indígenas del subcontinente indio que servían en los ejércitos de distintos estados y compañías comerciales europeas; a partir de la segunda mitad del siglo XIX, estos soldados pasaron a integrar las filas del Ejército Indio Británico (Cartwright, 2022). En el contexto del presente estudio, este término era usado por ETA y el entorno de la IA de forma despectiva para criticar el papel de los *ertzainas* como supuestos colaboradores de unas «fuerzas de ocupación o represión colonial», en alusión a las FCSE.

Desde ese momento, ETA y, por ende, su entorno político-social, generaron un discurso hostil contra la Ertzaintza, recrudecido con el paso del tiempo.

3.4 Integración de datos de la legislatura

Durante el verano de 1984, el Gobierno central declaró públicamente su disposición a entablar un diálogo con ETA, lo que marcaría el comienzo de los contactos informales que precedieron a las conversaciones de Argel. Estos encuentros se prolongaron hasta 1987 bajo la dirección del Gobierno socialista, sin que el PNV, pese a su interés, desempeñara un papel relevante (Sánchez y Simón, 2017; San Sebastián y Gurruchaga, 2000; Unzueta, 2016).

No obstante, el partido *jeltzale* sí asumió cierto protagonismo al realizar ciertas maniobras para obstaculizar las extradiciones de miembros de ETA desde Bélgica y Francia en julio y septiembre de 1984, obtenidas fruto de la nueva política antiterrorista del gobierno socialista y con su participación como mediador en la denominada «vía Azkarraga[20]» que permitió la reinserción de diversos internos terroristas (Domínguez, 2009; Sánchez y Simón, 2017; Unzueta, 2016).

A pesar de esos gestos de los *jeltzales*, en marzo de 1985, ETA decidió dar un salto cualitativo y perpetrar el asesinato de Arcocha, apelando al pasado militar del superintendente y evitando cualquier mención a su condición de *ertzaina* (ETA, 1985).

La reacción del Gobierno Vasco fue inmediata y contundente. El Parlamento Vasco emitió una declaración institucional de condena y se encargó un informe a una comisión internacional para analizar la situación de violencia en Euskadi. En paralelo, se creó una unidad especial de intervención dentro de la Ertzaintza, los BBT, concebida como una unidad de intervención para actuar en situaciones de alta peligrosidad, incluidas las operaciones contra ETA (Alfaro, 1985b; C. V., 1985; De Otálora y Calabor, 1995; Fernández *et al*., 2021).

[20] Durante el proceso de negociaciones para la disolución de ETA-Político Militar (ETA-pm), un grupo contrario a esa política, los *octavos*, continuaron con la actividad terrorista. Finalmente, en 1985, durante el Gobierno del Presidente Felipe González, aquellos *octavos* que no se habían integrado en ETA-m, siguieron el camino de sus antiguos compañeros *polimilis*, en lo que se denominó la «Vía Azkarraga», en referencia al entonces senador del PNV Joseba Azkarraga. Esta iniciativa de reinserción, que puede calificarse como exitosa y con una implicación directa del PNV, supuso la concesión de más de cuarenta indultos, principalmente a presos de ETA-pm, aunque también de ETA-m y de Comandos Autónomos Anticapitalistas (Unzueta, 2016).

El informe internacional fue publicado en marzo de 1986 y sus conclusiones respaldaron la creciente implicación en la lucha antiterrorista (Domínguez, 2009; Ruiz de Azúa, 1986). Ese mismo año, en virtud de la Orden de 20 de mayo de 1986, se conformaron los AVCS, el servicio de información de la policía autonómica, cuya misión era recopilar y analizar inteligencia sobre la actividad de ETA.

Paralelamente, el PNV optó por abrir su propia vía de contacto con ETA. A lo largo del primer semestre de 1986, se produjeron reuniones informales cuyo interlocutor principal fue Genaro García de Andoain, jefe del grupo Ekintza, luego de los AVCS, y figura de confianza tanto del partido como del Gobierno Vasco. Este canal se mantuvo al margen de las conversaciones oficiales lideradas por el Ejecutivo español (Díaz Herrera y Durán, 2002; Moreno, 2021).

En octubre de ese mismo año, ETA decidió tensar la situación y secuestró, en el marco de su campaña de extorsión económica, al empresario Lucio Aguinagalde, histórico peneuvista. En su comunicado, la organización llegó a amenazar a la cúpula del PNV de la gravedad que supondría que la Ertzaintza colaborase con «las fuerzas de ocupación españolas» para rescatar al empresario (ETA, 1986a).

El 1 de noviembre, en un operativo policial que hoy en día aún presenta demasiados claroscuros, la PAV liberaba a Lucio Aguinagalde (Arroyo, 1986; Fernández de Vallejo, 1986). Durante el desarrollo del dispositivo se produjo un tiroteo con los etarras en el que fue herido mortalmente García de Andoáin, a la vez jefe de la unidad antiterrorista de la Ertzaintza y representante del PNV y del Gobierno Vasco en las conversaciones con ETA. La operación marcó un punto de inflexión: ETA acusó abiertamente al PNV de instrumentalizar a la Ertzaintza en beneficio del Estado y comenzó a usar el término «cipayo» de forma sistemática para referirse de forma despectiva a la policía vasca (ETA, 1986b).

En definitiva, esta legislatura acababa con ETA señalando a la Ertzaintza por implicarse, aunque someramente, en la lucha antiterrorista, y con la vía de negociación iniciada por el PNV en dique seco tras el asesinato de Genaro. El Gobierno Vasco era consciente del problema que suponía la organización terrorista y se encontraba dotando a PAV de las estructuras necesarias para hacerle frente.

En el plano estatal, las conversaciones de Argel también fracasaron tras la muerte accidental de *Txomin* Iturbe en 1987, cerrando así un ciclo de intentos de diálogo sin resultados concretos (Sánchez y Simón, 2017; Unzueta, 2016).

4 III Legislatura (1987-1990). Traspasos de competencias a la Ertzaintza y primeras actuaciones

4.1 El papel del PNV

Al poco de comenzar la legislatura, el 16 de octubre de 1987, se aprobó en el Parlamento Vasco por unanimidad una petición de sustitución progresiva de la Guardia Civil y del Cuerpo Nacional de Policía en beneficio de la policía autonómica[21]. Esta propuesta instaba a los Gobiernos central y autonómico a negociar un plan conjunto que garantizase la coordinación de las diferentes Fuerzas y Cuerpos de Seguridad (Ruiz de Azúa, 1989).

A pesar de esta voluntad de sustituir, que no complementar, a las FCSE en el territorio del País Vasco, en el ínterin de este proceso político el Gobierno Vasco continuaba exteriorizando esa falta de proactividad en la lucha contra ETA. En consonancia, tras el asesinato del *ertzaina* José Luis Pacheco en octubre de 1988, desde la Consejería de Interior se apresuraron a clarificar que «no hubo orden de ningún superior para que actuaran como lo hicieron, sino que llevados de un exceso de celo y de buena voluntad intervinieron» (Fernández *et al.*, 2021: 560)[22].

Tras distintos altibajos[23], el proceso de negociación entre administraciones se materializó con el *Acuerdo de delimitación de servicios* de marzo de 1989 que, en materia antiterrorista, suponía que la PAV ejercería, conjuntamente con las FCSE, las competencias en la lucha contra el terrorismo y de todos los delitos

[21] Esta proposición contó con el apoyo los siguientes grupos parlamentarios, ordenados de mayor a menor representación: Partido Socialista de Euskadi-Partido Socialista Obrero Español (PSE-PSOE), PNV, Eusko Alkartasuna (EA), Euskadiko Eskerra (EE), Alianza Popular (AP) y Centro Democrático y Social (CDS).

[22] El 16 de octubre de 1988, ETA alertó de la colocación de varios explosivos en la vía férrea a su paso por la localidad guipuzcoana de Legazpi. Mientras los agentes de la PAV realizaban cometidos de aseguramiento, búsqueda y localización, uno de los artefactos explosionó y, cuando se aproximaron para comprobar los destrozos, se produjo una segunda deflagración, que alcanzó de lleno al *ertzaina* Juan José Pacheco, causándole la muerte en el acto, según obra en la Sentencia 7/1997 de 28 de enero de la Audiencia Nacional.

[23] Las conversaciones se retomaron tras los ceses del Ministro del Interior, José Barrionuevo, y del consejero de Interior, Luis María Retolaza, siendo sustituidos por José Luis Corcuera y Juan Lasa, respectivamente. Estos cambios propiciaron el restablecimiento de las conversaciones relativas al plan de despliegue de la PAV (Jar, 1995).

cuyo enjuiciamiento correspondiese a la Sala de lo Penal de la Audiencia Nacional. Resulta paradójico que en esta ocasión el Gobierno Vasco sí reconociese la competencia de este Tribunal cuando, en la anterior legislatura, tras la liberación de Lucio Aguinagalde, se negase el traslado a Madrid de los miembros de ETA detenidos.

Finalmente, al contrario de lo ocurrido tras el asesinato del *ertzaina* Pacheco, tras la operación policial desarrollada en Bizkaia en abril de 1990, y de la que se hablará en el siguiente apartado, el Gobierno Vasco, a través del *lehendakari* Ardanza, procedió a felicitar públicamente al cuerpo autonómico. A estos parabienes se sumó el ministro del Interior, José Corcuera, dando visibilidad a la coordinación que había existido entre la PAV y las FCSE (Gorospe, 1990).

4.2 El papel de la Ertzaintza

El asesinato del *ertzaina* Pacheco en octubre de 1988 generó una gran polémica, sobre todo por las declaraciones desde la Consejería de Interior trasladando la responsabilidad «al exceso de celo y de buena voluntad» de los agentes (Fernández *et al.*, 2021: 560).

No obstante, lo que realmente puso de manifiesto este asesinato, y de lo que se hizo eco el sindicato policial de *ertzainas* ErNE (Ertzainen Nazional Elkartasuna), fue el cuestionamiento sobre la forma en la que se desarrolló el dispositivo, denunciando que los agentes intervinientes carecían de la capacitación adecuada y que los procedimientos no fueron bien aplicados (Egin, 1988a).

Esto permite deducir que, independientemente de la responsabilidad material de los autores del atentado, la Ertzaintza adolecía de una estructura, organización y experiencia operativa suficientes para hacer frente a una lucha en la que había entrado desde el mismo momento de su reconstitución, a pesar de la reticencia de los responsables políticos del Gobierno Vasco y del PNV.

Esta ausencia de una orgánica apropiada se pone de manifiesto tras la aprobación del *Acuerdo de delimitación de servicios* de marzo de 1989 que definía meridianamente la competencia de la PAV para la investigación criminal, incluyendo la lucha contra el terrorismo, para así reconocer formalmente a la Ertzaintza un rol activo en la lucha contra ETA. Sin embargo, ante esa evidente carencia en el cuerpo policial autonómico de la infraestructura

necesaria, se estableció un plazo de ocho años para la asunción de esa competencia antiterrorista (Etxarri, 1989).

De las lecciones identificadas, la Ertzaintza, en su proceso de desarrollo organizativo, comenzó a fortalecer su estructura contraterrorista en los ámbitos de la investigación criminal y de otras especialidades.

En consonancia, la PAV detectó la necesidad de disponer de una unidad de desactivación de explosivos, encomendando al antiguo policía, ya *ertzaina*, Luis Hortelano, la dirección de ese equipo y la formación de sus futuros miembros.

Para desarrollar este cometido y mantenerse actualizado en las técnicas, tácticas y procedimientos de la organización terrorista en lo relativo a artefactos explosivos, Luis Hortelano acompañaba con frecuencia a los artificieros de la Policía Nacional durante sus actuaciones (Fernández *et al.*, 2021), tarea durante la que fue asesinado por ETA en mayo de 1989[24].

A pesar de la incipiente estructura antiterrorista, la Ertzaintza comenzó sus primeras investigaciones. Así, a raíz del secuestro del industrial Adolfo Villoslada en noviembre de 1989, ejecutó diversas actuaciones en enero de 1990 contra el aparato de extorsión de ETA (Díaz Herrera y Durán, 2002). Por otro lado, el 4 de abril de 1990, la PAV desarrolló diversas actuaciones en Bizkaia que se saldaron con varias detenciones y registros y el desmantelamiento de una parte de la infraestructura de apoyo del comando *Bizkaia*, todo ello en coordinación con las FCSE (Gorospe, 1990).

No obstante, no se debe olvidar que, según se puede deducir de los asuntos tratados en la reunión secreta mantenida entre el presidente del PNV, Xabier Arzalluz, y representantes de Koordinadora Abertzale Sozialista[25] (KAS) en marzo de 1991, en

[24] El 24 de mayo de 1989 en Zorrotza (Bizkaia), tras la explosión de un artefacto explosivo, miembros de los equipos de desactivación de explosivos de la Policía Nacional, acompañados del *ertzaina* Luis Hortelano, se acercaron a inspeccionar la zona. Un segundo artefacto fue localizado y los artificieros procedieron intentar neutralizarlo, activando accidentalmente un dispositivo trampa. Esta segunda explosión ocasionó la muerte de dos policías nacionales, José María Sánchez García y Manuel Jódar Cabrera, y del *ertzaina* Luis Hortelano, según datos obrantes en la Sentencia 2/1994 de 29 de enero.

[25] KAS fue una organización integrada en el entramado de ETA que desempeñaba funciones de coordinación y dirección política dentro del denominado Movimiento de Liberación Nacional Vasco (MLNV) y de defensa de los mismos objetivos que el

esta época el Gobierno Vasco no estaría impulsando la realización de operaciones policiales contra ETA, «de hecho, es más bien lo contrario, que estamos frenando […] lo que ocurre es que a veces no le queda más remedio [a la Ertzaintza que actuar]» (San Sebastián y Gurruchaga, 2020: 53).

4.3 El papel de ETA

Durante esta legislatura, la organización terrorista asesinó a dos *ertzainas*, en 1988 y en 1989, si bien, como se verá a continuación, en sus reivindicaciones intentó retorcer las justificaciones para evitar vincular a la Ertzaintza como uno de sus *targets*.

Tras el asesinato del *ertzaina* Pacheco el 16 de octubre de 1988, la propia organización terrorista, en su comunicado reivindicativo, calificó la muerte como accidental, incidiendo en que la Ertzaintza, como cuerpo policial, no se constituía en un objetivo, derivando la responsabilidad al Gobierno Vasco, al permitir que la PAV participase «en las tareas represivas que las fuerzas de ocupación desarrollan [en alusión a las FCSE]» (ETA, 1988).

De nuevo, en un ejercicio de total incongruencia, ETA justificaba el asesinato en el hecho de que la Ertzaintza estaba colaborando con las FCSE realizando cometidos antiterroristas; siendo la realidad que el cuerpo autonómico había asumido esos cometidos por el carácter integral que le otorgaba el Estatuto de Autonomía, en detrimento de las competencias que previamente desarrollaban las FCSE.

Estas mismas ideas eran replicadas por su brazo político, HB, que, aparte de calificar igualmente el asesinato como accidental, responsabilizaba al Gobierno Vasco, compuesto por el PNV y PSE-PSOE, de intentar provocar un enfrentamiento civil entre ETA y la sociedad vasca (Egin, 1988a, citado en Fernández *et al.*, 2021).

Como se puede constatar, este atentado no tenía como *target* a un agente específico; no obstante, ETA era plenamente consciente de las funciones que desarrollaba la Ertzaintza y que, ante ese aviso de bomba, inspeccionaría el lugar. Asimismo, con esa disposición de los artefactos, con explosiones escalonadas, ETA se aseguraba de que se produjeran heridos y, como fue el

Frente Militar de ETA. KAS fue ilegalizada mediante la Sentencia de la Audiencia Nacional 73/2007 de 19 de diciembre, ratificada mediante STS 480/2009 de 22 de mayo.

caso, víctimas mortales. En esa ocasión concreta, la organización terrorista quizás no había colocado a la PAV como su objetivo, si bien, era plenamente consciente de que podía ocasionar víctimas y, aun así, lo asumió como parte de la acción cometida, lo que podría calificarse, en el ámbito del derecho penal, como «un» dolo eventual[26] «de manual».

No se puede obviar cuál era la postura de ETA ante la asunción de competencias de forma integral por parte de la PAV, sobre todo en lo atinente a la lucha antiterrorista. De ahí que, ante el acuerdo de marzo de 1989 sobre delimitación de servicios, Jon Idígoras, portavoz de HB, brazo político de ETA, manifestase su desconfianza por «la incorporación de la Ertzaintza a la lucha contrainsurgente» (Gorospe, 1989).

Esta desconfianza se tornó en muerte el 24 de mayo de 1989 con el asesinato del *ertzaina* Hortelano y sus dos compañeros policías. ETA, en un nuevo alarde de hipocresía, enfatizó en su comunicado de reivindicación la antigua condición de policía nacional de Luis Hortelano.

Otro asesinato de un miembro de la PAV y de nuevo la manida justificación apelando a su antigua pertenencia a las FCSE si bien, en este caso, cometido en el marco de una estrategia para actuar contra unidades especializadas en la lucha antiterrorista, como son los artificieros, de los cuales era conocido que se constituían en un recurso crítico de las fuerzas policiales (ETA, 1989).

Estas actuaciones iban en consonancia con la línea interna que se había marcado ETA. En 1989, la organización terrorista elaboró un documento titulado *EI MLNV ante la* Ertzaintza*. Significación política de la* Ertzaintza *actual y posicionamientos del MLNV*[27]

[26] Como establece, entre otras, la Sentencia del Tribunal Supremo (STS) 311/2014, de 16 de abril, se considera que existe dolo eventual cuando el sujeto, siendo consciente de que su conducta genera un peligro concreto y jurídicamente desaprobado, decide actuar y continuar con dicha conducta, sometiendo a la víctima a riesgos especialmente relevantes que no tiene la certeza de poder controlar o evitar. No es necesario que el autor persiga directamente la producción del resultado lesivo, sino que basta con que conozca la alta probabilidad de que su comportamiento lo provoque (Tribunal Supremo, 2014).

[27] El Movimiento de Liberación Vasco (MLNV) es la denominación genérica por la que puede designarse el sistema de organismos e instituciones surgido a partir de la teoría del desdoblamiento, en la que ETA aparecía representada solo por su *Frente Militar*, si bien controlando férreamente el resto de organismos de ese sistema. De esta forma, el MLNV se estructuraba en la *Vanguardia*, esto es, el *Frente Militar*, que ejercía la dirección global del MLNV y la específica de la actividad terrorista y en la parte de

ante ella, que servía como guía de actuación para ETA y para su entorno político-social y que se incluía en su publicación interna *Barne Buletina* de 1990.

De esta forma, antes de establecer como *target* a los *ertzainas* era preciso mentalizar a la base social y que no se viese como un conflicto entre vascos. La propia organización terrorista era consciente del problema que suponía para su «causa» que el conflicto vasco evolucionase de la manipulada visión de lucha entre Euskadi-Estado español, a una lucha dentro de la sociedad vasca, en la que la parte democrática combatiese los designios de una organización terrorista empleando una policía vasca (Barne Buletina, 1990, citado en López Fonseca, 1993; Barne Buletina, 1990, citado en Fernández *et al*., 2021).

El documento planteaba «dividir y fracturar política y socialmente la unidad existente [en la PAV]» entre la base y sus mandos, proponiendo como herramienta la «discriminación social» de los agentes (Domínguez, 2022a).

Para romper esa cohesión y unidad orgánica en el instrumento del Gobierno Vasco de aplicación de su política pública antiterrorista, ETA marcaba como objetivo denunciar públicamente a las unidades más implicadas en la lucha antiterrorista, como los AVCS y a los responsables de estas, contra quienes «se podrá valorar realizar acciones de un modo exclusivo, dirigido y ostensible» (Barne Buletina, 1990, citado en Fernández *et al.*, 2021: 567).

Por último, como venía siendo habitual cuando se producían acuerdos en materia de competencias entre las administraciones central y vasca, tras la aprobación en agosto de 1990 del *Plan de Despliegue de la* Ertzaintza *y Repliegue de las Fuerzas de Seguridad del Estado*, ETA, en un comunicado oficial, a la par que insistía en que nunca había amenazado a la PAV, nuevamente alertaba del peligro que suponía que este cuerpo realizara las mismas funciones, incluida la lucha antiterrorista, que las FCSE (ETA, 1990).

---

organismos sectoriales y de masas, estructurados en cuatro grandes bloques: LAB, como frente sindical, JARRAI, como organización juvenil, EGUIZAN, como frente de la mujer y un frente global de masas que incluiría al resto de los organismos populares dinamizados y controlados por los Abertzale Sozialista Komiteak (ASK). A partir de 1976, los organismos de masas se integraron en KAS, plataforma que se convirtió en una estructura estable para la defensa de los mismos objetivos que el *Frente Militar* de ETA (STS 480/2009 de 22 de mayo).

Estas expresiones públicas contrarias al papel de la PAV como policía integral eran replicadas por HB, el brazo político de ETA. Así, Gorka Martínez, miembro de la Mesa Nacional, realizaba unas declaraciones en una entrevista en abril de 1990[28], en las que acusaba a la PAV de haberse posicionado, en el marco del conflicto vasco, contra ETA en particular, y contra el independentismo vasco en general (Punto y Hora de Euskal Herria, 1990: 8).

> «La Ertzantza, y sus propias actuaciones así los [sic] atestiguan, está adoptando una postura beligerante contra el MLNV, en general, y contra ETA, en particular […] la Ertzantza está ocupando deliberadamente una trinchera en el actual enfrentamiento, y por eso mismo destacaría el riesgo y peligrosidad de una situación forzada que pueda alimentar un enfrentamiento entre los vascos»

Ante la pregunta del entrevistador acerca de si la asunción de cometidos antiterroristas por parte de la PAV podría provocar que ETA la considerase «objetivo militar», Gorka Martínez confirma lo siguiente (Punto y Hora de Euskal Herria, 1990: 8): «los métodos que está adoptando la Ertzantza puede provocar un cambio de esas valoraciones […] está dejando de tener la utópica imagen con que se nos presentaba y cada vez se parece más a los modelos [de las FCSE]».

Estas declaraciones se enmarcaban en la campaña que ETA y su entorno político-social habían activado tras los operativos de abril de 1990 y que, a su vez, eran complementadas con manifestaciones de otros responsables de HB, con pintadas y carteles con calumnias y con denuncias sistemáticas por malos tratos a los detenidos (Grech, 2011).

Esta estrategia es confirmada por Juan María Atutxa, consejero de Interior en esa época, quien afirmó que, ante el fracaso de la anterior fase de intentos de desprestigio de la Ertzaintza, por ejemplo, mediante pintadas, ETA pasó a tratar de fragmentar la PAV, atacando a unidades concretas como los AVCS (Vasco Press, 1992a).

Estas palabras lanzaban un claro mensaje. La línea seguida por la Ertzaintza en la lucha antiterrorista no era del agrado de ETA, y ese supuesto enfrentamiento «entre los vascos» que comentaba

[28] Como se expuso en el apartado anterior, en abril de 1990, la PAV realizó una operación contra el aparato de apoyo del comando *Bizkaia*.

Gorka Martínez, no era más que una justificación para situar a los *ertzainas* como *targets* de la organización terrorista.

4.4 Integración de datos de la legislatura

El nuevo Gobierno Vasco incluía a los socialistas y esta situación generó una mayor compenetración con el gobierno central de Felipe González, lo que se materializó en los distintos pactos políticos nacionales contra ETA y en la finalización del traspaso de competencias policiales entre las FCSE y la PAV (Arroyo, 2022; Moreno, 2023). Estas cuestiones no eran del agrado de la organización terrorista, a pesar de que seguía en la ronda de negociaciones con el Gobierno de España en el marco de las conversaciones de Argel.

Tres meses después del inicio de la legislatura, el 19 de junio, ETA inició su campaña de grandes atentados y perpetró la mayor masacre de su historia con el ataque contra el supermercado Hipercor en Barcelona[29], que provocó grandes críticas en el entorno del MLNV (De Miguel, 2021; García, 2022).

La respuesta política se materializó en el Pacto de Madrid del 5 de noviembre de 1987 y, posteriormente, en el Pacto de Ajuria Enea de enero de 1988[30]. En ambos se asumían los principios contenidos en la resolución sobre la violencia aprobada por el Parlamento Vasco en marzo de 1985 y suponían la mayor acumulación de fuerzas políticas en contra del terrorismo de ETA (Mata, 2018).

[29] El 19 de junio de 1987, un comando de ETA colocó un coche bomba en las proximidades del centro comercial Hipercor en Barcelona, cuya explosión causó veintiún muertos, entre ellos cuatro menores, y cuarenta y cinco heridos, convirtiéndose en el atentado más mortífero de la historia de la organización terrorista.

[30] El Pacto de Ajuria Enea, oficialmente Acuerdo para la Normalización y Pacificación de Euskadi, fue un pacto político firmado el 12 de enero de 1988 en Vitoria entre las principales fuerzas políticas nacionales y autonómicas (PNV, PSE-PSOE, AP, CDS, EE y EA) para enfrentar de manera conjunta el terrorismo de ETA y avanzar hacia la normalización política y social en el País Vasco.

El Pacto de Ajuria Enea marcó un punto de inflexión en la política vasca al consolidar un frente democrático contra la violencia y sentar las bases para futuras iniciativas de paz (Mata, 2018).

Su vigencia se extendió durante una década, celebrándose la última reunión el 17 de marzo de 1998. En ese momento, dos de los firmantes, PNV y EA, se encontraban en un proceso secreto de negociaciones con ETA, que desembocaron en la Declaración de Estella-Lizarra de septiembre de 1998, la cual supuso la ruptura, de facto, del Pacto de Ajuria Enea (González, 2018; Sánchez y Simón, 2017).

Entre enero de 1988 y abril de 1989, se produjeron una serie de encuentros enmarcados en las conversaciones de Argel entre el Gobierno estatal y ETA que desembocaron en la breve tregua de enero a abril de 1989, que finalizó abruptamente tras el fracaso definitivo de las conversaciones (Sánchez y Simón, 2017; Unzueta, 2016).

A pesar de esta ronda de conversaciones, la Ertzaintza siguió sufriendo bajas, incluyendo el asesinato del *ertzaina* Juan Pacheco en octubre de 1988 y del artificiero Juan Hortelano en mayo de 1989, poco tiempo después de la ruptura de la tregua (Audiencia Nacional, 1997; 1994). En el caso del primero, ETA calificó la muerte como accidental y negó tener a la PAV entre sus objetivos, responsabilizando al PNV por implicarla en «tareas represivas» (ETA, 1988). Por su parte, el Gobierno Vasco señaló el exceso de celo de los agentes y la ausencia de órdenes de los superiores para justificar la actuación de los agentes, mientras que desde la Ertzaintza se denunció la carestía de capacitación adecuada y la falta de aplicación adecuada de los procedimientos (Egin, 1988a; Fernández *et al*., 2021).

Como se puede observar, lejos de asumir la necesidad de actuar contra ETA, desde el Gobierno Vasco se pretendió trasladar la responsabilidad de lo ocurrido, y por tanto del fallecimiento del *ertzaina*, a los propios agentes actuantes. Se les achacaba que su exceso de profesionalidad causó la muerte de su compañero.

Por otro lado, la buena sintonía política entre los gobiernos central y vasco facilitó el impulso de la transferencia completa de competencias a la Ertzaintza. Así, en marzo de 1989 y agosto de 1990 se aprobaron, respectivamente, el *Acuerdo de delimitación de servicios* y *Plan de Despliegue de la Ertzaintza y Repliegue de las Fuerzas de Seguridad*, que suponían un reconocimiento formal como policía integral y del rol activo de la PAV en la lucha contra el terrorismo.

Esta asunción de competencias era vista con desconfianza por el brazo político de ETA, que dudaba de esa «incorporación de la Ertzaintza a la lucha contrainsurgente» (Gorospe, 1989). La desconfianza tomó forma y la organización terrorista elaboró el documento *EI MLNV ante la* Ertzaintza*. Significación política de la Ertzaintza actual y posicionamientos del MLNV ante ella*. El texto buscaba fracturar la unidad existente en el Cuerpo, apostando por la «discriminación social» de los agentes y por denunciar públicamente a las principales unidades antiterroristas (AVCS y

BBT) y a sus responsables (Barne Buletina, 1990, citado en López Fonseca, 1993; Barne Buletina, 1990, citado en Fernández *et al*., 2021; Domínguez, 2022a). De esta forma, ETA intentaba mentalizar a su base social ante una eventual conversión de la PAV en un «objetivo militar».

El desarrollo competencial, el apoyo político, la buena coordinación con Madrid y una mayor capacitación permitieron que la PAV desarrollase diversas investigaciones contra ETA a partir de 1990, entre ellas el desmantelamiento de parte de la estructura de apoyo del comando *Bizkaia* en abril de ese año (Gorospe, 1990).

Este nuevo enfoque policial fue recibido con gran indignación por el entorno político-social de ETA y por la organización terrorista, que volvió a alertar del peligro que suponía que la PAV realizara las mismas funciones que las FCSE, entre ellas la lucha antiterrorista (ETA, 1990). Las campañas de discriminación social, incluyendo denuncias sistemáticas por malos tratos a los detenidos, pintadas y carteles con calumnias, continuaron; sin embargo, la imposibilidad de romper la cohesión de la Ertzaintza provocó que ETA cambiase de estrategia (Grech, 2011; Vasco Press, 1992a).

5 IV Legislatura (1991-1993). La Ertzaintza contra ETA y viceversa

5.1 El papel del PNV

A pesar de la deriva que ETA había iniciado en legislaturas anteriores, con atentados dirigidos contra *ertzainas* y con la PAV estableciendo estructuras orgánicas antiterroristas y desarrollando sus primeras operaciones, el Gobierno Vasco seguía manteniendo la tesis, ya sin fundamento, de que no existía posibilidad de que la Ertzaintza se convirtiera en un objetivo para ETA. El propio consejero de Interior, Juan María Atutxa, al poco de estrenar su cargo, manifestó que, si bien alguna acción terrorista contra la PAV era materialmente posible, la organización terrorista no iba «a ir contra la policía vasca[31]» (Vasco Press, 1992c).

[31] Estas declaraciones contradicen a las del ex consejero de Interior Luis Retolaza, quien ocupó esta cartera entre 1980 y 1988, tres años antes que Atutxa. En otro artículo de la misma publicación, Luis Retolaza, en alusión al asesinato de Arcocha perpetrado diecisiete años antes, explicó que «contra un mando o un político de la Ertzaintza. Siempre habíamos pensado que alguno caería […] No voy a decir esperado, pero sí asumido» (Vasco Press, 1992b: 6).

No se debe obviar que esta legislatura comienza con la reunión que el presidente del PNV, Xabier Arzalluz, mantuvo con representantes de KAS en marzo de 1991. De esta reunión, si bien de carácter secreto incluso para muchos de los principales cargos del PNV y del Gobierno Vasco, se tiene conocimiento a través de un acta confeccionada por los representantes del brazo político-social de ETA.

Este minucioso documento[32] contiene frases literales atribuidas a Arzalluz que ilustran la presunta voluntad del dirigente peneuvista y que, obviamente, involucran a su partido y, por ende, al propio Gobierno Vasco[33], durante la que habría reconocido que este último no estaba empleando con profusión la Ertzaintza contra ETA, ya que la organización terrorista no era el verdadero enemigo del PNV (San Sebastián y Gurruchaga, 2000: 50):

> «El Gobierno de Vitoria *jamás ha utilizado a la Ertzaintza* contra la banda terrorista, sino que, antes, al contrario, ha *frenado muchas actuaciones de la Policía Autónoma vasca*, especialmente en Guipúzcoa, y, desde luego, *jamás ha permitido* que existiera *flujo de información entre la Ertzaintza y la Policía Nacional*».
> *La cursiva es del autor.

Sí es cierto que, durante la época de Atutxa como consejero de Interior (1991-1998), la Ertzaintza se involucró de una manera creciente en la lucha contra ETA, incluyendo un aumento sustancial de efectivos de los AVCS en virtud de la Orden de 15 de julio de 1993.

El propio consejero Atutxa confirmaba la implicación de la PAV contra ETA y, por ende, del Gobierno Vasco, reconociendo que cumplían con su obligación ya que no podían «hacer distingos entre el delito cometido por un terrorista vasco y el de un carterista de donde fuera. El delito es delito y punto» (Arroyo, 2022).

Esta mayor implicación de la PAV iba a conllevar una reacción de ETA. La secuencia lógica de evolución de los acontecimientos desembocó en el asesinato del *ertzaina* Joseba Goikoetxea quien, además, era un histórico militante *jeltzale*, en lo que supuso «el

[32] El informe fue posteriormente intervenido durante una operación policial en mayo de 1992.

[33] Dado que la reunión tuvo lugar al comienzo de la presente legislatura, se considera que los comentarios vertidos harían alusión a la política planteada por el Gobierno Vasco en la anterior legislatura (III), motivo por el que se recogen igualmente en el apartado correspondiente a la misma.

primer atentado directo contra un miembro de la Ertzaintza y del PNV» (Deia, 1993, citado en Fernández *et al.*, 2021: 574)[34].

El asesinato de Goikoetxea generó un gran revuelo político en el seno del PNV y, por tanto, del Gobierno Vasco. Personalidades relevantes del partido[35] realizaron airadas intervenciones criticando el asesinato del agente, no tanto por su pasado como *ertzaina*, sino por su pública y dilatada militancia en el PNV durante más de veinticinco años, llegando a calificar el mismo como un ataque frontal contra el PNV (Fernández *et al.*, 2021; Grech, 2011; Olabarri, 2013).

Más airadas fueron las críticas del Presidente del PNV en esa época, Xabier Arzallus, quien llegó amenazar directamente a la organización terrorista (Díaz Herrera y Durán, 2002: 256): «¡Que ETA tome nota! Si vuelven a atacar a uno de los nuestros, que se preparen, porque somos más y podemos matarlos a todos ellos cuando queramos».

Otros miembros del Gobierno Vasco, como Juan María Atutxa, traspasaron la línea que años antes habían cruzado políticos populares o socialistas y culparon al brazo político-social de ETA de ser igualmente responsables, mencionando expresamente a HB, KAS o el propio diario *Egin*[36] (Fernández *et al.*, 2021; Grech, 2011; Olabarri, 2013).

---

[34] En noviembre de 1993, ETA asesinó al *ertzaina* Joseba Goikoetxea Asla, quien había ejercido como responsable de las unidades antiterroristas de la *Ertzaintza* desde 1986, en sustitución de Genaro García de Andoáin, hasta principios de 1993, cuando fue inhabilitado. Desde enero de 1992, investigaciones de la Guardia Civil confirmaron que miembros del comando *Bizkaia* habían realizado seguimientos sobre su persona para recoger información. Las actividades preparatorias finalizaron el 22 de noviembre de 1993, cuando Goikoetxea fue mortalmente herido mediante disparos, falleciendo a los cuatro días (Domínguez, 2009; Grech, 2011; Fernández *et al.*, 2021).

[35] Entre otros, Joseba Egibar, portavoz del partido; Iñaki Anasagasti, portavoz en el Congreso; Juan María Atutxa, consejero de Interior; Ramón Labayen, exalcalde peneuvista de San Sebastián, y Emilio Guevara, ex diputado general de Álava por el PNV (Deia ,1993, citado en Fernández *et al*., 2021: 575-577).

[36] Según el apartado *Hechos Probados* de la STS 480/2009, el diario *Egin* era un periódico escrito creado en 1977 perteneciente al grupo *Orain*, del cual se constató su absoluta dependencia política respecto a ETA, convirtiéndose en el medio de comunicación de HB y de la propia organización terrorista. Entre las diversas funciones de *Orain-Egin* se encontraban el mantener la cohesión interna del MLNV; servir como «instrumento de coacción e intimidación al servicio de todos los demás frentes de la organización terrorista» y presentar públicamente el ejercicio de la violencia como un fenómeno natural (Tribunal Supremo, 2009). En palabras de las juventudes del PNV, la labor de este diario se simplificaba aún más: «*Egin* apunta y ETA mata» (Díaz Herrera y Durán, 2002: 410).

5.2 El papel de la Ertzaintza

En esta legislatura, se puede considerar culminada la organización e implantación de la PAV en todo el territorio del País Vasco e iniciada su implicación real contra el terrorismo de ETA. Bajo la dirección del consejero de Interior Juan María Atutxa, la PAV comenzó su etapa de mayor intensidad en la lucha antiterrorista desarrollando diversas investigaciones contra ETA. La Ertzaintza apostó por la proactividad en vez de la reactividad.

De forma cuantitativa, aparte del número de operaciones desarrolladas contra ETA que se verá *ut infra*, es preciso destacar el aumento de los efectivos de los AVCS, que, en virtud de la Orden de 15 de julio de 1993, quintuplicaron la plantilla aprobada en el año 1986.

Cualitativamente, como continuación a la investigación de abril de 1990, agentes de los servicios de información de la Ertzaintza (AVCS) y del Grupo Especial de Intervención actuaron el 29 de agosto de 1991 contra los miembros del comando *Bizkaia* y sus colaboradores, ante las evidencias de la preparación de un nuevo atentado. Durante el desarrollo del dispositivo se produjo un tiroteo, falleciendo en el intercambio de disparos el miembro de ETA Juan María Ormazábal, *Tturko*, y siendo herido mortalmente el *ertzaina* Alfonso Mentxaka Lejona, miembro del Grupo Especial de Intervención (Santarén, 2016; Audiencia Nacional, 1995).

Los éxitos policiales se suceden, destacando, en enero de 1992, la operación contra la «red Easo», el aparato de extorsión de ETA que había puesto en el punto de mira a numerosos empresarios afines al PNV; la detención, ese mismo año, del etarra *Javi de Usánsolo*, tras una espectacular operación policial, prácticamente televisada en directo y la operación *Diru-Gutxi* en agosto de 1993, en colaboración con la policía francesa, contra la estructura de ETA destinada al cobro del «impuesto revolucionario»[37] (Díaz Herrera y Durán, 2002; Vasco Press, 1992a).

[37] Al día siguiente de la operación *Diru-Gutxi*, en una comparecencia, Juan María Atutxa mostró públicamente una serie de vídeos en los que se observaba a los detenidos «negociando» con uno de los empresarios extorsionados. En un claro ejemplo de imprudencia grave, los vídeos mostraron el coche particular del empresario, tratándose de Isidro Usabiaga Esnaola. Casi tres años después, el 26 de julio de 1996, ETA asesinaba en Ordizia (Gipuzkoa) al empresario (Barbería y Angulo, 1996; Díaz Herrera y Durán, 2002).

Tras el asesinato de Joseba Goikoetxea en noviembre de 1993, las operaciones policiales continuaron durante los siguientes años[38], si bien la etapa de mayor actividad de la Ertzaintza en la lucha antiterrorista contra ETA comenzaba a apagarse.

En los siguientes años se produjo un creciente descontento de las bases del cuerpo y un, cada vez mayor, distanciamiento con los mandos políticos, lo cual desembocó en acusaciones de falta de implicación contra ETA y la *kale borroka* (De Otálora, 1997; San Sebastián y Gurruchaga, 2000).

5.3 El papel de ETA

En línea con el final de la legislatura anterior, la organización terrorista ETA y su brazo político, HB, continuaban criticando la paulatina asunción de competencias que permitió alcanzar a la Ertzaintza su carácter de policía integral.

Al hilo de lo anterior, Jon Idígoras, portavoz de HB, posicionaba a la Ertzaintza del lado del Ejecutivo Central en la supuesta «confrontación Euskadi-Estado español» (Vasco Press, 1992d: 20).

A estos posicionamientos de la organización terrorista contribuyeron acontecimientos como la muerte del etarra Tturko, en un intercambio de disparos en el que también fue herido de muerte el *ertzaina* Alfonso Mentxaka Lejona.

Esta operación, fruto de una investigación previa, marcó un punto de no retorno para ETA con respecto a su posicionamiento contra la PAV. El propio agente Mentxaka, antes de fallecer en el hospital y plenamente consciente de este punto de inflexión, le compartió a su madre «qué de problemas va a traer eso [la muerte de Tturko]» (Santarén, 2016).

Mentxaka no se equivocaba y el fallecimiento de Tturko fue instrumentalizado por los aparatos mediáticos vinculados a la IA para atacar a la Ertzaintza. Desde el diario *Egin* al brazo político-social de ETA, representado por HB y por KAS, se negó la versión oficial, se difundió el mensaje del asesinato doloso de Tturko

[38] Detenciones en noviembre de 1994 de varios miembros del comando *Bizkaia*, operativo en el que falleció el miembro de ETA Ángel Irazabalbeitia; así como de un colaborador de ETA en ese mismo mes de noviembre (Guenaga e Intxausti, 1994; El País, 1994). Respecto de Ángel Irazabalbeitia, según el relato del fiscal de la Audiencia Nacional, fue el autor material del asesinato del *ertzaina* Joseba Goikoetxea el 22 de noviembre de 1993 (Grech, 2011).

y se criticó el salto cualitativo del cuerpo autonómico en su lucha contra ETA (Egin, 1991a; 1991b; 1991c).

De esta forma, la IA y ETA aplicaron con meridiana precisión la estrategia contenida en el *Barne Buletina* de 1990 y con esta versión alienada de la realidad, que buscaba criminalizar a la PAV, se allanaba el camino a cualquier posible actuación futura de ETA contra los agentes.

Las unidades dedicadas a la lucha antiterrorista, AVCS o BBT, y sus integrantes, se convirtieron en el objetivo de la organización terrorista ETA. El 25 de octubre de 1991, ETA difundió en un comunicado oficial la identidad de ocho miembros de esas unidades, entre ellos Joseba Goikoetxea, a quien tildaba de «despreciable torturador y asesino de encargo» (ETA, 1991; Grech, 2011).

La secuencia fue rápida. Tras el comunicado, miembros del comando *Bizkaia* realizaron seguimientos sobre Goikoetxea desde, al menos, enero de 1992, y el 22 de noviembre de 1993 fue mortalmente herido mediante disparos (Domínguez, 2009; Fernández *et al.*, 2021; Grech, 2011). En palabras de Olabarri (2013) «Goikoetxea fue un símbolo elegido por ETA para extender su amenaza a la Ertzaintza y a los militantes abertzales que se atreviesen a hacerle frente».

A raíz del atentado y de las acusaciones del PNV a ETA y a su entorno político-social, expuestas anteriores apartados, HB emitió un comunicado justificando que su perpetración era una consecuencia de la actividad de la Ertzaintza, que «por decisión política del PNV, quiere ser puesta en manos de la estrategia del Estado, convirtiéndola en un elemento represivo de primer orden contra las reivindicaciones de nuestro pueblo» y exigiendo la retirada de la PAV de la lucha antiterrorista (Grech, 2011; Olabarri, 2013).

Otros dirigentes de HB, como el coportavoz Floren Aoiz, se expresaron con mayor dureza acusando al PNV de haber «buscado y haber provocado», palabras que tuvieron que ser matizadas por el portavoz de la formación, Jon Idígoras, quien aclaró que el asesinato no podía considerarse un atentado contra el PNV y ni siquiera contra la Ertzaintza, sino que lo era contra «determinadas actitudes» (Fernández *et al.*, 2021: 579)

De forma material, estas palabras se tradujeron en la aparición en muchas comisarías de la PAV de pasquines del entorno de la IA con el mensaje «Si no nos atacas, yo no te ataco». Como bien

había expresado el propio Goikoetxea tiempo antes «tanto a ETA como a su mundo les duele que sea "gente de casa" la que va a por ellos. Pero soy vasco y seguiré viviendo en Euskadi» (Vasco Press, n. d., citado en Olabarri, 2013).

ETA no podía soportar que una parte de la sociedad vasca, simbólicamente representada a través de la lucha antiterrorista de la Ertzaintza, abandonase el tradicional discurso del conflicto entre Euskadi-Estado español y, como sociedad democrática, no comulgase con la actuación de una organización terrorista. La estrategia de ETA de fragmentar la Ertzaintza estaba fracasando.

5.4 Integración de datos de la legislatura

Esta legislatura se caracterizó por los frecuentes acercamientos entre el PNV y ETA. Así, a las negociaciones entre el partido *jeltzale* y HB, previas a las elecciones forales de mayo de 1991[39], les siguió la reunión secreta en marzo de 1991 entre Xabier Arzalluz y diversos representantes de KAS y, finalmente, las conversaciones oficiales entre HB y PNV de abril de 1992 para establecer un diagnóstico común sobre la violencia, fracasadas por la creciente influencia y control de KAS en el partido político (San Sebastián y Gurruchaga, 2000).

Especialmente destacable fue el encuentro secreto de marzo de 1991, en el que el representante del PNV, Xabier Arzalluz, reconoció que desde el Gobierno Vasco se estaba frenando la actuación de la Ertzaintza en tareas contraterroristas y, de mayor gravedad, que la organización terrorista no era el verdadero enemigo del partido (San Sebastián y Gurruchaga, 2000: 50).

No obstante, a pesar de las afirmaciones de Arzalluz, este periodo puede considerarse como el de mayor implicación de la Ertzaintza contra ETA, coincidiendo con la época de Atutxa como consejero de Interior entre 1991 y 1998. Aparte del aumento del número de efectivos dedicados a estas funciones (Orden de 15 de julio de 1993), se concatenaron varias operaciones policiales contra ETA: comando *Bizkaia*, «Red Easo», operación Diru-Gutxi, etc. (Díaz Herrera y Durán, 2002; Santarén, 2016; Audiencia Nacional, 1995; Vasco Press, 1992c).

[39] En enero de 1991, en vísperas de las elecciones forales de mayo, el PNV, al objeto de arrebatar al Diputación Foral de Gipuzkoa a EA, pacta con HB a cambio de apoyar el cambio de trazado de la autovía de Leizarán (San Sebastián y Gurruchaga, 2020).

La contra reacción de la organización terrorista no se hizo esperar, sobre todo por el fallecimiento del etarra Tturko y, en consonancia con la estrategia planificada en el documento EI *MLNV ante la Ertzaintza*, el 25 de octubre de 1991, ETA difundió un comunicado oficial con la identidad de ocho miembros de las unidades antiterroristas, entre ellos, Joseba Goikoetxea (ETA, 1991; Grech, 2011).

Dos años después, el antiguo jefe de los servicios de información de la PAV era tiroteado, convirtiéndose en el primer *ertzaina* asesinado premeditadamente por ETA que no tenía un pasado como militar o en las FCSE (Domínguez, 2009; Grech, 2011; Fernández *et al*., 2021).

Militante *jeltzale*, veterano *ertzaina*, miembro histórico del servicio de información de la PAV y hombre de confianza de los dirigentes del PNV, el asesinato de Joseba fue la forma en la que ETA decidió trasladar su amenaza. La organización terrorista no iba a permitir que una parte de la sociedad vasca, simbólicamente representada por la lucha antiterrorista de la PAV, se opusiera a sus designios.

Con este asesinato, ETA cumplía un doble objetivo, golpear a la Ertzaintza y «advertir al PNV que se acababan los tiempos de impunidad» (Landaburu, 1994: 36).

6 Conclusiones

Podría parecer obvio que, tras su reconstitución como policía integral en el País Vasco, la Ertzaintza debía ejercer, como una pieza más, su papel dentro del complejo tablero de ajedrez que constituye el modelo policial español. Y eso, obvia y principalmente, incluía la lucha contra ETA.

Sin embargo, el desarrollo de este artículo ha permitido evidenciar que ese pensamiento no era compartido, al menos no inicial, o no públicamente, por las autoridades político-administrativas encargadas de construir, implementar, ejecutar y evaluar la política pública antiterrorista en el ámbito autonómico vasco, esto es, el Gobierno Vasco y, por evidente analogía, el PNV.

Tras identificar la tríada de los actores protagonistas en esta política pública, (Gobierno Vasco-Ertzaintza-ETA), el análisis realizado de las interacciones entre sí o con terceros, así como de sus propias conductas, demuestra que las respuestas del Gobierno

Vasco a la violencia terrorista desde el punto de vista policial variaron en función del contexto de cada momento.

Así, a lo largo de trece años, el Gobierno Vasco pasó de una postura inicial de inacción y ambigüedad frente a ETA a una implicación directa y coordinada en la lucha antiterrorista, a medida que la realidad se imponía al idealismo y, en cierto modo, a la voluntad partidista.

No obstante, esta evolución no fue lineal ni estuvo exenta de contradicciones y claroscuros; más bien estuvo marcada por puntos de inflexión críticos, como ataques, asesinatos, acuerdos políticos y fracasos de negociaciones, que obligaron al Gobierno Vasco a reconsiderar sus estrategias.

Cada legislatura analizada presenta rasgos propios condicionados por el contexto vigente en cada momento, pero se observa un patrón general a medida que la amenaza de ETA se intensificaba y que el entorno político evolucionaba desde la transición democrática y los primeros pactos hasta el amplio consenso contra la violencia de finales de los ochenta. Las estrategias del Gobierno Vasco fueron ajustándose gradualmente de la pasividad a la acción.

Inicialmente, primó una visión idealista, o quizás negacionista, que resultó insostenible frente a la violencia real; después vino una fase de transición en la que convivieron intentos de diálogo y medidas incipientes; finalmente, ante la evidencia de que ETA no haría concesiones y que la sociedad demandaba seguridad, el Gobierno Vasco asumió plenamente su responsabilidad en la lucha antiterrorista, acompañada, eso sí, de acercamientos permanentes a la organización terrorista o a su brazo político-social.

No en vano, haber sido creada como una «policía del partido para el partido», arrastraba a la Ertzaintza a luchar contra el terrorismo de ETA con calculada ambigüedad en muchos aspectos del conflicto y, obligada por el PNV, hacía que sus responsabilidades antiterroristas fueran cuestionadas en algunas ocasiones, tanto por una presunta inacción o por una forma de proceder que se salía de los patrones lógicos, generando la sensación de ser cómplice involuntario de la organización terrorista.

Para la Ertzaintza, la relación con la organización terrorista no fue sencilla ni cómoda, pero, como se expuso en la introducción, las relaciones entre «hermanos» no tienen por qué serlo.

En definitiva, como conclusión central del presente artículo, se puede sintetizar que la política antiterrorista del Gobierno Vasco frente a ETA experimentó un proceso de evolución desde el *laissez-faire* hasta la acción decidida, con la Ertzaintza como actor principal en esa transformación, y que ese desarrollo solo fue posible cuando el Gobierno Vasco abandonó la ambigüedad inicial y asumió plenamente su responsabilidad institucional frente al terrorismo.

Bibliografía

Alfaro, E. (1985a). Las organizaciones terroristas sitúan a las instituciones autónomas en su punto de mira. *El Correo Español- El Pueblo Vasco*. 8 de marzo, p. 17.

—. (1985b). Amagos a la Ertzantza. *El Correo Español- El Pueblo Vasco*. 8 de marzo, p. 17.

—. (2022). En el corazón de Berroci [en línea]. El Correo. [Consulta: 4 marzo 2026]. Disponible en: https://www.elcorreo.com/especial/40-aniversario-ertzaintza/embrion-ertzaintza-berroci-alava-exclusiva-elcorreo-20220206103217-nt.html

Arroyo, M. (1986). Interior admite que la Ertzantza usó cartuchos de postas «que pueden herir, pero nunca matar». *El Correo Español- El Pueblo Vasco*.

—. (2022). La Ertzaintza de todos [en línea]. El Correo. [Consulta: 4 marzo 2026]. Disponible en: https://www.elcorreo.com/especial/40-aniversario-ertzaintza/ertzaintza-40-aniversario-20220206114524-nt.html

Audiencia Nacional. (1994). Sentencia 2/1994 de la Sección Segunda de la Sala de lo Penal, de 29 de enero.

—. (1995). Sentencia 69/1995 de la Sección Tercera de la Sala de lo Penal, de 18 de diciembre.

—. (1997). Sentencia 7/1997 de la Sección Tercera de la Sala de lo Penal, de 28 de enero.

—. (2007). Sentencia 73/2007 de la Sección Tercera de la Sala de lo Penal, de 19 de diciembre.

Balantx, P. (1982). Policía Autónoma ¿CONTRA ETA? [en línea]. Punto y Hora de Euskal Herria. N.º 276, pp. 11-12. [Consulta: 4 marzo 2026]. Disponible en: https://mega.nz/file/g4knAK5Y#w_0VbN3BSO5JH5A5XVCs1y1xsrGIQdv5SmoGSWRlEEA

Barbería, J. L. y Angulo, C. (1996). ETA asesina a tiros a un industrial de Guipúzcoa que había pagado el 'impuesto revolucionario' [en línea]. El País. [Consulta: 4 marzo 2026]. Disponible en: https://elpais.com/diario/1996/07/27/espana/838418419_850215.html

Bueno Fernández, A. (2020). El targeting como capacitador de las operaciones militares en OTAN. *Revista del Instituto Español de Estudios Estratégicos*. N. º15, pp. 13-41.

Buesa, M. (2012). Los presos de ETA y el juego del gallina [en línea]. Documento de trabajo. Instituto de Análisis Financiero de la Universidad Complutense de Madrid. N.º 13. [Consulta: 4 marzo 2026]. Disponible en: https://docta.ucm.es/rest/api/core/bitstreams/e033bc42-1a6c-4a6f-9445-93b419cd6d7f/content

Cartwright, M. (2022). Cipayo [Sepoy] [en línea]. World History Encyclopedia. [Consulta: 4 marzo 2026]. Disponible en: https://www.worldhistory.org/trans/es/1-21089/cipayo/

C. V., J. (1985). El Parlamento vasco aprueba hoy un documento contra la violencia. *El Correo Español- El Pueblo Vasco*. 14 de marzo, p. 13.

Dávila, C. (2006). *Ertzaintza: Historia de la Policía Autónoma Vasca (1936-2006)*. Bilbao. Elea Argitaletxea.

De Miguel, C. (2021). El sufrimiento de los menores provocado por ETA. Veintiún ataúdes blancos [en línea]. Revista Internacional de Estudios sobre Terrorismo. N.º 2, pp. 58-69. [Consulta: 4 marzo 2026]. Disponible en: https://observatorioterrorismo.com/eedyckaz/2021/04/4-El-sufrimiento-de-los-menores-provocado-por-ETA-Carlos-De-Miguel.pdf

De Otálora, O. B. y Calabor, L. (1995). Ertzainas de élite. La unidad secreta de la policía vasca [en línea]. defensa.com. [Consulta: 4 marzo 2026]. Disponible en: https://www.defensa.com/ayer-noticia/ertzainas-elite-unidad-secreta-policia-vasca

—. (1997). Los sindicatos dicen que la Ertzaintza carece de medios ante las algaradas. *El Correo*. 8 de febrero, p. 17.

Díaz Herrera, J. y Durán, I. (2002). *ETA. El saqueo de Euskadi*. 3.ª ed. Barcelona, Planeta.

Domínguez, F. (2009). La Ertzaintza contra ETA [en línea]. El Correo. [Consulta: 4 marzo 2026]. Disponible en: https://www.elcorreo.com/vizcaya/20090627/politica/ertzaintza-contra-20090627.html

—. (2022a). El brutal acoso de ETA y de su entorno político [en línea]. El Correo. [Consulta: 4 marzo 2026]. Disponible en: https://www.elcorreo.com/especial/40-aniversario-ertzaintza/brutal-acoso-entorno-20220206174131-nt.html

—. (2022b). Los 'topos' de ETA [en línea]. El Correo. [Consulta: 4 marzo 2026]. Disponible en: https://www.elcorreo.com/especial/40-aniversario-ertzaintza/topos-ertzaintza-eta-de-juana-chaos-20220206134632-nt.html

Egin. (1988a). La explosión de una bomba en las vías férreas, a su paso por Legazpia, ocasionó la muerte de un ertzaina. *Egin*. 17 de octubre, pp. 6-7.

—. (1988b). Pacto de Ajuria-Enea (texto íntegro) [en línea]. Egin. [Consulta: 4 marzo 2026]. Disponible en: https://www.naiz.eus/media/asset_publics/resources/001/068/322/original/Pacto-ajuria-enea-texto-integro.pdf

—. (1991a). Un muerto y dos heridos en una emboscada de la Ertzantza. *Egin*. 30 de agosto, p. 1.

—. (1991b). Un ertzaina mató a Ormazabal de un tiro a quemarropa. *Egin*. 31 de agosto, p. 3.

—. (1991c). KAS: «La Ertzantza ha pasado la reválida para catalogarse como policía represiva». *Egin*. 31 de agosto, p. 5.

El Correo. (1980). En Berroci (Álava) se entrenan los futuros componentes del cuerpo de seguridad de las Instituciones vascas. *El Correo Español-El Pueblo Vasco*. 13 de julio, p. 17.

—. (1983a). Un hertzaina, presunto implicado en el secuestro de Orbegozo. *El Correo Español-El Pueblo Vasco*. 17 de enero, p. 9.

—. (1983b). ETA-m asaltó a la Ertzaina pero no quiere enfrentarse a ella. *El Correo Español-El Pueblo Vasco*. 3 de marzo, p. 12.

—. (1983c). Retolaza: «Es el ataque más directo contra las instituciones vascas». *El Correo Español-El Pueblo Vasco*. 3 de marzo, p. 13.

—. (1983d). Garoikoetxea: «ETA-m, enfrentada al pueblo». *El Correo Español-El Pueblo Vasco*. 3 de marzo, p. 13.

El Mundo. (1987). El Pacto de Madrid [en línea]. [Consulta: 4 marzo 2026]. Disponible en: https://www.elmundo.es/eta/documentos/pacto_madrid.html

ETA. (1980). Comunicado. *Egin.* N.º 698, p. 28.

—. (1983). Comunicado. *Egin.* N.º 1669, p. 3.

—. (1985). Comunicado. *Egin*. 9 de marzo, p. 3.

—. (1986a). Comunicado. *Egin*. 24 de octubre, p. 10.

—. (1986b). Comunicado. *Egin*. 5 de noviembre, p. 6.

—. (1988). Comunicado. *Egin*. 20 de octubre, p. 6.

—. (1989). Comunicado. Egin. 27 de mayo, p. 4.

—. (1990). Comunicado. *Egin*. 5 de septiembre, pp. 1, 4.

—. (1991). Comunicado. *Egin*. 25 de octubre, pp. 4-5.

Fernández de Vallejo, M. (1986). Con esta operación espero que se callen todas las tonterías que se han dicho sobre la Ertzantza. *El Correo Español-El Pueblo Vasco*. 3 de noviembre, p. 11.

Fernández Redondo, I. *et al*. (2021). ETA contra la Ertzaintza. En: Pérez Pérez, J. A. (coord.). *Historia y Memoria del Terrorismo en el País Vasco II 1981-1994.* Volumen II. Polonia, Confluencias, pp. 525-581.

Etxarri, T. (1989). Corcuera y Lasa se reúnen hoy para firmar el despliegue de la Ertzaintza [en línea]. El País. [Consulta: 4 marzo 2026]. Disponible en: https://elpais.com/diario/1989/02/13/espana/603327611_850215.html

García Varela, P. (2022). Los menores de edad víctimas mortales de ETA [en línea]. Pasado y Memoria. N.º 24, pp. 322-341. [Consulta: 4 marzo 2026]. Disponible en: https://doi.org/10.14198/PASADO2022.24.13

Garrigó, A (1984). La decisión de Bélgica de entregar dos etarras ha sido calificada de histórica. *La Vanguardia*. 15 de julio.

Guenaga Bidauzarraga, A. e Intxausti, A. (1994). KAS arremete contra el PNV y la Ertzaintza en el homenaje al etarra muerto en el tiroteo de Loiu [en línea]. El País. [Consulta: 4 marzo 2026]. Disponible en: https://elpais.com/diario/1994/11/20/espana/785286001_850215.html

Departamento de Cultura y Política Lingüística. (2019). itzuli. Itzultzaile neuronala [en línea]. Gobierno Vasco, Departamento de Cultura y Política Lingüística. [Consulta: 4 marzo 2026]. Disponible en: https://www.euskadi.eus/traductor/

Gorospe, P. (1989). El Ejecutivo vasco cree "trascendental" el acuerdo sobre la Ertzaintza [en línea]. El País. [Consulta: 4 marzo 2026]. Disponible en: https://elpais.com/diario/1989/02/15/espana/603500417_850215.html

—. (1990). La Ertzaintza captura en Bilbao y Lekeitio a tres colaboradores del 'comando Vizcaya' [en línea]. El País. [Con-

sulta: 4 marzo 2026]. Disponible en: https://elpais.com/diario/1990/04/05/espana/639266404_850215.html

Grech, M. J. (2011). Joseba Goikoetxea, creador de la unidad antiterrorista de la Ertzaintza, y tres víctimas más [en línea]. Libertad Digital. [Consulta: 4 marzo 2026]. Disponible en: https://www.libertaddigital.com/espana/in-memoriam/joseba-goikoetxea-creador-de-la-unidad-antiterrorista-de-la-ertzaintza-y-tres-victimas-mas-10716/

Jar Couselo, G. (1995). *Modelo policial español y policías autónomas*. Madrid, Dykinson.

Knoepfel, P. et al. (2007). Hacia un modelo de análisis de políticas públicas operativo. Un enfoque basado en los actores, sus recursos y las instituciones [en línea]. Ciencia Política. (3), pp. 6-29. [Consulta: 4 marzo 2026]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3663617.pdf&ved=2ahUKEwij_K6i2oaTAxVBRv4FHQmrD1AQFnoECA0QAQ&usg=AOvVaw1iDYUq2Xr6uTbGymd-LYwu

Landaburu, G. (1994). Pelea entre hermanos [en línea]. *Cambio 16*. N.º 1202, pp. 36-40.

López Fonseca, O. (1993). Los planes de ETA contra la "Ertzaintza": documentos de la banda apuntan cómo "dividir" a la Policía vasca con atentados [en línea]. *Época*. N.º 458, pp. 38-39.

Mata López, T. (2018). *Terrorismo y comportamiento político: España y el caso de ETA*. Universidad Autónoma de Madrid.

Méndez, J. (1986). García de Andoaín fue precursor de la investigación terrorista. *El Correo Español- El Pueblo Vasco*. 3 de noviembre, p. 8.

Moreno, I. (2023). *La organización del sistema de seguridad pública, especial referencia a la policía autónoma vasca, la Ertzaintza* [trabajo de fin de máster]. Escuela Superior de las Fuerzas Armadas.

Moreno Bibiloni, I. (2021). De la indiferencia frente al terror a la movilización ciudadana. En: Pérez Pérez, J. A. (coord.). *Historia y Memoria del Terrorismo en el País Vasco II 1981-1994 - Volumen II*. Polonia, Confluencias, pp. 591-635.

M. P., A. (2008). Los 25 asesinatos de De Juana Chaos [en línea]. Radio Televisión Española. [Consulta: 4 marzo 2026]. Disponible en: https://www.rtve.es/noticias/20080801/25-asesinatos-de-juana-chaos/124751.shtml

Olabarri, D. S. (2013). El día en el que ETA puso en la diana a la Ertzaintza y al PNV [en línea]. El Correo. [Consulta: 4 marzo 2026]. Disponible en: https://www.elcorreo.com/vizcaya/20131122/mas-actualidad/politica/eta-puso-diana-ertzaintza-201311191230.html

País Vasco. (1993). Orden de 15 de julio de 1993, del Consejero de Interior, por la que se reestructura parcialmente la estructura de la plantilla de la Ertzaintza, modificando el contenido actual de la aprobada por Orden de 18 de enero de 1988 [en línea]. Boletín Oficial del País Vasco. 22 de julio, núm. 138. [Consulta: 4 marzo 2026]. Disponible en: https://www.euskadi.eus/web01-bopv/es/bopv2/datos/1993/07/9302415a.pdf

—. (1986). Orden de 20 de mayo de 1986, del Departamento de Interior, por la que se aprueba la estructura funcional del Cuerpo de Policía de la Comunidad Autónoma del País Vasco [en línea]. Boletín Oficial del País Vasco. 30 de mayo, núm. 105. [Consulta: 4 marzo 2026]. Disponible en: https://www.euskadi.eus/web01-bopv/es/bopv2/datos/1986/05/8601248a.pdf

Panisello, S. (2016). Extradiciones de Francia a España: treinta años de envíos [en línea]. Historia Actual Online. 39(1), pp. 29-38. [Consulta: 4 marzo 2026]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5411290.pdf

Punto y Hora de Euskal Herria. (1990). La Ertzantza está ocupando deliberadamente una trinchera en el actual enfrentamiento con ETA [en línea]. Punto y Hora de Euskal Herria. N.º 569, pp. 6-9. [Consulta: 4 marzo 2026]. Disponible en: https://mega.nz/file/8wVXXJga#V9I3TLhK46R8e0lCkzu0IsztpvqSYh4xP29WKlgwB9w

Reventós, J. (1993). *Misión en París. Memorias de un embajador*. Barcelona, Edicions 62.

Ruiz de Azúa, V. (1986). El dictamen de los expertos sobre la violencia en Euskadi sólo se hará público parcialmente [en línea]. El País. [Consulta: 4 marzo 2026]. Disponible en: https://elpais.com/diario/1986/03/20/espana/511657214_850215.html

—. (1989). Superposición o sustitución [en línea]. El País. [Consulta: 4 marzo 2026]. Disponible en: https://elpais.com/diario/1989/02/14/espana/603414003_850215.html

Sánchez, M. y Simón, M. (2017). *Historia de un desafío. Cinco décadas de lucha sin cuartel de la Guardia Civil contra ETA.* Barcelona, Península.

San Sebastián, I. y Gurruchaga, C. (2000). *El Árbol y las nueces. La relación secreta entre ETA y PNV*. 12.ª ed. Madrid, Temas de Hoy.

Santarén, E. (2016). Le acribillaron a tiros y él no podía matar una mosca [en línea]. Noticias de Guipúzcoa. [Consulta: 4 marzo 2026]. Disponible en: https://www.noticiasdegipuzkoa.eus/politica/2016/08/28/le-acribillaron-tiros-podia-matar-4056986.html

Tribunal Constitucional. (2004a). Sentencia 5/2004, de 16 de enero de 2004. Recurso de amparo 2330-2003. Promovido por Batasuna frente a la Sentencia de la Sala Especial del artículo 61 LOPJ del Tribunal Supremo que decretó su ilegalización [en línea]. Boletín Oficial del Estado. 12 de febrero, núm. 37. [Consulta: 4 marzo 2026]. Disponible en: https://www.boe.es/boe/dias/2004/02/12/pdfs/T00023-00063.pdf

—. (2004b). Sentencia 6/2004, de 16 de enero de 2004. Recurso de amparo 3153-2003. Promovido por Herri Batasuna frente a la Sentencia de la Sala Especial del artículo 61 LOPJ del Tribunal Supremo que decretó su ilegalización [en línea]. Boletín Oficial del Estado. 12 de febrero, núm. 37. [Consulta: 4 marzo 2026]. Disponible en: https://www.boe.es/boe/dias/2004/02/12/pdfs/T00063-00068.pdf

Tribunal Europeo de Derechos Humanos. (2009). Caso Herri Batasuna y Batasuna Vs. España. Solicitudes n.º 25803/04 y 25817/04 [en línea]. Tribunal Europeo de Derechos Humanos (Sección Quinta). [Consulta: 4 marzo 2026]. Disponible en: https://hudoc.echr.coe.int/spa?i=001-93348

Tribunal Supremo. (2003). Sentencia de la Sala Especial del Artículo 61 de la Ley Orgánica del Poder Judicial, de 27 de marzo de 2003.

—. (2009). Sentencia 480/2009 de la Sala de lo Penal, de 22 de mayo.

—. (2014). Sentencia 311/2014 de la Sala de lo Penal, de 16 de abril.

Unzueta Kareaga, H. (2016). *Nanclares vis a vis. Cara a cara con la disidencia de ETA*. San Sebastián, Erein.

Vasco Press. (1992a). La Ertzaintza: Símbolo de autogobierno. *Crónica Vasco Press*. N.º 540, pp. 1-4.

—. (1992b). Los recuerdos de Retolaza. *Crónica Vasco Press*. N.º 540, pp. 5-13.

—. (1992c). Atutxa y el Futuro. *Crónica Vasco Press*. N.º 540, pp. 14-17.

—. (1992d). Encuesta: La opinión de los partidos sobre la Ertzaintza. *Crónica Vasco Press*. N.º 540, pp. 18-23.

—. (1992e). Los consejos del ministro Barrionuevo. *Crónica Vasco Press*. N.º 540, pp. 31-33.

Capítulo séptimo

Adaptación del mando y control (C2) de las Fuerzas Armadas (FAS) españolas a las Operaciones Multidominio (MDO)

Fernando Casado Yagüe

Resumen

La aparición de nuevas y complejas amenazas, el exponencial desarrollo tecnológico y la necesidad de poder actuar en todos los dominios de forma sinérgica, ya sea en los físicos como en los no físicos, han generado un nuevo enfoque para las operaciones militares: el multidominio. En este contexto, las Fuerzas Armadas (FAS) españolas afrontan el reto de adaptar su sistema de mando y control (C2) para que la Fuerza Conjunta (FC) pueda responder con eficacia a estos escenarios caracterizados por su complejidad, incertidumbre y dinamismo.

La tecnología se configura como un elemento clave para alcanzar la agilidad que requieren las Operaciones Multidominio (MDO). La conectividad, la gestión del dato en un campo de batalla totalmente sensorizado o el empleo de tecnologías emergentes, como la inteligencia artificial (IA) o el 5G, se convierten en una prioridad en este proceso. Sin embargo, el factor humano, a través de una adecuada formación y un liderazgo que potencie la delegación de autoridad, la iniciativa y la innovación, marcará el éxito o el fracaso del tránsito hacia el enfoque multidominio.

A través de un análisis detallado de las publicaciones nacionales, entre ellas el reciente Plan de implantación del JEMAD, y de entrevistas a expertos involucrados en el desarrollo del concepto MDO, el presente trabajo busca obtener una visión realista y objetiva de la situación actual, que permita valorar si las FAS avanzan en la dirección correcta para adaptarse a los desafíos de las Operaciones Multidominio.

Palabras clave

Operaciones Multidominio (MDO), Mando y control de las operaciones multidominio (C2MDO), Fuerza Conjunta (FC), Sistema de Mando y Control Nacional (SC2N), Nube de combate.

Adaptation of the Spanish Armed Forces Command and Control to Multi-Domain Operations

Abstract

The emergence of new and complex threats, the exponential development of technology, and the need to operate synergistically across all domains, both physical and non-physical, have given rise to a new approach to military operations: the multidomain concept. In this context, the Spanish Armed Forces (FAS) face the challenge of adapting their Command and Control (C2) system so that the Joint Force can respond effectively to scenarios characterized by complexity, uncertainty, and dynamism.

Technology emerges as a key enabler for achieving the agility required in Multidomain Operations (MDO). Connectivity, data management on a fully sensorized battlefield, and the use of emerging technologies such as Artificial Intelligence (AI) and 5G become priorities in this transformation process. However, it will be the human factor, through appropriate training and leadership that fosters delegated authority, initiative, and innovation, that ultimately determines the success or failure of the transition toward the multidomain approach.

Through a detailed analysis of national publications, including the recent Implementation Plan of the Chief of the Defence Staff (JEMAD), and interviews with experts involved in the develop-

ment of the MDO concept, this study seeks to provide a realistic and objective view of the current situation. Its aim is to assess whether the FAS are moving in the right direction to meet the challenges posed by Multidomain Operations.

Key words

Multidomain Operations (MDO), Multidomain operations command and control (C2MDO), Joint Force, National Command and Control System (SC2N), Combat cloud.

Lista de abreviaturas

A2/AD	Denegación de acceso y área / Anti-access Area Denial
IA	Inteligencia Artificial / Artificial Intelligence
BOE	Boletín Oficial del Estado
C2	Mando y Control / Command and Control
C2MDO	Mando y control de las operaciones multidominio
CE	Concepto exploratorio
CECOPI	Centro de Coordinación Operativa Integrado
CEMFAS	Curso de Estado Mayor de las Fuerzas Armadas
CESEDEN	Centro Superior de Estudios de la Defensa Nacional
CESTIC	Centro de Sistemas y Tecnologías de la Información y las Comunicaciones
CIS / TIC	Sistemas y Tecnologías de la Información y Comunicaciones
COEM	Centro de Operaciones Electromagnéticas
COP	Imagen Operacional Común / Common Operational Picture
COS	Centros de Operaciones de Seguridad
DCS	Seguridad centrada en el dato / Data Centric Security
DIGEREM	Dirección General de Reclutamiento y Enseñanza Militar
DIVPLA	División de Planes
DOPE	Departamento de Operaciones

DoD	Departamento de Defensa de Estados Unidos
E2T	Especialidad de Segundo Tramo
EDT	Tecnologías Emergentes y Disruptivas
EGLET	Escuela de Guerra y Liderazgo del Ejército de Tierra
EMACON	Estado Mayor Conjunto de la Defensa
EMAD	Estado Mayor de la Defensa
ESFAS	Escuela Superior de las Fuerzas Armadas
EO	Entorno operativo
ET	Ejército de Tierra
EW	Guerra electrónica / Electronic Warfare
FAS	Fuerzas Armadas
FC	Fuerza Conjunta
FCAS	Future Combat Air System
FOC	Capacidad Operacional Final / Final Operational Capability
GT	Grupo de Trabajo
HQ	Cuartel General / Headquarters
I3D	Infraestructura Integral de Información para la Defensa
IOC	Capacidad Operacional Inicial / Initial Operational Capability
JADC2	Joint All-Domain Command and Control
JEMAD	Jefe del Estado Mayor de las Fuerzas Armadas
JOA Area	Área de Operaciones Conjunta / Joint Operational
JOC	Centro Conjunto de Operaciones / Joint Operational Centre
LA	Línea de Actuación
LoE	Línea de esfuerzo / Line of Effort
MADOC	Mando de Adiestramiento y Doctrina
MAUEC	Ministerio de Asuntos Exteriores, Unión Europea y Cooperación

MCCE	Mando Conjunto del Ciberespacio
MDO	Operaciones Multidominio / Multi-Domain Operations
MINISDEF	Ministerio de Defensa
ML	Aprendizaje Automático / Machine Learning
MoM	Mando orientado a la misión / Mission Command
MOPS	Mando de operaciones
NCOP	NATO Common Operational Picture
OODA	Observación, Orientación, Decisión y Acción
OTAN/NATO	Organización del Tratado del Atlántico Norte
PDC	Publicación Doctrinal Conjunta
SC2N	Sistema de Mando y Control Nacional
SFD	Situación final deseada
TD	Transformación digital
TOA	Transferencia de Autoridad / Transfer of Authority
TTP	Tácticas, Técnicas y Procedimientos
UME	Unidad Militar de Emergencias
VUCA	Volatilidad, incertidumbre, complejidad y ambigüedad

1 Introducción

«Lo único que hay más difícil que introducir una idea nueva en la mente de un militar es sacar una vieja»

Basil H. Liddell Hart

Las Operaciones Multidominio[40] (MDO) se han configurado como una solución para afrontar los escenarios actuales, caracterizados por un gran dinamismo, complejidad y desarrollo tecnológico. Los esfuerzos para implantar el concepto[41] doctrinal en las Fuerzas Armadas (FAS) españolas han dado como resultado publicaciones como el «Concepto Exploratorio (CE) Mando y Control de las Operaciones Multidominio» o «Transformación digital de las FAS para el combate multidominio». En este marco, el mando y control (C2) se configura como un elemento clave para poder aplicar el enfoque multidominio de forma efectiva (EMAD, 2023).

Sin embargo, esta aplicación del mando y control de las operaciones multidominio (C2MDO) requiere un cambio de mentalidad estructural en la organización y una evolución tecnológica que debe ser planificada y medida. Las FAS están llevando a cabo iniciativas de desarrollo tecnológico, como el Sistema de Mando y Control Nacional (SC2N) o la nube de combate, dentro de un proceso de transformación digital (TD).

El objetivo es poder responder a las necesidades de las MDO, poder facilitar una mejor gestión de la información y alcanzar una mayor interoperabilidad entre los diferentes elementos de la Fuerza Conjunta en todos los dominios de las operaciones. Sin embargo, surgen numerosos desafíos en el ámbito humano, organizacional y tecnológico. La formación multidominio, consolidar el liderazgo más adecuado para este tipo de operaciones o gestionar la avalancha de datos e información para alcanzar la

[40] Las MDO se definen como «aquellas operaciones realizadas por la Fuerza Conjunta (FC) que, por su agilidad y complejidad, necesitan de una adecuada interoperabilidad y conectividad que posibiliten un control distribuido de los medios para permitir la integración de todas sus capacidades y así poder producir efectos en y desde cualquiera de los dominios de operación» (JEMAD, 2020: 5).

[41] El concepto de MDO surge en los Estados Unidos para poder hacer frente al desarrollo de sistemas y despliegues Anti-Acceso/Denegación de Área (A2/AD) desarrollados por China y Rusia, que evitan la aproximación de fuerzas a su territorio y una vez dentro, limitan, en gran medida, su libertad de acción (US DoD, 2020).
US dispone de publicaciones doctrinales como el «US Army. FM 3-0 Operations» (2022) y está enfocado en aplicar el concepto Joint All Domain Command and Control (JADC2), que tiene como objetivo conectar todas las plataformas, armas y sensores a través de todos los dominios a una sola red, de forma que permita una sincronización de todas las capacidades.

superioridad en el ciclo de la decisión son retos que deben superarse para alcanzar la capacidad multidominio.

Por todos estos motivos, el jefe de Estado Mayor de la Defensa (JEMAD) aprobó, en el mes de febrero del año 2025, el «Plan de implantación de las MDO en las FAS». Este documento tiene como objeto principal establecer una progresiva adaptación a estas operaciones cuya situación final deseada (SFD) es capacitar a la FC para planear, ejecutar y conducir las MDO (EMAD, 2025).

Esta investigación tiene el objetivo principal de determinar el grado de necesidad y suficiencia de las medidas que se están implementando para adaptar el factor humano, la estructura y los procesos de mando y control a las MDO en el nivel operacional y en el marco de las FAS. Además, este trabajo pretende contribuir y aportar valor a la mejora del proceso de adaptación de estas operaciones a las FAS españolas debido a la coincidencia temporal con el «Plan de implantación del JEMAD» y la reciente incorporación a la doctrina de las FAS españolas del concepto MDO.

Para ello, se plantea la validación o refutación de la siguiente hipótesis: «Las Fuerzas Armadas españolas están implementando medidas necesarias y suficientes para adaptar el factor humano, la estructura y los procesos de mando y control a las Operaciones Multidominio».

Este trabajo se acota temporalmente desde el año 2020, fecha de la incorporación del concepto MDO a la doctrina nacional (JEMAD, 2020), hasta las acciones que se están llevando a cabo en la actualidad. La publicación del «Plan de implantación del JEMAD», en el mes de febrero de 2025, supone un hito fundamental para el avance multidominio en las FAS.

1.1 Factores de estudio

Para materializar el análisis y valorar si las medidas que se están aplicando son necesarias y suficientes, el presente estudio ha identificado tres (3) factores en la publicación «CE. Mando y Control de las Operaciones Multidominio» (JEMAD, 2024b: 13). Este documento incide en las particularidades del C2 para las MDO y establece el factor humano, los procesos y la estructura del C2MDO como los elementos esenciales para evolucionar al enfoque multidominio. Por este motivo, estos tres factores se han considerado el marco para analizar la suficiencia y necesidad de

las medidas que se están adoptando en las FAS para adaptar el C2MDO.

Con respecto al primer factor, el avance hacia la adaptación de las MDO implica una evolución en la forma actual de materializar el C2 por parte de las personas. Cuanto mayor es la complejidad y la incertidumbre más importancia cobra el factor humano y en concreto, el aspecto de la formación y el liderazgo. El avance hacia las MDO implica potenciar un liderazgo dispuesto a asumir riesgos y experimentar con enfoques innovadores y una cultura de delegación de autoridad, como el estilo del MoM, algo esencial en entornos complejos como las MDO. La formación del personal de las FAS en la complejidad inherente a los entornos actuales multidominio y el manejo de tecnologías emergentes serán necesarios para la aplicación efectiva de la visión multidominio.

Con respecto a los procesos en el C2MDO, el reto radica en gestionar la avalancha de datos e información que está disponible en los entornos actuales. Procesar esa información y presentársela al comandante o el combatiente, que debe tomar la decisión o actuar, requiere una evolución tecnológica que incremente la conectividad con soluciones como la nube de combate. La conectividad, el gobierno del dato y la incorporación de EDT, como la IA o el 5G, son elementos esenciales para asegurar una adecuada adaptación a las MDO.

El tercer factor son las estructuras de C2 en las MDO. La necesidad de compatibilizar dominios, niveles y cadenas de mando a la hora de ejecutar una MDO, supone un desafío para el que será fundamental implementar modelos y estructuras ágiles. Adoptar inicialmente un C2 apropiado y poder modificarlo cuando el establecido no sea el adecuado o haya cambiado la situación, se configura como un elemento clave.

1.2 Variables de estudio

Por otro lado, se identifican ocho (8) variables, que se encuentran contenidas en el factor humano, procesos y estructura del C2MDO (ver figura 1). Estas variables han sido seleccionadas[42], principalmente, con base en la publicación *PDC-01(B) Doctrina para el empleo de las FAS*, donde se determinan cuáles son los

[42] Además de la *PDC-01(B) Doctrina para el empleo de las FAS*, las variables se han establecido del análisis de los documentos «CE. Mando y Control de las Operaciones Multidominio y CE. Evolución de la FC hacia las MDO».

factores clave de las MDO (Ministerio de Defensa, 2024d: 57). En concreto:

– *Formación*. Dentro del factor humano, la formación se constituye como un pilar esencial para efectuar una adecuada adaptación del C2 a las MDO, ya que permite proporcionar al personal, civil y militar, las herramientas necesarias para operar en la complejidad y el dinamismo que caracterizan estas operaciones.

  El aprendizaje e incorporación de las nuevas tecnologías, el conocimiento en profundidad de todos los dominios de las operaciones con sus correspondientes interacciones entre ellos, el enfoque integral para la creación de sinergias o la toma de decisiones son algunos de los factores esenciales que debe incorporar la formación multidominio.

  Además, los ejercicios de instrucción y adiestramiento deberán diseñarse con escenarios multidominio que exijan la colaboración de otros instrumentos de poder con objeto de experimentar nuevos procesos y estructuras.

– *Liderazgo*. Las MDO requieren un cambio de mentalidad en la FAS y el C2MDO requiere un liderazgo que fomente la colaboración y la delegación de autoridad. Esto implica potenciar modelos como el MoM o el liderazgo transformacional[43], de forma que permitan la mayor iniciativa e innovación en entornos dinámicos y complejos como las MDO.

  Las operaciones multidominio «necesitan líderes dispuestos a asumir riesgos y experimentar con enfoques innovadores» que impulsen la mejora continua y la adaptación. La disposición a asumir riesgos y explorar enfoques innovadores garantizará la ventaja operativa en un entorno en constante evolución (EMAD, 2024: 16).

– *Conectividad*. En el contexto de las MDO y dentro de los procesos del C2, este elemento clave se refiere a la capacidad de interconectar, en tiempo real y de forma segura, todas las plataformas, sensores, sistemas de armas, unidades y mandos dentro del entorno operativo en una operación.

[43] «El líder transformacional es aquel capaz de concienciar a los subordinados de la importancia del trabajo a realizar, de hacerles trascender su propio interés en beneficio del grupo y de modificar la jerarquía de necesidades del seguidor» (Molero y Moriano, 2020: 23).

La conectividad es clave para garantizar un enlace permanente que permita simultanear acciones en todos los dominios y así, obtener la superioridad en la JOA. Obtener los datos necesarios, hacerlos llegar al lugar adecuado y analizarlos de forma precisa es esencial para mejorar la velocidad del ciclo OODA[44] y agilizar la toma de decisiones.

- *Gestión del dato y la información*. La capacidad de procesar, proteger y explotar los datos y la información de manera eficiente es otro de los elementos clave en los que se basan las MDO. Esta variable se enmarca en los procesos del C2MDO y se encuentra íntimamente ligada a la conectividad.

  En España, el SC2N y el proyecto de nube de combate pretenden proporcionar la capacidad para capturar, procesar y distribuir los datos, a la vez que prestan los servicios necesarios para facilitar y agilizar la toma de decisiones.

- *Incorporación de tecnologías emergentes y disruptivas*. La adaptación de las MDO en las FAS va a estar directamente relacionada con la capacidad de integrar determinadas EDT, especialmente la IA y las tecnologías de la comunicación como el 5G. «La incorporación de la IA al sistema de C2 permitirá determinar y asesorar las acciones más aconsejables en cada momento, llegando a automatizar determinadas decisiones para agilizar los procesos (EMAD, 2023: 18).

  Dentro de los procesos del C2MDO, esta variable de estudio está estrechamente ligada a la gestión del dato y la conectividad. Por un lado, las MDO van a producir una avalancha de datos debido a la sensorización del campo de batalla. Estos datos necesitan ser almacenados, analizados y trasladados a la persona adecuada siendo el tiempo un factor crítico.

- *Agilidad*. Enmarcada dentro de la estructura del C2MDO, esta variable es la capacidad de adaptación a los cambios que se producen en el entorno operativo. En el contexto de las MDO, la agilidad implica modificar la estructura de mando, los procesos para descentralizar la toma de decisiones y la integración de todas las capacidades disponibles para asegurar que la FC puede llevar a cabo operaciones en entornos de gran incertidumbre y complejidad.

[44] Observar, orientar, decidir y actuar.

El éxito de las MDO no solo descansa en la velocidad de la toma de decisiones, sino también en la habilidad de modificar la estructura de C2 cuando las circunstancias así lo aconsejen. Se requiere un enfoque en el que los comandantes puedan establecer el sistema de C2 más adecuado en cada situación.

- *Enfoque integral*. Las MDO van a requerir una coordinación efectiva de las FAS con múltiples y diversos actores. Los otros instrumentos de poder del Estado, empresas públicas y privadas, elementos del sector de la seguridad o del ámbito tecnológico son solo algunos de los actores no militares esenciales para poder actuar en todos los dominios de una manera integrada y coordinada.

  El propósito fundamental es alcanzar la mayor sinergia en el planeamiento y ejecución de las operaciones para alcanzar los objetivos operacionales que sin la integración de estos elementos no podrá ser posible (EMAD, 2021).

- *Interoperabilidad*. Se define como «la voluntad y la capacidad para superar las diferencias culturales, organizativas, de procedimiento y tecnológicas, con el fin de operar con eficacia hacia un objetivo común». Esta variable de estudio y elemento clave de las MDO se basa, desde el punto de vista militar, en la unidad de doctrina y en la compatibilidad de sistemas (Ministerio de Defensa, 2024d: anexo B-14).

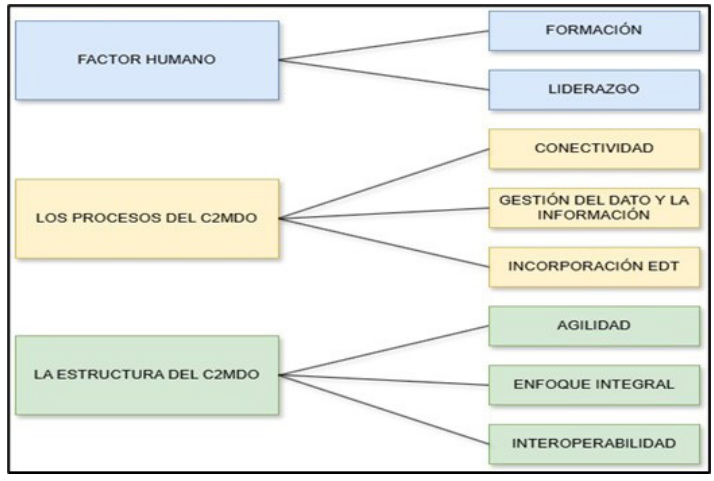


Figura 1. Los factores y las variables de estudio. Fuente: elaboración propia

Estas variables se confrontan con los conocimientos, valoraciones y reflexiones de una serie de expertos con amplia experiencia en la implantación y desarrollo conceptual de las MDO en las FAS españolas. De esta forma, los resultados obtenidos del análisis permiten valorar el grado de necesidad y suficiencia de las medidas que están siendo implementadas para adaptar el C2MDO en las FAS. En concreto se realizan siete (7) entrevistas:

- Entrevista al general de división Fernando Luis Morón Ruiz, autor del primer capítulo del documento «Transformación digital de las FAS para el combate multidominio», publicado en el año 2023. El general Morón se centra, principalmente, en la importancia del factor humano para efectuar una adecuada adaptación del C2MDO en las FAS.
- Entrevista al general de brigada Carlos Javier Frías Sánchez. El general Frías ha formado parte de un Grupo de Trabajo (GT) para el desarrollo del concepto del multidominio y cuenta con numerosas publicaciones de temas relacionados con las MDO[45].
- Entrevista al teniente coronel Raúl López Resusta, oficial responsable de elaborar el «CE. Mando y Control de las Operaciones Multidominio», que fue publicado en julio del año 2024.
- Entrevista al teniente coronel Francisco Elías Entrialgo, responsable de las Operaciones Multidominio en J5[46] del mando de operaciones (MOPS).
- Entrevista al comandante Fabián Granados Armuña, destinado en la Sección de Planificación Tecnológica de la División de Planes (DIVPLA) del Estado Mayor Conjunto de la Defensa (EMACON) del EMAD.
- Entrevista al comandante del Ejército del Aire y del Espacio Juan Ramón González Espadas, piloto de combate en su etapa de servicio activo y actualmente asesor en el programa Future Combat Air System (FCAS) de la empresa Airbus. El comandante González Espadas es el autor del quinto capítulo del documento «Transformación digital de las FAS para el combate multidominio», en el que trata la TD necesaria para adaptar el C2 al entorno multidominio.

[45] *Inteligencia Artificial en el campo militar* (Frías Sánchez, 2024) o *¿Un campo de batalla «transparente»?* (Frías Sánchez, 2023) son algunas de las publicaciones relacionadas con el campo de las MDO del general Frías.

[46] J5 es la sección encargada del planeamiento de un Cuartel General del nivel operacional.

– Entrevista al teniente coronel del ET Rubén Vega Bustelo, autor del cuarto capítulo del documento «Transformación digital de las FAS para el combate multidominio» y se centra en el desarrollo tecnológico y la seguridad necesaria para el multidominio.

Las entrevistas[47] realizadas están basadas en una serie de preguntas que buscan analizar las variables seleccionadas, teniendo en consideración los conocimientos, experiencia y visión de los expertos. La información obtenida se confronta en unas tablas de doble entrada[48] que permiten valorar el grado de necesidad y suficiencia.

2 Las MDO en las FAS españolas

La publicación doctrinal *PDC-01(B) Doctrina para el empleo de las FAS* define la función conjunta mando y control como «las actividades relacionadas con el ejercicio de la autoridad y la dirección de las fuerzas asignadas para el cumplimiento de la misión» (Ministerio de Defensa, 2024d: 74).

El liderazgo, el ciclo de la decisión, la delegación de autoridad, la doctrina, el asesoramiento especializado, los sistemas de información y comunicaciones o el enfoque integral, además de otros elementos, son los principales pilares en los que se basa esta función conjunta (ver figura 2).



Figura 2. Fundamentos del Mando y Control. Fuente: Ministerio de Defensa (2024d: 103)

47 Se puede acceder a las entrevistas completas contactando con el autor de esta investigación a través del siguiente correo electrónico fcasyag@hotmail.es, o a través del siguiente enlace:
https://drive.google.com/file/d/1BKPi_Pm9kwdJ4TuorE2Zjt2OkAf968AU/view?usp=sharing

48 Las tablas de doble entrada se pueden consultar en el siguiente enlace: https://drive.google.com/file/d/10eLY6mDBf8T50g3DvGtP0TmmV8MLTJKG/view?usp=sharing

Las MDO han surgido para hacer frente a un entorno operativo con amenazas muy complejas y dinámicas. Para poder aplicar esta visión multidominio es necesario mejorar la habilidad de las FAS para poder producir efectos en y desde todos los dominios y la función conjunta C2 desempeña un papel fundamental. La gestión de la información, la toma de decisiones y las actuales estructuras de C2 requieren un cambio de mentalidad y una evolución del actual enfoque para los desafíos que presentan las MDO.

En el marco de las FAS españolas, el concepto MDO se implantó en la doctrina nacional en el año 2020, con la publicación de la «Nota Conceptual del JEMAD». Esta publicación propuso utilizar, por primera vez en la doctrina nacional, el término multidominio en el entorno conjunto de las FAS, con objeto de reflejar esta nueva forma de operar y alinearla con la terminología y conceptos utilizados por los aliados y miembros de la OTAN.

Desde ese momento, se han ido efectuando diversas publicaciones que han profundizado en el entorno y las operaciones multidominio, definiendo y acotando el concepto MDO. Las más importantes y que se centran de una forma directa en estas operaciones son las que a continuación se relacionan:

- «Concepto Exploratorio. Evolución de la Fuerza Conjunta hacia las operaciones multidominio». Publicado en marzo del año 2023, este documento identifica aquellos aspectos que deben cambiar a corto, medio y largo plazo para poder implementar este enfoque en el marco de las FAS. El CE identifica los elementos clave de las MDO como el C2, la gestión de la información, la incorporación de EDT, la conectividad o la interoperabilidad.
- «Transformación digital de las FAS para el combate multidominio». Este documento, publicado en el año 2023, expone como la TD de las FAS es la base que debe sustentar los elementos clave para las MDO. Se analiza la importancia de efectuar un cambio de mentalidad, un C2 más colaborativo que permita la participación de actores no militares, la coordinación de acciones entre dominios y la ampliación del espacio de las Fuerzas Armadas en la zona gris. Para ello, es necesario el cambio de cultura organizativa que debe implicar a todo el personal y a todas las estructuras, siendo clave adoptar el mando orientado a la misión (MoM[49]).

[49] «El MoM es una filosofía que promueve la concesión a los subordinados del máximo grado de iniciativa posible dentro del propósito del jefe, para acortar el ciclo de toma

- Esta publicación también evalúa cómo la incorporación de nuevas tecnologías permite acelerar el ciclo de la decisión y facilitar efectos multidominio. La nube de combate[50] se presenta como una solución técnica para potenciar la interoperabilidad entre los elementos de la fuerza de todos los dominios.
- *Concepto Exploratorio. Mando y Control de las Operaciones Multidominio*. Firmada en julio de 2024, esta publicación se configura como la guía y orientación para el desarrollo del C2MDO en la FC de las FAS. El documento centraliza la información esencial reflejada en las dos publicaciones anteriores y las amplía en el campo del mando y control multidominio.
- *PDC-01 (B) Doctrina para el empleo de las FAS.* Es la publicación doctrinal militar de más alto nivel. Describe la forma de empleo de las FAS y establece las normas fundamentales bajo las que estas actúan. Además, armoniza los contenidos con otras publicaciones nacionales de carácter conjunto en vigor, contempla nuevos conceptos surgidos en los últimos años y se alinea con la doctrina aliada. En concreto, incluye el concepto de MDO y dedica un espacio concreto al C2MDO.

Por otro lado, existen publicaciones recientes que tienen una gran relevancia para el desarrollo e implantación de las MDO. En concreto, las publicaciones *Visión del JEMAD de la Nube de Combate* o la *Visión de la Inteligencia Artificial en las FAS*, del año 2022 y 2024, respectivamente, desarrollan y sientan las bases de dos herramientas esenciales para poder efectuar una adecuada adaptación a las MDO.

2.1 Plan de implantación de las MDO en las FAS

Como ya se ha expuesto, durante la investigación de este trabajo y en concreto, en febrero del año 2025, el JEMAD firmó el «Plan de implantación de las MDO en las FAS». Esto supone un hito en el proceso de adaptación de estas operaciones en España al efectuar una aproximación efectiva y estructurar una implantación de medidas, de forma gradual, que permitan alcanzar el objetivo de capacitar a la FC para planear, conducir y ejecutar las MDO.

---

de decisiones y facilitar la adaptación operativa en beneficio de la misión» (Ministerio de Defensa, 2024d: 101).

[50] La nube de combate se configura como «una solución tecnológica avanzada a las capacidades militares que permite su empleo, especialmente el mando y control, en el multidominio (EMAD, 2022).

La visión del JEMAD para las MDO se alcanza en tres (3) fases diferenciadas, con un horizonte temporal hasta el año 2040. En concreto, la primera fase se establece para el año 2025-2026, la segunda fase para el periodo 2027-2032 y la tercera fase del año 2033 al año 2040 (ver figura 3).

El documento incide en la importancia de alcanzar la superioridad en la gestión de la información y el conocimiento, ya que esto permite materializar la agilidad necesaria en la toma de decisiones y, en consecuencia, obtener la superioridad operativa frente a los adversarios.



Figura 3. Diseño general del Plan de implantación de las MDO. Fuente: (EMAD, 2025, Anexo I)

Para ello, el Plan establece cuatro (4) objetivos generales, asignando a cada uno de ellos una línea de esfuerzo (LoE). En concreto:

- LoE A: «Formación»: asegurar la adecuada formación del personal de las FAS en las MDO.
- LoE B: «Ejercicios, Experimentación y Wargaming»: potenciar el planeamiento y la conducción de ejercicios, y el adiestramiento en el marco de las MDO.

– LoE C: «Doctrina y Conceptos»: impulsar el desarrollo de doctrina y conceptos para la adaptación a las MDO.
– LoE D: «Digitalización»: alcanzar la transformación digital y tecnológica de las FAS que permita planear, conducir y ejecutar las MDO.

3 Implementación de medidas en el factor humano

En las FAS, el capital humano está considerado el recurso más valioso y se establece como la base principal para mantener las capacidades operativas. De hecho, la preparación y la gestión del talento del personal están definidas como los elementos que van a marcar la diferencia a la hora de alcanzar una ventaja cualitativa con potenciales adversarios (JEMAD, 2022a: 98).

El enfoque que necesitan las MDO exige un profundo cambio de mentalidad y de cultura organizacional dentro de las FAS. Según establece la publicación de «Transformación digital de las FAS para el combate multidominio», el cambio de cultura está vinculado al tipo de liderazgo, a las dinámicas entre las personas y a una organización más horizontal y ágil que facilite la toma de decisiones (Morón Ruiz *et al.*, 2023).

El ritmo impuesto por las MDO y las posibilidades que van a permitir las EDT incrementan la importancia de la preparación y el liderazgo del personal como elemento diferenciador. Publicaciones como el «CE. Mando y Control de las MDO» reflejan la estrecha relación existente entre las variables de formación y liderazgo, siendo los centros docentes militares el primer paso para impulsar el cambio de mentalidad y cultura organizacional que requieren las MDO (EMAD, 2024).

3.1 Formación

La LoE A del Plan de implantación del JEMAD está dedicada en exclusiva a la formación y debe asegurar que el personal de las FAS interiorice y adquiera los conocimientos necesarios del enfoque multidominio. Para ello, se ha generado un Grupo de Trabajo (GT) «Formación» y se han establecido una serie de líneas de actuación (LA) entre las que destacan la determinación de las competencias necesarias, así como la implantación y verificación de actividades formativas para adaptar las MDO a las FAS (EMAD, 2025).

Para el comandante Granados Armuña, la formación debe actuar de palanca principal que impulse el resto de acciones identificadas con objeto de alcanzar la adaptación al C2MDO. Además, en su entrevista explica que los Ejércitos y la Armada ya están desarrollando seminarios de conceptos emergentes, existiendo contenidos de las MDO aprobados para impartir en los cursos para la adquisición de las Especialidades de Segundo Tramo (E2T) de operaciones, inteligencia o logística, así como en determinadas acciones formativas.

De igual modo, la Escuela Superior de las FAS (ESFAS) del CESEDEN, especialmente su Departamento de Operaciones (DOPE) está incorporando los conceptos MDO en su formación. En el momento en el que estos son aprobados por la doctrina nacional y aliada, se están impartiendo conocimientos multidominio en las distintas acciones formativas de los diferentes cursos de Altos Estudios de la Defensa Nacional, por ejemplo, en el Curso de Estado Mayor de las FAS (CEMFAS) XXVI[51] (2024-2025).

Sin embargo, según el criterio de otros expertos consultados, como el GD Morón, se considera que la enseñanza no se unificará hasta que el «Plan de implantación del JEMAD» se aplique de una forma efectiva. Aunque, actualmente, existan iniciativas particulares a pequeña escala por parte de los diferentes Ejércitos y la Armada, la coherencia para centralizar una formación adecuada en las MDO debe emanar de la Dirección General de Reclutamiento y Enseñanza Militar (DIGEREM) y, por lo tanto, el Ministerio de Defensa (MINISDEF).

Es decir, aunque existan actividades puntuales en los Ejércitos y la Armada como por ejemplo la que lleva a cabo el Departamento de Liderazgo de la EGLET con el MoM o mediante acciones formativas/informativas no regladas, esto es insuficiente para implantar de forma eficaz el concepto MDO en las FAS. Se requiere una formación específica de base común para todas las FAS que permita una visión unificada y facilite la integración del personal en la ejecución de este tipo de operaciones.

Por otro lado, el GB Frías considera que antes de iniciar la formación del personal de las FAS en MDO es necesario establecer claramente la doctrina y los procedimientos a trasladar. Es decir, lo primero hay que saber qué se quiere hacer y de qué forma,

[51] El CEMFAS XXVI, en su asignatura 12 «Fundamentos de las Operaciones Conjuntas» dirigida por el DOPE, trata en profundidad las Operaciones Multidominio.

y solo después se podrá actuar sobre el personal. El esfuerzo doctrinal efectuado hasta el momento para implantar el concepto MDO, definir los dominios o establecer los elementos clave de las MDO es evidente, como ya se ha expuesto. Sin embargo, más allá de dichas publicaciones y los puntos descritos no hay nada más establecido o normalizado.

A modo de ejemplo y utilizando un dominio no físico como el ciberespacial, se pueden observar los múltiples interrogantes que surgen a la hora de poder actuar desde dicho dominio. ¿A qué nivel se va a combatir en ciber? Si es en el nivel operacional: ¿quién tiene la autoridad para ejecutar una operación ciberofensiva?, ¿qué Tácticas Técnicas y Procedimientos (TTP) están autorizadas a utilizarse en una MDO?, ¿cómo se evalúa el posible daño colateral en una operación ciber?, ¿qué nivel de daño sería admisible?, ¿se podrían llevar a cabo ataques con efectos físicos o solo de *software*?

Este tipo de cuestiones de procedimiento pueden trasladarse a cualquier otro dominio dejando patente que es necesario definir claramente cómo se va a materializar una MDO y de qué forma se puede contribuir generando efectos desde y en cada uno de los dominios. De los expertos consultados existe unanimidad en torno a esta necesidad. En concreto, el teniente coronel López Resusta expone en su entrevista que el concepto MDO y el enfoque multidominio no se está divulgando actualmente de forma adecuada en las FAS.

Además, el teniente coronel Elías Entrialgo considera que el primer paso debe ser establecer una normativa nacional en la que se profundicen en los conceptos inherentes a la ejecución de las MDO y se establezcan las líneas de acción para llevarlas a cabo. Posteriormente y de una forma transversal, se debería proceder con la formación del personal.

Otro punto que destacar dentro de la variable formación es la necesidad de impulsar el adiestramiento en las MDO a través de ejercicios, experimentación y *wargaming*. Para ello, el «Plan de implantación» cuenta con la LoE B que permitirá reforzar la formación en el ámbito individual y colectivo, especialmente en el planeamiento y conducción de MDO.

El teniente coronel López Resusta destaca que los ejercicios y la experimentación van a resultar esenciales para avanzar en la necesaria adaptación al enfoque multidominio. En la misma línea, el GD Morón considera que esto fomentará una actitud de innovación al aplicar el proceso

«probar, fallar con la práctica y aprender rápido en un intento continuo de mejora. Asumiendo que se cometan errores no intencionados durante los procesos de aprendizaje y en el desarrollo de actividades, se fomentará la iniciativa frente a la inacción».

Por otro lado, en el «CE. Evolución de la Fuerza Conjunta hacia las MDO» se establece que la formación debe orientarse a promover un cambio de mentalidad (ver figura 4) y cultura organizacional que permita premiar las «soft skills»[52], el conocimiento técnico, la innovación o la creatividad. También, esta publicación marca que deben fomentarse las actitudes críticas constructivas con el propio sistema con objeto de poder adaptar la FC al entorno multidominio (EMAD, 2023).

Sin embargo, aquí surge la duda sobre qué medidas prácticas deben implementarse en la enseñanza militar para llevar a cabo el necesario cambio de mentalidad que permita la adaptación a la complejidad inherente de las MDO.



Figura 4. Elementos para el cambio de mentalidad. Fuente: (EMAD, 2023: 12)

[52] «Combinación de habilidades sociales y de comunicación, rasgos de la personalidad, actitudes, atributos profesionales, inteligencia social e inteligencia emocional que facultan a las personas para moverse por su entorno, trabajar bien con otros, realizar un buen desempeño y, complementándose con las habilidades duras, conseguir sus objetivos» (EMAD, 2023: 12).

El reciente premio de investigación «Hernán Pérez del Pulgar 2024», «¿Es posible mejorar la respuesta de los ejércitos frente a la complejidad?», sugiere que la formación debe ir dirigida a potenciar una «doctrina viva que fomente la adaptación a nuevas situaciones, la adopción de tácticas innovadoras y sobre todo la asunción de riesgos» (Andrés Ibarzo, 2024: 23).

Esta publicación establece que la asunción de riesgos marca la diferencia entre un ejército que lucha por una amenaza vital y el que lo hace por unos objetivos menos importantes. Un ejército con una gran carga burocrática limita los riesgos y, por lo tanto, coarta la iniciativa y la adaptación. La formación MDO exige creatividad porque el enemigo, la siempre presente «niebla[53] de guerra» y el combate en un ambiente degradado inherente a un conflicto de alta intensidad no permitirán aplicar los procedimientos tal y como se trabajan en tiempo de paz.

Por lo tanto, la enseñanza multidominio debe dirigirse a formar personal para encontrar soluciones a problemas complejos, asumiendo riesgos donde sea necesario. El adiestramiento debe fomentar el uso de la iniciativa, el ingenio y la improvisación. Esto no se podrá conseguir sin un cambio estructural en el que la cadena de mando de las FAS incremente la tolerancia al error y lo convierta en una oportunidad para mejorar.

Por lo expuesto en este punto y tras analizar las publicaciones MDO, se extrae que la variable formación es esencial para alcanzar el necesario cambio de mentalidad. Este cambio cultural debe proporcionar a las FAS mandos intuitivos, sin temor al fallo y predispuestos a promover cambios de gran calado en aspectos de personal, impulsando nuevos procedimientos de adiestramiento y proponiendo cambios relevantes en la organización. Es decir, la formación debe ir dirigida a implantar el MoM y el liderazgo transformacional, que se van a exponer en el siguiente punto y que permiten ligar la primera variable de estudio con la segunda: «liderazgo».

3.2 Liderazgo

Publicaciones como el «CE. Mando y Control en las MDO» o «Transformación digital de las FAS para el combate multidominio» dejan patente que el modelo de liderazgo en el que se dele-

[53] El concepto de niebla de guerra hace referencia a la incertidumbre, confusión generalizada, falta de información, o dificultades no previstas que surgen a lo largo de un conflicto bélico. Este término fue acuñado por primera vez por Carl von Clausewitz.

gan las decisiones, como el MoM, es el que mejor se adapta a la complejidad y dinamismo de las MDO. Además, se remarca que será deseable un estilo de liderazgo «transformacional», que permita vencer la resistencia natural al cambio donde los líderes estén dispuestos a asumir riesgos y experimentar con enfoques innovadores (Ministerio de Defensa, 2024d).

Según el GD Morón, en todos los niveles de la jerarquía será deseable un estilo de liderazgo transformacional, orientado al cambio, porque es el que produce el mayor impacto en la cultura de la organización. Por otro lado, el general coincide con la importancia de aplicar el MoM en las MDO, dado que es el modelo de liderazgo que logra el mayor nivel de compromiso de todos los miembros en este entorno operativo.

Esto permite extraer que las MDO requieren líderes capaces de adaptarse al cambio, con espíritu crítico, que evalúen constantemente la situación y propongan mejoras sin miedo al error y con capacidad para experimentar nuevas opciones. Es decir, el enfoque multidominio necesita personal con la capacidad de «think out of the box» para estar en disposición de sorprender al adversario.

Sin embargo, analizando las entrevistas a los expertos y determinadas publicaciones, como el mencionado premio de investigación «Hernán Pérez del Pulgar 2024», se han identificado múltiples barreras y obstáculos que impiden que esta filosofía pueda calar en las FAS actualmente y que se van a exponer a continuación.

En primer lugar y según el GB Frías, existe una clara tendencia a la microgestión en las FAS. Este «micromanagement» se produce cuando los niveles superiores están «desocupados» y la tecnología lo permite. También, se menciona en la entrevista que, cuando el mando está saturado de trabajo, la microgestión desaparece, ya que existe la necesidad de delegar. Aunque sea a un bajo nivel, la microgestión es casi inevitable, pero tiene el gran inconveniente de crear una cultura de centralización y de «esperar órdenes».

Además, la característica y arraigada cultura organizacional de las FAS puede ser inicialmente un inconveniente para adaptar la mentalidad multidominio en la variable del liderazgo. La primacía de la disciplina sobre la iniciativa, la continuidad de la cadena orgánica o la dificultad de mantener un pensamiento crítico y creativo cuando es diferente de la opinión general establecida

son claros ejemplos de obstáculos en la organización (Andrés Ibarzo, 2024).

Enlazado con el último párrafo, el GB Frías considera que, tras trescientos años de mando detallado[54] («detailed Command»), se ha creado un sistema que premia la disciplina y penaliza la iniciativa, que es la base del MoM. Esto se basa en la desconfianza hacia el subordinado y que tiene su reflejo, en muchas ocasiones, en la posterior desconfianza hacia el jefe. El general enfatiza en la entrevista que este punto costará mucho cambiarlo.

Las MDO requieren un liderazgo transformacional, ya que implica delegar en un entorno cambiante. Este enfoque tiene numerosas connotaciones como, por ejemplo, permitir que los subordinados puedan sorprender a sus mandos y, por lo tanto, asumir sus errores, ya que la responsabilidad no se delega. Además, es necesario reconocer sus éxitos y concienciar a todo el personal de que todo error es una oportunidad de aprender (Molero y Moriano, 2020).

Sin embargo, actualmente en las FAS existe una clara orientación al logro en los actuales planes de personal, además de una escasa tolerancia al error. Esto potencia el liderazgo transaccional[55] en lugar del transformacional. El GB Frías considera que este tipo de liderazgo es muy negativo para las FAS, ya que fomenta el egoísmo, incluso a costa de la falta de coordinación. Además, se priorizan los fines del individuo a los de la organización, se dificulta la compartición de información y destruye el compañerismo. Al final, esto genera frustración en el personal de las FAS, ya que la estructura es piramidal y es imposible que todos pueden alcanzar los puestos de mayor responsabilidad.

El liderazgo transaccional y la actual orientación al logro se puede considerar una herramienta empresarial pensada para motivar al personal por la vía de la competencia, alcanzando recompensas. El enfoque que requieren las MDO es un liderazgo orien-

[54] En el «detailed Command» el mando proporciona toda la información a los niveles inferiores con objeto de marcar claramente lo que deben hacer. Es decir, se intercambia velocidad por información completa. Sin embargo, este estilo de mando limita la iniciativa, la creatividad, disminuye el compromiso de los subordinados al no comprender de forma completa el propósito del mando y, por lo tanto, exige un mayor control de la cadena de mando (Meier, 2022).

[55] El liderazgo transaccional se basa en un intercambio de recompensas entre el líder y los subordinados. Promueve el logro de metas a través de la supervisión, castigando el bajo rendimiento. Este tipo de liderazgo no se centra en mejorar la organización en su conjunto.

tado al cambio que premie el talento, la iniciativa, el compromiso y el beneficio de la organización, es decir, aplicar un liderazgo transformacional.

Por otro lado, el teniente coronel Elías Entrialgo considera que las FAS no se encuentran en una situación de suficiente madurez para efectuar un cambio al modelo de liderazgo transformacional. Para razonarlo explica que los actuales planes de personal son distintos para cada ejército y no existe una política que aborde los desafíos del futuro de una forma conjunta. Además, las MDO requieren una estructura capaz de evaluar la información y tomar decisiones que van a afectar a muchos dominios al mismo tiempo y el personal militar, por regla general, suele adolecer de esta visión de conjunto.

Todos estos obstáculos dificultan en gran medida asimilar la visión que aporta el MoM y el liderazgo transformacional. Por lo tanto, desde este punto de vista, la cultura actual de las FAS se puede considerar opuesta o, por lo menos, muy alejada de lo que las MDO necesitan.

Las FAS han efectuado un esfuerzo doctrinal para adaptar el cambio en la cultura organizativa a través del MoM, ya que este concepto se refleja como una necesidad en todas las publicaciones oficiales. Sin embargo, este cambio no se va a producir si no se interioriza por completo en el factor humano y actualmente no existen garantías de que esto se pueda materializar.

Para poder adaptar la mentalidad MDO, el GD Morón explica la necesidad de fomentar el control sobre los resultados y no sobre las tareas. Es fundamental no percibir de forma excesiva el control de los escalones superiores ya que, debido al efecto cascada, el líder que recibe control va a transmitir control y aquel que recibe libertad de acción otorgará libertad de acción a sus subordinados. Además, el general Morón considera que la autoridad debe delegarse hasta el escalón más bajo que tenga capacidad para tomar decisiones con la suficiente información. La organización será tanto más eficaz cuanta más responsabilidad se otorgue a su personal y se aproveche la delegación y el MoM.

Para el comandante Granados Armuña es esencial que exista un cambio de mentalidad que incremente la confianza en los niveles inferiores para que la necesaria descentralización de las MDO sea una realidad funcional. Sin esta transformación cultural, los avances tecnológicos podrían ser insuficientes o incluso contraproducentes, al reforzar patrones tradicionales de centralización.

En contrapartida, el mando al que le han delegado la autoridad deberá ejercerla con responsabilidad, teniendo siempre presente el propósito del mando y valorando el efecto de sus acciones en los diferentes dominios, de tal forma que los pueda gestionar. Con las posibilidades que ofrecen las nuevas tecnologías para ver en tiempo real lo que sucede en el campo de batalla, va a ser un reto el conseguir que desde el nivel superior no se den órdenes de acompañamiento que condicionen la actuación de las pequeñas unidades en el campo de batalla.

La redarquía[56] está considerado el modelo organizativo de la era digital y se basa en la conectividad y la cooperación. Su funcionamiento permite una mayor agilidad en comparación con el de la estructura jerárquica y libera al modelo tradicional de organigramas y burocracia facilitando la iniciativa y la colaboración, considerando el capital humano el elemento central (Ranstad, 2022).

El GD Morón defiende en el capítulo 1 de la publicación «Transformación digital de las FAS para el combate multidominio» la necesidad de evolucionar a un modelo de redarquía por parte de las FAS, ya que considera que «es el modelo que mejor se adapta a la perspectiva, agilidad e iniciativa que requieren las MDO y su modelo de liderazgo» (Morón Ruiz *et al.*, 2023: 58). Aquí considera que este modelo es el que mejor aprovecha el potencial de los datos, facilita el enfoque integral y la iniciativa disciplinada (basada en el propósito del mando), núcleo del MoM. La complejidad de las MDO y su elevado tempo[57] implican que las estructuras de C2 y las relaciones de mando tradicionales no se adaptan de manera eficaz.

Sin embargo, el GB Frías considera que la redarquía es un modelo interesante a nivel empresarial, pero que es difícil que este sea adaptable a las estructuras militares. Para el general Frías, un MoM bien aplicado, una delegación de autoridad bien analizada, una doctrina clara en MDO y el planeamiento concurrente ampliado a los nuevos dominios deberían ser elementos suficientes para operar con éxito en los nuevos dominios.

[56] «La redarquía es un modelo organizativo basado en redes de colaboración, donde múltiples actores interactúan compartiendo talento y conocimiento, de forma abierta en relaciones de igual a igual. A diferencia del modelo jerárquico, la redarquía funciona de abajo arriba, habilitando que las decisiones y soluciones emerjan de manera creativa como resultado de la cooperación colectiva» (Cabrera, 2017).

[57] Tempo es la relación existente entre la velocidad del ciclo de decisión propio y la del adversario.

En la misma línea que el GB Frías, el teniente coronel Elías Entrialgo considera muy difícil llevar a cabo una evolución organizativa, a corto, medio o largo plazo, a un modelo tipo redarquía. La resistencia al cambio inherente a las personas, unida a la mentalidad jerárquica de las FAS, va a impedir o, al menos, dificultar en gran medida la evolución a un sistema de este tipo.

Del análisis de los expertos se extrae que el verdadero problema no radica, inicialmente, en encontrar un nuevo sistema organizativo que se adapte a las MDO, sino en aplicar un verdadero y eficaz MoM y liderazgo transformacional, que ahora se ve totalmente dificultado por las razones expuestas en el presente capítulo. Por otro lado, la estructura de las FAS es jerárquica desde sus inicios y esto ha marcado la cultura de la organización. Las MDO requieren un liderazgo que incremente la agilidad en la toma de decisiones. El MoM es una herramienta que permite reducir la rigidez actual y aplanar la estructura, pero manteniendo el carácter jerárquico.

4 Implementación de medidas en los procesos de mando y control

Las FAS están afrontando el reto tecnológico de adaptar las necesidades de conectividad que requieren las MDO para poder gobernar y gestionar la avalancha de datos e información que producen. En un campo de batalla sensorizado, gobernar el dato implica disponer de sistemas que permitan almacenar, analizar y determinar qué información necesita la autoridad con la responsabilidad de decidir o actuar.

Para ello, es necesario valorar los retos y dificultades que surgen en el campo de la seguridad del dato, en la implementación de tecnologías emergentes o la forma de presentar la información disponible a aquellos que deberán decidir o actuar. Todos estos puntos buscan establecer que los procesos de C2 sean lo más ágiles posible y así poder obtener la superioridad en el ciclo de la decisión frente a adversarios con unas mismas capacidades tecnológicas.

4.1 Conectividad

Los entornos multidominio requieren una gran velocidad en el análisis de la información para poder obtener la superioridad en

el ciclo de la decisión. Por este motivo, la conectividad se configura como un elemento esencial para habilitar las MDO. A través de la interconexión de los distintos sensores disponibles en todos los dominios, se habilitará un intercambio de datos en tiempo real que propiciará un C2 más ágil.

La conectividad también facilitará el concepto del «edge computing», es decir, acercar la potencia de procesamiento al lugar del campo de batalla donde se generan los datos, denominados «centros de procesamiento». Esta computación, integrada en las redes militares, permitirá la toma de decisiones descentralizada y una mejora en el conocimiento de la situación, habilitando los requerimientos de C2 que necesitan las MDO (EMAD, 2023).

El ingeniero de Sistemas de Indra Manuel Buesa Bueno expone que la base para efectuar la integración de los diferentes dominios es la conectividad: «todos los elementos que forman parte de la batalla deben tener la posibilidad de conectarse con el resto, tanto si son sensores, efectores, sistemas de procesamiento de datos o unidades de C2» (Morón Ruiz *et al.*, 2023: 88).

Sin embargo, la principal dificultad radica en disponer de los datos adecuados, en el momento y lugar adecuados, de forma que estos puedan ser analizados con herramientas potentes, como la IA, para alcanzar la superioridad en el análisis de la información y acelerar el proceso de la toma de decisiones.

En las FAS españolas, la conectividad necesaria que habilite las MDO se pretende alcanzar a través de la integración de todas las capacidades de la FC en un único Sistema de Mando y Control Nacional (SC2N) y con la denominada nube de combate. Para ello, en julio del año 2023 se alcanzó la capacidad operacional inicial (IOC) de la Infraestructura Integral de Información para la Defensa (I3D[58]), que es el «sistema nervioso» que proporciona la necesaria conectividad y seguridad y en el que se encuentra integrado el SC2N.

El comandante Granados en su entrevista hace énfasis en la importancia de materializar a corto plazo un sistema de mando y control único como es el SC2N. Destaca que este tiene el potencial

[58] «La I3D se define como la infraestructura tecnológica, bajo una autoridad operativa única, que mediante la convergencia de los sistemas de información y telecomunicaciones y los servicios que éstos proporcionan, optimice el uso de éstos y facilite a los organismos y usuarios el acceso eficaz a la información de la Defensa de forma segura» (Ministerio de Defensa, 2018: 28).

necesario para mejorar exponencialmente la capacidad C2MDO, ya que su diseño permitirá integrar los diferentes dominios operativos en una estructura unificada que facilitará el planeamiento y la conducción de estas operaciones.

Actualmente, el SC2N dispone de un núcleo inicial, acreditado para manejar información clasificada hasta «Reservado Nacional», que proporciona una capacidad limitada de planeamiento y conducción de operaciones. Este núcleo debe evolucionar para alcanzar su capacidad operativa plena (FOC), en un único sistema, con un único proveedor de servicios y sobre una misma infraestructura (EMAD, 2023: 4).

Por lo tanto, el SC2N se encuentra en una fase de desarrollo intermedia, con avances tangibles en infraestructura y capacidades básicas, pero con retos significativos en términos de seguridad, interoperabilidad y estandarización, que deben resolverse para lograr su plena operatividad.

El hecho de que las FAS dispongan de un sistema único de C2 adaptable a cualquier entorno operativo debería impulsar las sinergias entre los diferentes dominios. Actualmente, las diferencias entre los diferentes sistemas de C2 de los Ejércitos y la Armada suponen una barrera para las operaciones MDO, según el criterio del comandante Granados.

Del mismo modo, el teniente coronel Elías Entrialgo valora en su entrevista que el sistema SC2N todavía no está rindiendo al máximo de su capacidad. Sin embargo, expone que el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC[59]) ha transmitido que cuando el sistema esté a pleno rendimiento, será un sistema potente y que cubrirá todas las necesidades que requiere el C2MDO. Por otro lado, deja claro que hoy existen muchas limitaciones que deberán solventarse porque su rendimiento actual no permite lo que las MDO van a demandar.

Con respecto a la nube de combate, el comandante Granados Armuña considera que es un «sistema de sistemas» que actuará como facilitador de las MDO y generará un efecto multiplicador

[59] «El CESTIC es el órgano directivo al que le corresponde la planificación, desarrollo, programación y gestión de las políticas relativas a los sistemas y tecnologías de la información y las comunicaciones (CIS/TIC), la transformación digital, la gestión de datos, información y conocimiento y la seguridad de la información» (Ministerio de Defensa, 2025a).

de las capacidades militares en todos los niveles de conducción de las operaciones. En el nivel operacional, la nube de combate debe permitir a la Fuerza Conjunta planear y ejecutar operaciones sincronizadas, simultáneas y secuenciales, integrando las capacidades de todos los dominios. La nube de combate no es un fin en sí mismo, debe considerarse un facilitador para el planeamiento, conducción, integración y coordinación de las MDO (EMAD, 2022: 3).

Durante su entrevista, el comandante Granados explica que la nube de combate se materializará, con su epicentro en la I3D, en los centros de procesamiento de datos, mencionados anteriormente, y tendrá extensiones que permitirán el acceso a la información y la explotación de diferentes servicios en el nivel táctico. Además, los datos obtenidos en el nivel táctico se cargarán en la nube y llegarán al nivel operacional a través del SC2N.

Sin embargo, la nube de combate conjunta todavía no existe. Para poder materializarla es necesario, en primer lugar, consolidar esos centros de procesamiento de datos y disponer de un sistema común, el SC2N, que permita la conexión con los sistemas tácticos de los Ejércitos y la Armada. Lo que tampoco es posible, hoy en día, debido a la falta de interoperabilidad que será expuesta más adelante.

Por lo tanto, del análisis efectuado y de la información aportada por los expertos, se extrae que existe un alto grado de inmadurez en la estructura que debe aportar la conectividad necesaria para habilitar las MDO actualmente en las FAS. Para ello, el Plan de implantación del JEMAD, a través de su LoE D «Digitalización», ha establecido una serie de medidas encaminadas a paliar esta situación (EMAD, 2025: 18).

Por otro lado, la conectividad, aunque beneficiosa en términos de acceso a la información y coordinación, conlleva riesgos e inconvenientes que deben ser analizados. En primer lugar, la conectividad habilita un entorno en el que la toma de decisiones puede verse influenciada por los diferentes niveles de las operaciones de forma simultánea. Esto implica una tendencia a la centralización operativa en momentos críticos, especialmente en contextos donde las implicaciones políticas son significativas o donde se perciben riesgos elevados.

Como ejemplo, el teniente coronel Elías Entrialgo expone que, durante la conducción de la evacuación de Sudán en el año 2023, desde el Centro de Operaciones Conjuntas (JOC) del MOPS, se

produjo un cierto solapamiento entre los niveles político, estratégico, operacional y táctico. Al existir riesgo para el personal de las FAS implicado en la operación, el nivel político y estratégico quiso estar presente durante la conducción, resultando en un solape de los escalones C2. Sin embargo, también explica que esta situación fue algo puntual y no tendría por qué convertirse en algo habitual para las MDO.

Por otro lado, es relevante tener en consideración que las capacidades que proporciona la conectividad e incrementado por la potencia de los actuales sistemas de C2, pueden generar una «ilusión de control» en un campo de batalla transparente[60]. Según el GD Morón, las FAS deben estar preparados para que todo falle, para operar en un entorno degradado, con información confusa y poco fiable, con un elevado riesgo de decepción y numerosos ciberataques.

Este punto es especialmente importante ya que el concepto MDO surge para hacer frente a las estrategias A2/AD de grandes potencias como China o Rusia. En un hipotético conflicto de alta intensidad con grandes potencias militares y tecnológicas, resulta lógico plantear que todos o la mayor parte de los dominios puedan estar degradados y la conectividad necesaria para llevar a cabo una MDO, tal y como está definida, puede que no sea viable.

4.2 Gestión del dato y la información

Respecto a la gestión del dato, estar en condiciones de ejecutar una MDO implica obtener, analizar y compartir toda la información posible para alcanzar un completo conocimiento de la situación que permita alcanzar la superioridad en el ciclo de la decisión. Esto va a suponer un crecimiento exponencial de sensores interconectados en todos los dominios. La sensorización de la JOA implicará seleccionar, gestionar, evaluar y compartir una ingente cantidad de datos con aquellas unidades, mandos, plataformas o entidades que lo precisen (EMAD, 2023: 16).

Como opina el comandante Granados, el enfoque debe partir de la gobernanza del dato, estableciendo un marco normativo y técnico que garantice que los datos sean recolectados, almacenados, procesados y distribuidos de manera estructurada y segura.

[60] Un campo de batalla transparente es aquel en el que todo lo que despliega en su interior es susceptible de ser detectado, identificado y, en la mayoría de los casos, atacado en un corto periodo de tiempo (Frías Sánchez, 2023).

La creación de un sistema basado en el concepto de «dato único» es fundamental, asegurando que todas las partes accedan a una única fuente de información fiable y actualizada. Este principio debe ser habilitado por la integración de tecnologías emergentes como la IA, el aprendizaje automático (ML) y la nube de combate, que faciliten la automatización y el procesamiento masivo de los datos.

El teniente coronel Elías Entrialgo destaca que este proceso de gestión y análisis de la información es un problema que se va a agravar a corto plazo. Cada vez se manejan más datos, más factores, más actores y todo ello debe ser analizado en tiempo real para poder tomar las decisiones necesarias durante la operación. Además, el teniente coronel considera que el nivel de C2MDO en las FAS es bajo porque la información que se está manejando actualmente es asequible. En cuanto el volumen de información crezca y se tengan que utilizar volúmenes considerables de datos, las FAS deberán emplear un sistema de C2 evolucionado, donde el empleo de potentes herramientas de análisis como la IA estén totalmente integradas, lo que ahora mismo no es posible.

Por otro lado, el comandante Granados Armuña expone que, actualmente, existen soluciones específicas para ciertas unidades que permiten analizar grandes volúmenes de datos, como es el caso de PALANTIR, empleado por el CIFAS para el análisis de inteligencia. Sin embargo, estas herramientas no están disponibles en la actualidad para ser empleadas en una MDO por la FC.

Para alcanzar o avanzar en la necesaria superioridad en el dato y en la decisión que requieren las MDO, el comandante González Espadas considera que el dato es fútil si no se fusiona, se analiza y se transforma en información acorde a las necesidades específicas de cada usuario. Además, esta se debe distribuir en tiempo y por las vías adecuadas, aseguradas y protegidas para garantizar su integridad. La conclusión que se extrae es que, obviamente, ser mejores en la obtención del dato es positivo, pero el verdadero objetivo es alcanzar la superioridad en el tratamiento de dichos datos, es decir, en la transformación de datos en información para ser utilizada en la toma de decisiones.

El teniente coronel Vega Bustelo expone que un sistema C2MDO, que merezca tal nombre, debe ser capaz de poner a disposición de cada combatiente la información que necesita y con el nivel de detalle preciso. El sistema debe ser capaz de saber dónde está el usuario, cuál es su misión y que información necesita para mos-

trársela de forma automática y adecuada a sus necesidades. Esto implica que todos los datos deben estar etiquetados y contener metadatos.

Por otro lado, la sensorización de la JOA va a generar una gran cantidad de datos que deben ser almacenados, analizados y distribuidos convenientemente. Sin embargo, todo este proceso no tiene valor si la información, ya analizada y adecuadamente filtrada, no se presenta de forma adecuada a la persona que tiene que tomar la decisión o actuar.

Para poder disponer de un completo SA, la información procedente de todos los dominios de la operación se debe visualizar integrada y de forma clara, intuitiva y concisa en una Common Operational Picture (COP). Es decir, la COP es una representación visual que proporciona una visión actualizada y completa de la situación en la JOA (EMAD, 2023).

El comandante Granados explica en detalle como la herramienta NCOP[61] puede materializar la COP en las FAS. Esta herramienta proporciona un acceso seguro a múltiples COP sobre mapas georreferenciados. La interfaz es una aplicación donde es posible superponer información en diferentes capas.

Sin embargo, existen importantes retos y problemas, actualmente, para poder materializar una COP que aporte la información adecuada en las FAS. El principal reto es discernir qué información es la verdaderamente importante representar para evitar una saturación que impida agilizar la toma de decisiones. Como ejemplos de problemas detectados, existe una falta de interoperabilidad entre los sistemas utilizados por los diferentes Ejércitos y la Armada o la dificultad para integrar la información procedente de los dominios ciberespacial y cognitivo.

Por otro lado, en la entrevista al comandante Granados se expone que la integración de los dominios ciberespacial y cognitivo en una COP es viable y puede materializarse a través de la implementación y desarrollo de herramientas como CEMACOP e INFOCOP[62],

[61] NCOP es una herramienta que proporciona conocimiento del entorno de una misión mostrando una COP alimentada por varios servicios de áreas funcionales.

[62] El CEMACOP es una herramienta táctica que proporciona conocimiento de la situación integrando información de ciberdefensa, guerra electrónica y gestión del espectro electromagnético. El INFOCOP está diseñado para la evaluación del entorno de información y la generación de una COP cognitiva. Integra análisis avanzados como categorización, análisis de credibilidad, detección de patrones, y dinámicas de opinión, aplicados a fuentes como redes sociales, informes y transmisiones multimedia.

las cuales están diseñadas para fusionar y representar datos de estos dominios de manera complementaria y efectiva.

Sin embargo, el teniente coronel Elías Entrialgo, responsable de MDO en J5 MOPS, no tiene constancia de que exista una previsión de integración de estos dominios en una COP, aparte de lo mencionado en el «Concepto Exploratorio. C2 de las MDO». Además, el teniente coronel López Resusta destaca que todavía las FAS están identificando qué información realmente es necesaria conocer y representar de los dominios ciberespacial, cognitivo, espacial y del espectro electromagnético en una COP.

Por lo tanto, del análisis y lectura de este último punto se extrae que, aunque existen herramientas en desarrollo que pueden facilitar la integración de información de los dominios no físicos en una COP, esta no está materializada actualmente en el nivel operacional. Además, se considera necesario definir de forma clara qué información es determinante para priorizar la obtención de los datos precisos, efectuar su análisis y posteriormente representarlos, evitando de esta forma la saturación con información innecesaria.

Otro aspecto esencial, que va ligado a la gestión del dato y la información, es la seguridad. Para poder establecer un adecuado C2MDO será necesario blindar el dato durante todas las etapas. De hecho, el profesor Rafael Calduch destaca, en su libro «El multidominio: fundamento de una nueva concepción estratégica», la importancia de la seguridad en la transmisión de los datos y la necesidad del adecuado funcionamiento de las telecomunicaciones (Calduch, 2025).

Esto supone aplicar un enfoque de seguridad desde que se obtiene el dato en la JOA, a través de uno de los sensores desplegados, hasta su almacenamiento y transmisión, de forma que se garantice que solo los usuarios autorizados puedan utilizarlo (EMAD, 2024: 18).

En este sentido, las FAS están trabajando en implementar el Data Centric Security (DCS), que consiste en aplicar una capa de defensa en profundidad que ofrece un mayor nivel de control sobre los datos y una mejor compartición al facilitar la gestión de identidades y accesos más detallada. DCS se enfoca en proteger los datos como el núcleo de cualquier estrategia de seguridad, asegurando su protección en reposo, en tránsito y en uso, independientemente del sistema o red en que se encuentren.

El comandante Granados Armuña explica que, hoy en día, estas capacidades no están implementadas, ya que se encuentran en fase de planeamiento. Esto no significa que no existan medidas de seguridad en los sistemas de las FAS. Actualmente, los Centros de Operaciones de Seguridad (COS[63]) centralizan las alertas y monitorizan los sistemas para poder responder ante una eventual amenaza de seguridad.

Sin embargo, el nivel actual de seguridad puede ser insuficiente para hacer frente a la demanda que las MDO van a generar, debido principalmente al enorme volumen de información y a la velocidad que debe ser transmitida. Esto implica que las vulnerabilidades que impidan garantizar la seguridad de las comunicaciones pueden restringir y retrasar el desarrollo de las redes multidominio.

En este campo, las FAS, a través de la LoE D «Digitalización» del Plan de implantación del JEMAD, se han marcado el objetivo de adoptar medidas de seguridad avanzadas que permitan la compartición de la información necesaria de forma segura.

4.3 Incorporación de Tecnologías Emergentes y Disruptivas

No se pueden entender las MDO sin la incorporación de tecnología avanzada en las FAS. La implantación de diferentes tecnologías de conectividad facilitará el crecimiento exponencial de sensores interconectados en todos los dominios de la JOA. Sin embargo, las EDT no se van a limitar a la gestión de la información. «La integración progresiva de las tecnologías que habiliten su ejecución, como el 5G o la IA, proporcionará la conectividad, la explotación de la información, la automatización y, en definitiva, la agilidad que requieren las MDO» (EMAD, 2023: 18).

Por lo tanto, se puede diferenciar, dentro de las EDT necesarias para implantar las MDO en las FAS, entre tecnologías de la comunicación (5G) y la propia IA. La primera permitirá mayores velocidades de conexión (ancho de banda), incrementando la capacidad de conectar dispositivos y la obtención y compartición de datos, mientras que la segunda tendrá un aspecto transversal que afectará a la mayor parte de las capacidades militares.

[63] «Estos centros están coordinados por el MCCE, en concreto, por la Fuerza de Operaciones en el Ciberespacio (FOCE) y realizan acciones de defensa, explotación y respuesta en el ciberespacio» (Ministerio de Defensa, 2025b).

Con respecto a la IA, el comandante Granados Armuña explica que, actualmente, existen numerosos proyectos para utilizar la IA en la gestión de datos dentro de las FAS, buscando algunos de estos procesar fuentes de información masivas para la gestión de datos en operaciones. Sin embargo, en la misma entrevista destaca que muchos proyectos se encuentran en fase de definición, algunos en fase de desarrollo, pero muy pocos en funcionamiento. De hecho, el comandante deja claro que, con las implementaciones actuales, la IA no puede facilitar la toma de decisiones, aunque sean de escasa relevancia.

El GB Frías expone que, en las FAS y en concreto en el ET, se está tratando de mecanizar con IA labores tradicionales de planeamiento que son esencialmente numéricas, como los cálculos logísticos. Sin embargo, expone que la situación actual se encuentra por detrás de otras Fuerzas Armadas en las que ya se está empleando en procesos complejos como el *targeting*.

Por otro lado, aunque existen desarrollos propios dentro del MINISDEF que en su gran mayoría desarrolla el «Instituto Nacional de Técnica Aeroespacial Esteban Terradas» (INTA), las empresas y la industria privada juegan un papel indispensable en el desarrollo de estos proyectos de IA, como ya lo hace con otros desarrollos de *software* del Ministerio.

Como explica el comandante Granados, en la actualidad, no se puede trabajar con soluciones de IA sin el apoyo de la industria privada. Lo habitual es que haya una empresa privada detrás de cada proyecto de IA y con la mayoría de implementaciones de nuevas tecnologías. La capacidad de desarrollo de soluciones dentro del MINISDEF está prácticamente limitada al INTA.

Esto supone serios retos y problemas para las FAS que hay que tener en consideración a la hora de buscar soluciones con empresas ajenas al MINISDEF. La seguridad en el empleo de herramientas que son proporcionadas desde el ámbito civil o la necesidad de garantizar la autonomía de las FAS sobre los productos o aplicaciones con IA que se adquieran de la empresa privada son dificultades añadidas que las FAS deben abordar.

Con respecto a las tecnologías de la comunicación, el Plan de implantación del JEMAD, a través de la LoE D «Digitalización», ha establecido la LA-3 «Proyecto 5G conjunto». En esta línea de actuación, se marcan las pautas para homogeneizar las distintas iniciativas relativas a tecnología 5G. Sin embargo, esta medida, que es esencial para el buen funcionamiento de la nube de com-

bate, se encuentra en fase de definición y aunque, actualmente, hay activo un GT 5G, no se esperan resultados tangibles hasta la fase II (2027-2032) (EMAD, 2025: A12).

Esta LA cobra especial importancia si se tiene en consideración el gran protagonismo que las redes de telefonía móvil han cobrado en la guerra de Ucrania. El capitán de navío Luis Francisco Astorga González explica en el capítulo 2 de la publicación *TD de las FAS para el combate multidominio* que Ucrania ha hecho uso de redes 3G y 4G en sus operaciones y les ha negado su empleo a los rusos, impidiendo cualquier servicio de *roaming* procedente de Rusia o Bielorrusia (Morón Ruiz *et al.*, 2023: 75).

Una conclusión parcial de este punto es que las FAS inmersas en una MDO van a necesitar utilizar las redes comerciales disponibles, también en el 5G y en el futuro 6G, además del despliegue de su propia infraestructura. Por lo que la LA-3 se configura como esencial para alcanzar la capacidad MDO.

Otro factor para tener en consideración es que, aunque la incorporación progresiva de las nuevas tecnologías será determinante para alcanzar la madurez multidominio, los numerosos medios tecnológicos pueden convertirse en una fuente de dependencia si no se integran en la organización de una manera transcendente. El teniente coronel Vega Bustelo explica que la tecnología multiplica la productividad si se usa correctamente, pero si su uso no es eficaz, se va a producir el efecto contrario multiplicando las ineficiencias. Además, añade que las nuevas tecnologías, a través del proceso de TD de las FAS y unido a la implantación efectiva del MoM consolida un círculo con efectos verdaderamente multiplicadores de la capacidad de combate (Vega Bustelo, 2021).

Esto permite extraer que el papel de la formación multidominio y el liderazgo son esenciales para que se lleve a cabo una incorporación efectiva de las EDT en las FAS. Estas tres variables de estudio están totalmente relacionadas y cualquier aplicación tecnológica que se produzca en el campo del C2MDO debe tener su reflejo, de forma inmediata, en los planes de estudios de los cuadros de mando que van a liderar al personal de las FAS.

5 Implementación de medidas en la estructura de mando y control

La transformación del C2 hacia un enfoque multidominio requiere adaptar sus estructuras para operar con mayor flexibilidad, coor-

dinación e integración. La capacidad de generar efectos en todos los dominios demanda estructuras que permitan actuar con agilidad, integrando múltiples actores y facilitando la cooperación entre los Ejércitos/Armada y con países aliados y amigos.

5.1 Agilidad

En el contexto del C2MDO, esta variable de estudio es la capacidad que permite a la FC adaptar las condiciones iniciales del C2 y efectuar las modificaciones necesarias, en tiempo útil, para adaptarse a los cambios del entorno operativo. Esto implica que la FC, durante la conducción de una operación, debe identificar que la situación ha cambiado, seleccionar el enfoque de C2 más adecuado y ser capaz de llevar a cabo una transición eficaz (EMAD, 2024: 7).

Las diversas publicaciones MDO han identificado diferentes modelos y estructuras de C2, que se caracterizan por un determinado grado de descentralización, colaboración y disponibilidad de la información (ver figura 5).

Entre los diferentes modelos, el denominado «Edge C2» se basa en una descentralización del mando y control, permitiendo tomar decisiones en los niveles más bajos y mejorando la agilidad en entornos dinámicos y complejos. Este modelo es el más adecuado para hacer frente a las máximas exigencias de una MDO, pero también requiere un alto grado de descentralización, colaboración y disponibilidad de la información.

En el «C2 colaborativo», el comandante se comunica con su Estado Mayor y con los múltiples nodos, plataformas y sensores disponibles para tener un mejor conocimiento de la situación. De esta forma, podrá tomar la decisión de actuar o delegar la acción a su Cuartel General (HQ), permitiéndole seguir observando y conduciendo la operación.

En tercer lugar, el «C2 coordinado» propone la centralización del mando y control usando tecnologías avanzadas que permitan la toma de decisiones desde un punto central, lo que puede mejorar la eficiencia con respecto a los modelos anteriores, pero a costa de la flexibilidad.

Por último, existen modelos mixtos que buscan un enfoque híbrido con todos los anteriores, creando un sistema de C2 adaptable y resiliente, que sea capaz de enfrentarse a la gran variedad de desafíos existentes (Meddings, 2021).

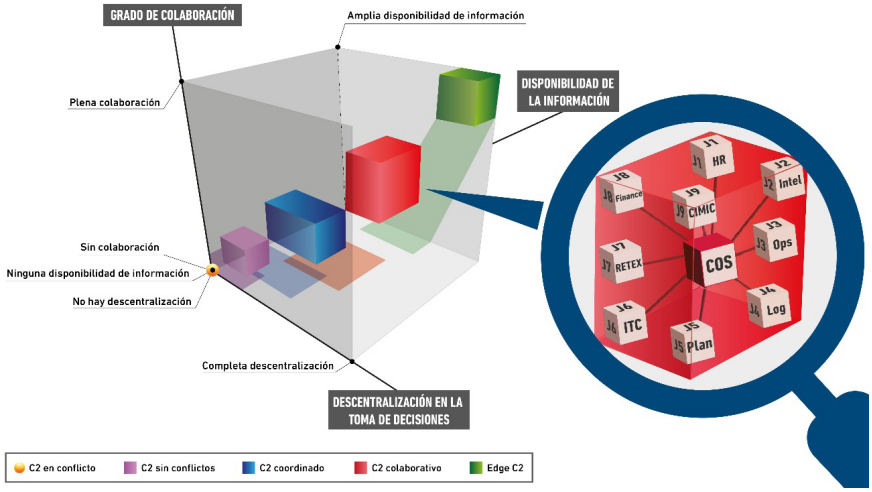


Figura 5. Diferentes modelos de mando y control. Fuente: EMAD (2024: 26)

Analizando las entrevistas a los expertos, el comandante González Espadas considera que el objetivo que se debe alcanzar para adaptar el C2MDO no es la descentralización del C2, sino la capacidad de descentralizar el C2 cuando sea necesario. Es decir, habrá situaciones donde el modelo C2 centralizado sea el más conveniente y otras en las que será necesario distribuir la función de C2 hasta donde las condiciones lo permitan. Por lo tanto, desde este enfoque, el C2 debe ser un capacitador para hacer frente al complejo y cambiante entorno operacional.

Actualmente, cada Ejército/Armada dispone de su propia estructura de C2, que se adapta a las necesidades de su dominio[64] de actuación principal. El comandante González, considera que, con independencia del dominio principal de actuación, se debe emplear el medio más adecuado para lograr el efecto deseado. Esto obliga a tener una estructura única de C2 capaz de ejercer su función sobre todos los medios disponibles que permita generar los efectos necesarios, independientemente del dominio. Esta es una de las funciones principales que el SC2N debe ser capaz de llevar a cabo, cuando alcance la madurez suficiente, para poder habilitar la ejecución de MDO en las FAS con la agilidad suficiente.

[64] Es decir, actualmente el Ejército de Tierra tiene un sistema de C2 adaptado al dominio terrestre, la Armada al marítimo y el Ejército del Aire y el Espacio al dominio aéreo/espacial.

Además, el comandante González Espadas pone el foco en que incrementar la agilidad en las FAS va a suponer reconsiderar la atribución de los derechos de decisión (quién decide), los patrones de interacción entre todos los actores participantes en una MDO y que información se comparte y entre quienes. Al valorar este último punto del comandante González, se extrae que no existe ninguna LA específica en el Plan de implantación del JEMAD que aborde estas cuestiones, aunque se podría considerar de forma implícita en la LoE B «Ejercicios, Experimentación y Wargaming» o en la LA «Ejercicios».

Con respecto a los cambios en la estructura de C2, el teniente coronel López Resusta considera que no son un concepto novedoso y que siempre se han producido en las FAS. Un ejemplo claro son las Transferencias de Autoridad (TOA[65]) que se llevan a cabo en Operaciones de Mantenimiento de la Paz. Lo que se plantea en las MDO sería algo muy similar, pero de forma mucho más ágil para adaptarse a las necesidades de estas operaciones.

Este enfoque que propone el teniente coronel López Resusta, que debe ser sustentado por la tecnología, permite visualizar como durante la conducción de una MDO se puede modificar la estructura de C2 según sea necesario. Cuando las circunstancias lo aconsejen, se efectuará la entrega o delegación de autoridad a aquel personal que se encuentre en las mejores condiciones para decidir o actuar, permitiendo una agilidad superior al adversario y, por lo tanto, obteniendo la superioridad en el ciclo de la decisión.

Sin embargo, materializar este último punto no es tarea sencilla, ya que requiere haber asentado la mayor parte de las variables de estudio tratadas hasta el momento. Para empezar, se requiere un MoM consolidado y una formación MDO sustentada por muchas horas de ejercicios y adiestramiento específico. Además, se necesitará el factor tecnológico (conectividad y gestión del dato) para poner a disposición del responsable de decidir o actuar la información suficiente que le permita tener un nivel adecuado de conocimiento de la situación del campo de batalla y así visualizar la necesidad y conveniencia de cambiar la estructura de C2.

[65] «La TOA se produce entre autoridades militares de diferentes estructuras. Todo comandante que delega o transfiere autoridad puede, en el momento que lo considere necesario, recuperarla o modificar las condiciones» (Ministerio de Defensa, 2024d: 105).

Por otro lado, y en opinión del GD Morón, para adaptar la agilidad a las necesidades del C2MDO, el principal cambio no es tecnológico, sino de cultura organizativa. Aunque la tecnología tendrá un papel fundamental, el general considera que para incrementar la agilidad se debe reducir la estructura vertical de la organización en la toma de decisiones, reduciendo los niveles jerárquicos. Además, remarca que se deberá materializar un verdadero cambio de mentalidad en las FAS, con menos planificación a largo plazo e incorporando realmente metodologías ágiles.

Como conclusión de este punto y tras el análisis efectuado de las publicaciones MDO y las opiniones de expertos, se extrae que la agilidad necesaria para el C2MDO requiere necesariamente del factor tecnológico, de forma que se pueda modificar el modelo de C2 cuando sea necesario durante una operación. Sin embargo, la tecnología, que en el caso de las FAS se materializará con el SC2N, es condición necesaria pero no suficiente, ya que necesita de otros aspectos humanos, conductuales y estructurales para obtener la agilidad necesaria en el entorno multidominio con el único fin de acelerar el ciclo de la decisión.

5.2 Enfoque integral

Las experiencias obtenidas en los conflictos de las últimas décadas, como Afganistán, han demostrado que el instrumento militar es necesario pero insuficiente para resolver las crisis o conflictos actuales, debido a la complejidad y multitud de actores involucrados. Además, las amenazas abarcan todos los dominios a través de guerras convencionales, conflictos híbridos, ciberataques o desinformación. Esta gran diversidad requiere un enfoque integral y multidominio para garantizar la seguridad (EMAD, 2024).

En el Plan de implantación del JEMAD, dentro de la LoE B «Ejercicios, Experimentación y Wargaming» y en concreto, en la LA «Experimentación y Wargaming» se incluye, como actores participantes, a todos los instrumentos de poder del Estado y a la Industria, además de los Ejércitos, la Armada y el EMAD. El principal objetivo es impulsar la coordinación de actividades de innovación y experimentación que faciliten la adaptación de las MDO en las FAS (EMAD, 2025: A6).

Además, los ejercicios planificados incluyen escenarios multidominio que promueven la participación de actores civiles y gubernamentales, simulando entornos de crisis y conflictividad

compleja. Esto busca fomentar la colaboración efectiva entre todos los actores implicados.

El teniente coronel Elías Entrialgo considera que la colaboración entre las autoridades civiles y militares, como parte de las operaciones militares, es cada vez mayor. De hecho, en las misiones NEO que se han conducido desde el MOPS, se ha contado con personal civil desde la fase de planeamiento hasta la de ejecución. Además, personal del Ministerio de Asuntos Exteriores (MAUEC) forma parte del JOC en el MOPS. En la misma línea que el teniente coronel Elías Entrialgo, el GD Morón utiliza el ejemplo de la participación de la Unidad Militar de Emergencias (UME) bajo el mando y dirección del CECOPI[66] en determinadas emergencias.

Con un enfoque diferente al expuesto hasta el momento, el GB Frías pone de relevancia que cuando las FAS y las organizaciones civiles trabajan juntas aparecen fricciones. Aunque las MDO requieren conocimientos específicos, hay que tener en consideración que la forma de trabajar de las FAS es muy diferente a la de las organizaciones civiles. En tiempo de paz es posible y relativamente sencillo incorporar elementos civiles en las operaciones, sobre todo en los dominios ciberespacial, espacial y cognitivo, ya que están activos permanentemente, incluso en tiempo de paz.

Sin embargo, en tiempo de guerra, con operaciones de combate, el GB Frías considera mucho más complicada que esta integración sea efectiva. En esos momentos, la disciplina es fundamental y las organizaciones civiles no están acostumbradas a ella. Este es uno de los motivos por los que se emplean a los ejércitos en caso de catástrofes, porque sin el «pegamento» de la disciplina, las organizaciones civiles colapsan en caso de crisis.

Los dominios no físicos y las EDT van a exigir una alta especialización. Personal con conocimientos en tecnología cuántica, expertos en ciberdefensa o en el dominio espacial serán recurso crítico a corto plazo. Las FAS van a necesitar este talento dentro de la organización, pero actualmente no pueden competir con la empresa civil por razones económicas y la inestabilidad inherente a la profesión militar.

[66] «El Centro de Coordinación Operativa Integrado (CECOPI) es una infraestructura (normalmente 112), que permite las labores de gestión, dirección y coordinación por el órgano de dirección del plan, así como la integración de los representantes de diferentes administraciones involucrados en la emergencia» (Ministerio del interior, 2019: 11).

La visión del GB Frías sobre el concepto de enfoque integral es la de un «grito de socorro» de las FAS cuando se enfrentan a problemas complejos que superan sus competencias. Es decir, el enfoque integral se contempla como una necesidad de disponer de personal no militar especializado en determinadas áreas para que permitan cumplir una misión a las FAS que no es por completo de índole militar. Una parte de este requerimiento de personal civil altamente especializado se podría mitigar, aunque no resolver, con una nueva regulación de la figura del reservista[67].

Por lo tanto, tras el análisis de este punto, se extrae que el éxito para alcanzar un enfoque integral efectivo no puede descansar exclusivamente en las FAS. Alcanzar la madurez en las MDO debe ser una responsabilidad que se inicie desde el nivel político. Es necesario un potente impulso desde el Gobierno que obligue a los tres niveles de la administración (Estado, autonomías y ayuntamientos) a operar armónicamente con las FAS. Con independencia de que las FAS se configuren como los principales impulsores de las MDO, el esfuerzo para alcanzar un enfoque integral efectivo debe ser iniciado desde el nivel político (MINISDEF) y debe calar en la sociedad a través de la potenciación de la cultura de defensa.

5.2.1 El enfoque integral y los dominios no físicos

La transversalidad de los dominios ciberespacial y cognitivo los convierten en esenciales para las MDO. El empleo de estos dominios no físicos se ha generalizado debido al desarrollo tecnológico, a su accesibilidad y a la facilidad para realizar acciones, que son difícilmente atribuibles, ya que favorecen el anonimato.

Tal y como describe el comandante Granados Armuña en su entrevista, España ha desarrollado una conceptualización propia sobre las MDO, reconociendo la importancia de integrar dominios tradicionales con los no físicos. Se enfatiza el carácter transversal del ámbito cognitivo, crucial para influir en la percepción y la toma de decisiones, y del ciberespacial, clave para la conectividad y la gestión de información.

Sin embargo, tras efectuar la investigación, se concluye que existe una falta de consenso nacional e internacional[68] y ambi-

[67] En España, la regulación de los reservistas se encuentra principalmente en el Título VI de la Ley 39/2007, de la carrera militar.

[68] Por ejemplo, la doctrina OTAN considera solo cinco dominios, limitando lo cognitivo a una dimensión de efectos. La doctrina nacional si lo tiene en consideración,

güedades en la definición de algunos dominios. Es decir, se han detectado discrepancias relevantes a la hora de establecer los elementos más básicos que deben quedar claros a nivel doctrinal y conceptual antes de seguir avanzando en la adaptación a las MDO en las FAS. Para demostrar este punto, a continuación, se van a exponer las opiniones y reflexiones de los expertos consultados a este respecto.

Con relación al dominio cognitivo, el GB Frías considera que su creación ha sido contraproducente. El general explica que el objetivo de las operaciones militares es «convencer» al enemigo de que se pliegue a nuestra voluntad. Esto quiere decir que todo lo que se hace en la guerra es «dominio cognitivo». Por este motivo, al crearlo de forma específica quita el sentido al resto de las operaciones, pues el dominio es solo el medio físico, pero no es la finalidad.

Sin embargo, el teniente coronel Elías Entrialgo considera un error que haya naciones que no consideren el dominio cognitivo en su doctrina. La razón que expone es que las MDO deben englobar todos los ámbitos y factores que puedan afectar a las operaciones y considera que la aproximación nacional conceptual es apropiada.

Por otro lado, esta investigación ha analizado la necesidad de establecer un «dominio electromagnético». Actualmente, el entorno electromagnético se considera parte del dominio ciberespacial. Sin embargo, son varios los expertos que consideran la necesidad de incluirlo como un dominio más.

En concreto, el teniente coronel Elías explica la relevancia que tiene el espectro electromagnético para las FAS y que ha implicado la creación en MOPS de una célula que se denomina Centro de Operaciones Electromagnéticas (COEM), que está incluida en todos los planeamientos, conducción y seguimiento de misiones y operaciones. Actualmente, esta célula gestiona informes requeridos por las operaciones dentro del entorno electromagnético.

Según el profesor Rafael Calduch, uno de los aspectos decisivos de la seguridad del dato corresponde a su transmisión, lo que vincula directamente este aspecto esencial, con el espectro electromagnético y la garantía de su correcto y estable funcionamiento en las telecomunicaciones. Este es uno de los motivos

desarrollándose este en el entorno de la información y cuyo espacio se delimita mediante audiencias (EMAD, 2025: 3).

principales por los que el profesor defiende que el espectro electromagnético debe ser un dominio propio diferenciado del ciberespacio (Calduch Cervera, 2025).

El teniente coronel López Resusta y el comandante Granados Armuña también consideran la necesidad de definir el entorno electromagnético como un dominio más, ya que forma parte de todos los dominios y permite influir en todos ellos, por lo que cumple con los requisitos para su consideración como tal.

Sin embargo, existen varios expertos que consideran esto un error. En concreto, el GB Frías expone que el entorno electromagnético es exclusivamente un medio y lo emplean las unidades que operan en cualquiera de los dominios ya establecidos. Separarlo implicaría crear restricciones adicionales al empleo de herramientas tan habituales como la radio, los radares o los láseres. De hecho, el GB Frías explica que los dominios son herramientas conceptuales, que se utilizan porque son útiles para confeccionar el espacio de las operaciones. Si crear un nuevo dominio no supone un beneficio o incluso provoca ser menos eficaz, hay que evitarlo, aunque, formalmente quede una construcción intelectual elegante.

El teniente coronel Vega Bustelo también considera un error la posibilidad de establecer un dominio electromagnético. Para ello, explica que la guerra electrónica es aquella que se libra en una parte de la capa física del dominio ciberespacial, la de los segmentos inalámbricos de las redes y los sensores. Por esta razón, no tiene ningún sentido considerarlos por separado. Como punto reseñable, el teniente coronel señala que el debate existente sobre este tema puede surgir de cierta resistencia por parte del ámbito de la EW, que ha pasado de ser el elemento referencia a una capa más del dominio ciberespacial.

Por lo tanto, se observa que existen tantos enfoques como expertos consultados con relación a la definición de los dominios no físicos. Esto permite extraer que, aunque las publicaciones doctrinales nacionales son coherentes y están alineadas en este punto, existe una deficiencia conceptual que debería abordarse por parte del grupo de trabajo que está desarrollando la LoE C «Doctrina y Conceptos» del Plan de implantación del JEMAD. De hecho, existe una LA «Conceptos» cuyo propósito es «apoyar la implantación de las MDO mediante los desarrollos conceptuales necesarios» (EMAD, 2025: 16).

Por otro lado, también se puede concluir que la complejidad inherente a las MDO exige que cualquier concepto doctrinal que se aplique en las FAS debe ir encaminado a facilitar y simplificar la acciones y los efectos que debe producir la FC. Cualquier elemento que no facilite el entendimiento de las MDO o no vaya en concordancia con la doctrina nacional o aliada va a suponer un obstáculo para avanzar en la adaptación al C2MDO y va a dificultar la necesaria interoperabilidad, que va a ser expuesta a continuación.

5.3 Interoperabilidad

Las MDO se basan en la conexión de todas las plataformas, armas y sensores, a través de todos los dominios, de forma que se permita una sincronización de todas las capacidades y un eficiente conocimiento de la situación. Esto solo se puede producir si se alcanza una interoperabilidad efectiva. Para el comandante González Espadas no se puede hablar de interoperabilidad sin tratar la conectividad, ya que están íntimamente relacionadas. Como ejemplo en este caso, la conectividad se presenta como los medios y sistemas de C2 utilizados y la interoperabilidad es habilitar que todos ellos hablen el mismo idioma.

En la misma línea, el comandante Granados Armuña explica la importancia de la interoperabilidad para alcanzar la adecuada agilidad que requieren las MDO. La integración de todas las capacidades de la FC en un único Sistema de Mando y Control Nacional (SC2N) es esencial para gestionar el gran volumen de información y reducir los tiempos en el proceso de toma de decisiones. Además, expone que la nube de combate es el otro elemento clave para garantizar la interoperabilidad. Su diseño como un «sistema de sistemas» interconectados permite integrar capacidades, plataformas y sensores de todos los dominios.

Para el teniente coronel Vega Bustelo, desde el punto de vista de interoperabilidad, lo más importante es la estandarización de datos y metadatos a través del modelo de seguridad centrado en los datos (DCS). Esta estandarización es lo que va a permitir que la información pueda fluir, a través de la red, entre cualquier equipo disponible.

Gran parte del esfuerzo de la LoE D «Digitalización», del Plan de implantación del JEMAD, se centra en reducir las dificultades de interoperabilidad y coordinación entre dominios y sistemas. Sin

embargo, se detecta que todas las medidas se centran de forma exclusiva en el campo tecnológico. En opinión del comandante Granados Armuña, abordar la interoperabilidad desde el enfoque multidominio implica eliminar los silos que existen actualmente y potenciar las sinergias entre los ejércitos, la Armada y el resto de actores involucrados en las operaciones militares. Actualmente, a pesar de que existen esfuerzos conjuntos, falta mucha coordinación e integración de procedimientos entre los diferentes actores que dificultan una adecuada interoperabilidad.

La interoperabilidad no solo debe alcanzarse a nivel nacional. Las MDO implican necesariamente la coordinación, en todos los dominios, de las FAS españolas con la OTAN y los países aliados. Al igual que ocurre en España, aunque la OTAN está avanzando hacia una visión conjunta de MDO, todavía se enfrenta a desafíos significativos relacionados con la unidad doctrinal. Los esfuerzos individuales de los países aliados para desarrollar las MDO y la falta de estándares claros han generado ambigüedades e incoherencias conceptuales[69].

Además, lecciones identificadas muestran que la OTAN tiene margen de mejora a la hora de ejecutar operaciones conjuntas, por lo que intentar evolucionar hacia las MDO, que requieren un mayor nivel de interoperabilidad, puede ser un desafío difícil de conseguir (Perkins y Olivieri, 2018).

Sin embargo, el teniente coronel López Resusta considera que existe suficiente unidad de doctrina en la OTAN, aunque de momento se identifiquen diferentes dominios. La OTAN está empezando a tomarse en serio la adaptación a las MDO[70] y tienen los mismos problemas que España a la hora de implementar medidas. Estas diferencias no son incapacitantes, aunque no exista actualmente una total interoperabilidad.

6 Conclusiones

La presente investigación se ha desarrollado con el propósito de analizar en profundidad el grado de adecuación de las medidas que las FAS españolas están implementando para adaptar su sistema de C2 a las exigencias de las MDO. A través del empleo de los métodos descriptivo y analítico, se ha efectuado una valo-

[69] Un ejemplo es el dominio cognitivo que identifican las FAS, pero no la OTAN.

[70] La OTAN aprobó en el año 2023 el *Alliance Concept for Multi-Domain Operations* como la publicación referencia que establece la estrategia de la OTAN para las MDO.

ración en profundidad de los factores y variables de estudio identificadas.

Con relación a la variable formación, se concluye que es una medida necesaria e imprescindible para implementar con éxito el enfoque multidominio. El Plan de implantación del JEMAD la recoge como una prioridad, a través de una línea de esfuerzo específica (LoE A). Sin embargo, la investigación valora que no se ha alcanzado todavía una formación unificada y coherente, lo que compromete su eficacia. En la actualidad, existen iniciativas parciales en los Ejércitos y la Armada, pero no hay una estrategia formativa consolidada desde el MINISDEF que garantice una base sólida y homogénea. La necesidad de una formación con base común, que sea transversal a todas las FAS, es esencial para lograr una visión unificada y facilitar la integración del personal en el planeamiento y ejecución de las MDO.

Por otro lado, se ha identificado la necesidad de desarrollar y definir con mayor profundidad la doctrina multidominio. Varios expertos señalan que no se puede formar en MDO sin una doctrina clara y unos procedimientos bien establecidos. Hoy en día, existen muchos interrogantes operativos, especialmente en los dominios no físicos como el ciberespacial, que impiden avanzar con solidez en el ámbito formativo.

En cuanto al cambio de mentalidad, se concluye que la formación debe ser el vector principal para transformar la cultura organizacional, potenciando habilidades como el pensamiento crítico, la creatividad y la capacidad para asumir riesgos. Estas competencias son claves en entornos complejos y cambiantes como los que caracterizan a las MDO.

La realización de ejercicios, experimentación y *wargaming* se considera fundamental para consolidar la adaptación al enfoque multidominio. Las primeras iniciativas previstas son un paso positivo importante, pero todavía insuficiente, ya que se necesita generalizar en todos los ámbitos de las FAS las prácticas MDO.

El estudio identifica el liderazgo en las FAS como una variable crítica actualmente insuficiente para abordar los desafíos de las MDO. La organización quiere apostar por el liderazgo transformacional y el Mando orientado a la Misión, ya que ambos modelos promueven la iniciativa, la delegación de autoridad y la adaptación al cambio. Todas las publicaciones doctrinales y relacionadas con las MDO identifican este tipo de liderazgo y cultura de delegación como la ideal.

Sin embargo, el análisis efectuado en base a las entrevistas a expertos revela que la cultura organizacional vigente supone un obstáculo estructural en la adaptación a las MDO. Predomina la microgestión, existe escasa tolerancia al error y se mantiene una fuerte orientación al logro individual, lo que dificulta en gran medida la iniciativa y la colaboración.

La estructura jerárquica tradicional, junto con una desconfianza hacia los niveles inferiores, refuerza un modelo de liderazgo transaccional que no se ajusta a la agilidad y descentralización requeridas por las MDO. La delegación de autoridad sigue siendo limitada y condicionada por la saturación de trabajo en los niveles superiores. En este contexto, el MoM no está siendo implementado de manera efectiva. Se percibe más como un concepto doctrinal que como una realidad operativa. La transformación cultural requerida exige un cambio profundo de mentalidad en la cadena de mando, donde el error se entienda como oportunidad y la iniciativa se premie como motor de innovación. Esta investigación concluye que con una correcta y eficaz implementación del MoM y del liderazgo transformacional sería viable y más rápido implementar el C2MDO en las FAS.

La conectividad se identifica como un habilitador esencial para el C2MDO, ya que permite operar con agilidad y sincronización en todos los dominios. Sin embargo, las capacidades actuales de las FAS aún están en fase de desarrollo, como evidencia el estado intermedio del SC2N y la inexistencia de una nube de combate conjunta plenamente operativa.

La Infraestructura Integral de Información para la Defensa constituye un avance tangible, pero todavía existen carencias en interoperabilidad, estandarización y despliegue de nodos, lo que limita la operatividad conjunta. Además, es necesario mitigar los efectos negativos que la conectividad podría suponer, como la centralización no deseada de las decisiones por los escalones superiores o una «ilusión de control» en entornos degradados, tal como advierten varios expertos.

Aunque el Plan de implantación contempla medidas como la LoE D «Digitalización» y líneas de actuación específicas, el sistema actual es insuficiente para satisfacer las exigencias del combate multidominio, aunque la investigación concluye que las necesidades están identificadas y se está trabajando para incrementar las capacidades.

La gestión eficaz de datos e información es fundamental para lograr la superioridad en la decisión en entornos multidominio. Las FAS están desarrollando capacidades incipientes, pero aún lejos de ser suficientes. Actualmente, el volumen de información manejado es asequible, pero se prevé una explosión de datos, derivada de la sensorización del campo de batalla, que requerirá herramientas de análisis como IA y sistemas etiquetados con metadatos, que aún no están integrados en el nivel de la FC.

Además, se destaca la necesidad de consolidar un sistema común de datos y asegurar su análisis y distribución adecuada a cada usuario, algo que hoy es más una aspiración que una realidad. Actualmente, existen herramientas, que se emplean de forma aislada por algunas unidades, que podrían ser una solución viable y global para las FAS en su conjunto.

Además, existen dificultades en la construcción de una *Common Operational Picture* robusta e integrada, especialmente en interoperabilidad entre ejércitos y en la integración de los dominios no físicos, como el ciberespacial o el cognitivo. Asimismo, la seguridad del dato, aunque abordada mediante protocolos y proyectos como el Data Centric Security (DCS), todavía no está implantada plenamente.

El uso de EDT como la IA o el 5G es fundamental para transformar el C2MDO. Sin embargo, en las FAS, la mayoría de los proyectos con IA se encuentran en fases tempranas de desarrollo o definición y solo algunas herramientas puntuales están en un uso limitado. La dependencia tecnológica de la industria privada plantea riesgos en cuanto a autonomía, seguridad y control de los sistemas. Por este motivo, se están impulsando medidas como el «Proyecto 5G conjunto», aunque los resultados no serán tangibles hasta la fase II del plan (2027-2032).

Por otro lado, la investigación permite establecer que la incorporación de EDT es imprescindible, pero no se logrará un impacto real sin que se produzca una transformación simultánea en liderazgo y formación, que asegure su integración efectiva. En este sentido, la tecnología no es suficiente sin que se interiorice una mentalidad en las FAS que abrace el cambio, la iniciativa y la innovación.

Las medidas que están adoptando las FAS en materia de agilidad para el C2MDO son necesarias, pero aun claramente insuficientes. La implementación del SC2N y el desarrollo de la nube de combate son avances esenciales, pero no garantizan la capacidad

de modificar eficazmente la estructura de C2 durante una operación. Es decir, la tecnología habilita la agilidad, pero no la va a generar.

La agilidad que se requiere a nivel operacional exige un sistema de C2 adaptable, capaz de alternar entre modelos centralizados y descentralizados según las circunstancias de la operación en curso. La investigación concluye que esta capacidad de transición, que constituye la esencia del C2MDO, no está interiorizada aún en la estructura de mando, donde persiste una configuración rígida, heredada de los dominios tradicionales.

Además, se ha identificado una necesidad de revisar los procedimientos de decisión, los patrones de interacción entre todos los actores que pueden darse en una MDO y los procedimientos de compartición de información, elementos clave para dotar de agilidad al sistema. Aunque algunas de estas necesidades están implícitas en iniciativas como los ejercicios y la experimentación, no existen líneas de acción específicas dentro del Plan de implantación del JEMAD que aborden la agilidad como objetivo transformador prioritario.

Por otro lado, los condicionantes estructurales y culturales siguen actuando como freno para la agilidad. Sin una transformación organizativa que aplane la estructura, delegue realmente decisiones en niveles inferiores y promueva la autonomía, cualquier intento de agilizar el C2MDO será limitado. En este sentido, la cultura organizativa actual de las FAS, centrada en la planificación detallada y el control vertical, no favorece la agilidad que requieren las MDO.

Asimismo, la incorporación de la agilidad en el C2MDO requiere haber consolidado previamente otras variables de estudio como la formación MDO, el liderazgo transformacional o la disponibilidad de la información necesaria en tiempo real. Sin estos pilares, las FAS no podrán efectuar una adaptación a las MDO eficaz.

Por tanto, se concluye que las medidas tecnológicas en curso son una condición necesaria, pero insuficiente. La agilidad real en las FAS dependerá de su capacidad para acometer una transformación cultural, doctrinal y organizativa que permita que la tecnología se convierta en un auténtico factor multiplicador. Sin este cambio profundo, las FAS seguirán operando con un modelo de C2 que, aunque tecnológicamente más avanzado, no responderá con eficacia a la dinámica compleja y cambiante de las MDO.

Las MDO requieren integrar actores civiles y militares para producir efectos en todos los dominios, especialmente en los no físicos. Aunque ya existen experiencias de colaboración, como las operaciones NEO ejecutadas en últimos años, persisten fricciones debido a la diferencia de cultura organizativa entre FAS y entidades civiles. Una parte del requerimiento de personal civil altamente especializado que requieren las MDO se podría mitigar con una nueva regulación de la figura del reservista.

Por otro lado, el Plan del JEMAD promueve la inclusión de actores civiles a través de ejercicios y programas formativos, lo cual es un paso positivo. Sin embargo, el éxito del enfoque integral no puede depender exclusivamente de las FAS. Es necesario un impulso político decidido y claro que coordine a los distintos niveles de la administración y fomente una cultura de defensa que facilite la colaboración. Aplicar el modelo de coordinación de la UME con la administración civil en los casos de emergencias para alcanzar un enfoque integral efectivo en una MDO podría ser una medida a explorar y desarrollar.

En relación con los dominios no físicos, como el cognitivo y el ciberespacial, persiste una falta de consenso conceptual. Mientras algunos expertos defienden su integración como dominios transversales, otros consideran que su definición como dominios independientes es confusa y contraproducente. Sin embargo, las publicaciones doctrinales nacionales son coherentes y están totalmente alineadas a la hora de definir los diferentes dominios.

La interoperabilidad es un pilar imprescindible para las MDO. Sin ella, la sincronización entre plataformas, sensores y armas en todos los dominios sería inviable. El SC2N y la nube de combate son elementos clave para lograr este objetivo, al permitir una arquitectura común y fluida de intercambio de información. A nivel doctrinal y técnico, las medidas recogidas en la LoE D «Digitalización» del Plan del JEMAD reflejan un esfuerzo serio y dirigido.

Sin embargo, estos avances se centran exclusivamente en la tecnología, dejando de lado aspectos de interoperabilidad en coordinación de procedimientos y diferencias culturales entre los Ejércitos/Armada. En suma, aunque las medidas tecnológicas son necesarias, no son por sí solas suficientes.

Tras el análisis en profundidad de la investigación, se valora que las Fuerzas Armadas españolas están implementando medidas necesarias y suficientes para adaptar el factor humano, la estruc-

tura y los procesos C2MDO. Sin embargo, esta validación se considera parcial, ya que las medidas implementadas son necesarias, pero no completamente suficientes, especialmente en lo relativo a la transformación cultural y organizativa de las FAS que exigen las MDO.

El estudio demuestra avances claros, especialmente, en el ámbito doctrinal y tecnológico. De hecho, el desarrollo del SC2N, la nube de combate y la planificación de ejercicios MDO, como el JFX/MDO-25, constituyen pasos decididos en la dirección correcta. No obstante, el cambio de mentalidad en liderazgo, la adopción real del MoM y la superación de resistencias estructurales requieren todavía mayor profundidad y compromiso. Además, es necesario alcanzar un enfoque integral más efectivo y establecer un mayor impulso en el campo de la interoperabilidad para garantizar la madurez del sistema.

En conclusión, las FAS están en el camino adecuado, pero deben consolidar e intensificar esfuerzos para alcanzar una adaptación plena al entorno multidominio.

Bibliografía

Andrés Ibarzo A. (2024). ¿Es posible mejorar la respuesta de los ejércitos frente a la complejidad? Adaptación orgánica [en línea]. MADOC, Ejército de Tierra. [Consulta: 12 enero 2025]. Disponible en: https://ejercito.defensa.gob.es/gl/Galerias/Descarga_pdf/Unidades/Granada/madoc/2025/pdf_notici_lecturas_madoc_2.pdf

Cabrera, J. (2017). Redarquía: más allá de la jerarquía [en línea]. Cabrera MC. [Consulta: 22 abril 2025]. Disponible en: https://cabreramc.com/redarquia/

Calduch Cervera, R. (2014). Métodos y técnicas de investigación internacional [en línea]. 2.ª. ed. Madrid, Universidad Complutense de Madrid. [Consulta: 20 octubre 2024]. Disponible en: https://www.ucm.es/data/cont/docs/835-2018-03-01-Metodos%20y%20Tecnicas%20de%20Investigacion%20Internacional%20v2.pdf

—. (2025). El multidominio: fundamento de una nueva concepción estratégica [en línea]. En: García García, M.ª I. (ed.) y García Bázquez, F. (coord.). *La ambición estratégica de España*. Dykinson S. L., pp. 203-220.

EMAD. (2021). *PDC-3. Doctrina de Operaciones*. Madrid, Ministerio de Defensa.

—. (2022). *Visión del JEMAD de la Nube de Combate*. Madrid, Estado Mayor Conjunto de la Defensa.

—. (2023). Concepto exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Madrid, Ministerio de Defensa, Centro Conjunto Desarrollo de Conceptos.

—. (2024). *Concepto Exploratorio. Mando y Control de las Operaciones Multidominio*. Madrid, Ministerio de Defensa, Centro Conjunto Desarrollo de Conceptos.

—. (2025). Plan del jefe de Estado Mayor de la Defensa para la implantación de las Operaciones Multidominio en las FAS. Madrid, Estado Mayor Conjunto de la Defensa.

España. (2007). Ley 39/2007, de 19 de diciembre, de la carrera militar [en línea]. Boletín Oficial del Estado. 20 de noviembre, núm. 278. [Consulta: 15 abril 2025]. Disponible en: https://www.boe.es/buscar/pdf/2007/BOE-A-2007-19880-consolidado.pdf

—. (2021). Real Decreto 1053/2021, de 30 de noviembre, por el que se aprueba el Reglamento de especialidades del segundo tramo de la carrera militar [en línea]. Boletín Oficial del Estado. 1 de diciembre, núm. 287, pp. 148171-148178. [Consulta: 19 abril 2025]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-19798

Frías Sánchez, C. (2023). ¿Un campo de batalla transparente? [en línea]. Ejército. N.º 987. [Consulta: 23 febrero 2025]. Disponible en: https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=341080

—. (2024). Inteligencia Artificial en el campo militar [en línea]. Global Affairs Journal. N.º 6. [Consulta: 23 febrero 2025]. Disponible en: https://www.unav.edu/documents/16800098/85691452/inteligencia-artificial-campo-militar.pdf

JEMAD. (2020). *Nota Conceptual Operaciones Multi-dominio*.

—. (2022a) Entorno Operativo 2035 1ª Rev. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/ENTORNO_OPERATIVO_2035_1_Rv.pdf.

—. (2023). Directiva 10/23 del jefe de Estado Mayor de la Defensa para la transición a la FOC del Sistema de Mando y Control Nacional (SC2N).

Martínez Leyva, J. L. (2022). Propuesta de arquitectura para la red táctica permanente multi-dominio JRE nacional [en línea]. Universidad de Vigo. [Consulta: 27 abril 2025]. Disponible en: https://calderon.cud.uvigo.es/server/api/core/bitstreams/7b81826b-87ab-4c3d-9c22-bcf2639c1a2f/content

Meddings, W. (2021). The Future of Command and Control: Four Models to Provoke Thought [en línea]. The Army Leader. [Consulta: 16 noviembre 2024]. Disponible en: https://thearmyleader.co.uk/future-of-command-and-control/#google_vignette

Meier, J. D. (2022). Two Ways to Lead: Detailed Command vs. Mission Command [en línea]. Sources of Insight. [Consulta: 17 abril 2025]. Disponible en: https://sourcesofinsight.com/detailed-command-vs-mission-command/#:~:text=Detailed%20Command%20is%20leading%20throughthe%20authority%20to%20take%20action

Ministerio de Defensa (2018). Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS). Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/p/l/plan_estrat_gico_de_los_sistemas_pecis_.pdf.

—. (2024a). Mando de Operaciones [en línea]. [Consulta: 30 enero 2025]. Disponible en: https://www.defensa.gob.es/ministerio/organigrama/emad/mops/

—. (2024b). Visión de la Inteligencia Artificial en las FAS.

—. (2024c). XXXI Curso Internacional de Defensa. Inteligencia artificial: oportunidades y desafíos para la seguridad y la defensa [en línea]. Ministerio de Defensa, Subsecretaría de Defensa, Secretaría General Técnica. [Consulta: 18 abril 2025]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/x/x/xxxi-curso-internacional-de-defensa.pdf

—. (2024d). *PDC-01(B). Doctrina para el Empleo de las Fuerzas Armadas*. Madrid, Ministerio de Defensa, Centro Conjunto Desarrollo de Conceptos.

—. (2025a). CESTIC. Funciones [en línea]. Ministerio de Defensa. [Consulta: 17 marzo 2025]. Disponible en: https://www.defensa.gob.es/cestic/mas/Mas_sobre_nosotros/

—. (2025b). Mando Conjunto del Ciberespacio [en línea]. EMAD. [Consulta: 18 abril 2025]. Disponible en: https://emad.defensa.gob.es/unidades/mcce/

Morón Ruiz, F. L. et al. (2023) Transformación digital de las FAS para el combate multidominio [en línea]. Ministerio de Defensa, Subsecretaría de Defensa, Secretaría General Técnica. [Consulta: 16 noviembre 2024]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/t/r/transformacion_digital_de_las_fas.pdf

Molero, F. y Moriano, J. A. (2020). Cómo preparar el liderazgo militar futuro [en línea]. Ministerio de Defensa, Instituto Español de Estudios Estratégicos. [Consulta: 13 marzo 2025]. Disponible en: https://publicaciones.defensa.gob.es/como-preparar-el-liderazgo-militar-futuro-libros-pdf.html

OTAN. (2023). Alliance Concept for Multi-Domain Operations.

Perkins W. y Olivieri A. (2018). Is NATO Today Sufficiently 'Joint' to Begin Discussions Regarding Multi-Domain Command and Control? [en línea]. The Journal of the Joint Air Power Competence Centre (JAPCC). Edición 26. [Consulta: 16 noviembre 2024]. Disponible en: https://www.japcc.org/articles/on-multi-domain-operations/

Ranstad. (2022). La redarquía, un nuevo modelo organizativo emergente [en línea]. Randstad. [Consulta: 15 marzo 2025]. Disponible en: https://www.randstad.es/contenidos360/cultura-empresarial/la-redarquia-un-nuevo-modelo-organizativo-emergente/

US Army. (2022). *FM 3-0 Operations*. US Department of the Army.

US DoD. (2020a). C3 Command, Control, and Communications. Modernization Strategy [en línea]. US Department of the Defense. [Consulta: 16 noviembre 2024]. Disponible en: https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf

—. (2022b). Summary of the Joint All-Domain Command and Control (JADC2) Strategy [en línea]. US Department of the Defense. [Consulta: 16 noviembre 2024]. Disponible en: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

Vega Bustelo, R. (2021). Liderazgo 2035, trabajo colaborativo y nuevas tecnologías [en línea]. Ejército. N.º 958. [Consulta: 24 marzo 2025]. Disponible en: https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=223786

Capítulo octavo

La inteligencia artificial en la toma de decisiones en el nivel operacional. Impacto en la confrontación y comparación de las líneas de acción

Jordi Francesc Rubio Carceller

Resumen

El trabajo analiza el impacto de la inteligencia artificial (IA) en la toma de decisiones en el nivel operacional, centrándose en dos fases críticas del planeamiento militar: la confrontación (*wargaming*) y la comparación de líneas de acción (COA). En un entorno caracterizado por la incertidumbre, la presión temporal y la complejidad multidominio, los métodos tradicionales presentan limitaciones en número de iteraciones, trazabilidad y consistencia analítica.

La investigación propone un modelo híbrido que integra IA con procedimientos doctrinales OTAN. En la fase de confrontación, se emplean técnicas basadas en teoría de juegos (minimax con poda alfa-beta) y medidas de efectividad (MoE), permitiendo analizar decenas de miles de combinaciones en tiempos reducidos, mejorar la objetividad y facilitar el refinamiento iterativo de las COA. En la fase de comparación, se combina IA con el método multicriterio Analytic Hierarchy Process (AHP), lo que permite estructurar la ponderación de criterios, reducir sesgos cognitivos y generar resultados trazables y justificables.

Los resultados evidencian mejoras significativas frente al método tradicional: reducción del tiempo de análisis, menor necesidad de personal y mayor consistencia en la aplicación de criterios. Además, la IA permite incrementar la calidad del análisis mediante iteraciones sucesivas y mejora la capacidad de explicación del proceso decisorio. No obstante, el estudio subraya que la IA no sustituye al comandante, sino que actúa como apoyo. Su valor reside en ampliar el espacio de análisis, reforzar la disciplina metodológica y mejorar la trazabilidad, siempre bajo control humano, con datos de calidad y alineación doctrinal, garantizando que la integración tecnológica no reemplace, sino complemente y fortalezca la autoridad decisoria del comandante en operaciones.

Palabras clave

Inteligencia artificial, Toma de decisiones operativas, Confrontación, Comparación, Sesgos humanos.

Artificial intelligence in decision-making at the operational level: Impact on the confrontation and comparison of courses of action.

Abstract

This study examines the impact of artificial intelligence (AI) on decision-making at the operational level, focusing on two critical phases of military planning: course of action (COA) wargaming and COA comparison. In an environment characterized by uncertainty, time pressure, and multidomain complexity, traditional methods exhibit structural limitations in terms of iteration capacity, traceability, and analytical consistency.

The research proposes a hybrid model that integrates AI with NATO doctrinal procedures. In the wargaming phase, techniques based on game theory (minimax with alpha-beta pruning) and measures of effectiveness (MoE) are employed, enabling the analysis of tens of thousands of combinations within reduced timeframes, enhancing objectivity, and supporting the iterative refinement of COAs. In the comparison phase, AI is combined with the multicriteria Analytic Hierarchy Process (AHP), allowing

for structured criteria weighting, the reduction of cognitive biases, and the generation of traceable and justifiable results.

The findings demonstrate significant improvements compared to the traditional approach, including reduced analysis time, lower personnel requirements, and greater consistency in the application of evaluation criteria. Furthermore, AI enhances analytical quality through successive iterations and improves the explainability of the decision-making process. However, the study emphasizes that AI does not replace the commander but rather acts as a decision-support tool. Its value lies in expanding the analytical space, reinforcing methodological rigor, and improving traceability, while ensuring human oversight, high-quality data, and doctrinal alignment. This guarantees that technological integration does not replace, but rather complements and strengthens, the commander's decision-making authority in operations.

Key words

Artificial intelligence, Operational decision-making, Confrontation, Comparison, Human bias.

1 Introducción

La toma de decisiones en el nivel operacional se desarrolla en un entorno caracterizado por la incertidumbre, la presión temporal y la interacción constante entre voluntades enfrentadas. El comandante y su Estado Mayor deben analizar grandes volúmenes de información, anticipar líneas de acción del adversario y seleccionar, en un plazo limitado, la alternativa que ofrezca mayores probabilidades de éxito para alcanzar el estado final deseado. Este proceso, tal como estructura la doctrina aliada para el planeamiento, exige convertir información fragmentaria en decisiones coherentes y oportunas (NSO, 2023).

Durante las últimas décadas, la complejidad del entorno operativo ha aumentado de forma significativa. La proliferación de dominios, la aceleración del ciclo de decisión y la disponibilidad de datos a diferentes niveles han incrementado la carga cognitiva de los órganos de planeamiento. Además, el Estado Mayor debe integrar variables militares, políticas, económicas, sociales y tecnológicas en un mismo marco de análisis, lo que dificulta construir una comprensión compartida del problema y mantenerla actualizada mientras la situación evoluciona.

En este escenario, la ventaja ya no depende únicamente de la superioridad material, sino de la capacidad para decidir con mayor rapidez y mejor fundamento que el adversario. La investigación aplicada en *wargaming* y apoyo a la decisión ha señalado que, bajo presión y con información incompleta, los equipos tienden a limitar el número de alternativas exploradas y a apoyarse en heurísticos o supuestos implícitos, lo que puede ocultar riesgos críticos (Tarraf *et al*., 2020). Esto afecta de forma directa a la calidad del planeamiento y al margen de adaptación del comandante.

La inteligencia artificial se ha consolidado como una tecnología de alto impacto para la defensa por su capacidad para procesar grandes volúmenes de datos, identificar patrones y apoyar tareas analíticas intensivas. En el nivel táctico, su incorporación es creciente en ámbitos como la sensorización, la logística o el mantenimiento predictivo. Sin embargo, su aplicación al nivel operacional plantea un reto distinto: no se trata solo de automatizar funciones, sino de reforzar la toma de decisiones en procesos donde la fricción, la ambigüedad y la interacción con un adversario adaptativo son determinantes. La literatura de seguridad nacional subraya precisamente el potencial de la IA como

apoyo al análisis y su impacto en la competencia entre actores, siempre que se preserve el control humano (Allen y Chan, 2017).

El planeamiento operacional dispone de procedimientos estructurados que permiten descomponer el problema, generar líneas de acción y evaluarlas antes de su selección. Dentro de este proceso, la confrontación y la comparación de líneas de acción constituyen fases particularmente sensibles. La confrontación (*wargaming*) introduce la lógica competitiva: evalúa cómo una línea de acción propia se comporta frente a reacciones plausibles del adversario y qué decisiones críticas emergen de esa interacción. La comparación, por su parte, sintetiza resultados y apoya la decisión del comandante al ponderar criterios como eficacia, riesgo, sostenibilidad o coherencia con la intención del mando (NSO, 2023).

No obstante, los métodos tradicionales empleados en estas fases presentan limitaciones estructurales. El *wargaming* consume tiempo y recursos, y su profundidad depende de la experiencia de los participantes y de su capacidad para manejar la complejidad del escenario. Los estudios sobre *wargaming* de nueva generación destacan que estas restricciones reducen el número de iteraciones practicables y dificultan capturar de forma sistemática resultados y supuestos, afectando a la trazabilidad y al aprendizaje posterior (Rasch *et al*., 2002). De forma complementaria, la comparación de líneas de acción puede verse condicionada por sesgos cognitivos y por la dificultad de mantener consistencia en la aplicación de criterios cuando el tiempo es limitado.

En este contexto, la inteligencia artificial ofrece la posibilidad de reforzar los procesos de confrontación y comparación ampliando el espacio de análisis sin sustituir al decisor humano. Modelos asistidos por IA permiten automatizar parte del procesamiento, explorar un mayor número de trayectorias de enfrentamiento, y documentar de manera estructurada decisiones, supuestos y resultados. La evidencia experimental en *wargaming* con plataformas habilitadas por IA muestra que estas herramientas pueden acelerar iteraciones y aportar consistencia en el análisis, siempre que el diseño del modelo y la calidad de los datos sean adecuados (Tarraf *et al*., 2020).

A la vez, la integración de la IA en la toma de decisiones operacionales exige prudencia. La dependencia de datos, la posible opacidad de ciertos modelos y la tentación de otorgar a los resultados una precisión superior a la real pueden generar una falsa sensación de certidumbre. Por ello, la IA debe concebirse como

apoyo a la decisión y no como sustituto del juicio del comandante; su función es ampliar la comprensión del problema y facilitar la evaluación de alternativas, preservando la responsabilidad y el control humanos (Garat, 2023).

Este trabajo aborda el impacto de la inteligencia artificial en la toma de decisiones operacionales, centrando el análisis en su aplicación a la confrontación y comparación de líneas de acción. A lo largo del documento, se presenta un modelo optimizado de confrontación y un modelo de comparación asistida, y se evalúa su utilidad a partir de su aplicación en un entorno de planeamiento realista. Para ello, se parte de procedimientos doctrinales y se introduce una formalización que permite comparar, de manera reproducible, el rendimiento del enfoque tradicional frente al asistido por IA en términos de tasas de éxito, tiempos de análisis y consistencia en la aplicación de criterios. La intención es que los resultados sean interpretables por el Estado Mayor y útiles para la decisión, no un ejercicio técnico aislado (Wong *et al*., 2019). El propósito es aportar un enfoque operativo y trazable que permita valorar, con rigor, cómo la IA puede complementar los métodos tradicionales y qué implicaciones se derivan para el comandante y su Estado Mayor.

2 La inteligencia artificial en la toma de decisiones operacionales

La inteligencia artificial se está incorporando al ámbito militar como una capacidad de apoyo a la decisión, no como un sustituto del mando. Su aportación más valiosa aparece cuando acelera el paso de información a conocimiento útil, ayuda a explorar más alternativas bajo presión de tiempo y deja un rastro trazable de supuestos, criterios y resultados. En el nivel operacional, donde la fricción y la incertidumbre son estructurales, esa trazabilidad importa tanto como la velocidad, porque permite revisar qué se asumió, qué se descartó y por qué, y facilita el aprendizaje en ciclos sucesivos.

El interés por la IA se entiende en tres planos complementarios. Primero, como factor de poder que influye en la competencia estratégica al modificar la capacidad de adaptación y el ritmo de decisión entre actores (Allen y Chan, 2017). Segundo, como habilitador del planeamiento aliado, al reforzar fases críticas del proceso doctrinal y sostener la coherencia en entornos conjuntos y multinacionales (NSO, 2023). Tercero, como respuesta a limi-

taciones recurrentes del enfoque tradicional, especialmente en número de iteraciones, consistencia del análisis y documentación de resultados para comparar alternativas con rigor (Wong *et al*., 2019).

2.1 Inteligencia artificial, poder militar y competencia estratégica

La inteligencia artificial se ha consolidado en los últimos años como una tecnología con un impacto creciente en el ámbito militar. Su capacidad para procesar grandes volúmenes de datos, identificar patrones complejos y apoyar procesos de análisis intensivos ha despertado un notable interés en relación con su posible aplicación a la toma de decisiones. En el nivel táctico y técnico, la incorporación de sistemas basados en inteligencia artificial es ya una realidad en ámbitos como la sensorización, la logística o el mantenimiento predictivo. Sin embargo, su aplicación en el nivel operacional, y en particular en los procesos de planeamiento y decisión, plantea retos conceptuales, doctrinales y organizativos que requieren un análisis específico (Wong *et al*., 2019).

La competencia por la IA se expresa en dos planos complementarios. El primero es el plano industrial y de conocimiento, donde el acceso a datos, talento y capacidad de cómputo condiciona la velocidad de desarrollo, entrenamiento y actualización de modelos (Farnell *et al*., 2024). El segundo es el plano doctrinal y organizativo, donde se decide cómo integrar esas capacidades en procesos reales de mando y control, evitando que la tecnología genere dependencias o falsas certezas. Se ha señalado que la IA tiene implicaciones directas para la seguridad nacional porque influye en la ventaja comparativa entre actores, en su capacidad de adaptación y en su margen para gestionar crisis, al tiempo que introduce nuevas superficies de riesgo (Allen y Chan, 2017).

Desde la perspectiva militar, la IA puede aportar ventajas en cuatro ejes. El primero es la velocidad de procesamiento de información y la reducción de carga cognitiva del Estado Mayor, especialmente cuando coexisten múltiples fuentes y formatos (Scott y Michell, 2023). El segundo es la capacidad de identificar patrones y tendencias en conjuntos de datos heterogéneos, apoyando la comprensión situacional y la detección de cambios relevantes (Carrasco, 2024). El tercero es la generación y evaluación rápida de alternativas, que permite ampliar el espacio de decisión y explorar trayectorias de enfrentamiento que el tiempo impide

considerar con métodos manuales. El cuarto es la trazabilidad: al registrar supuestos, criterios y resultados, se facilita la revisión posterior, el aprendizaje y la mejora del proceso decisorio (Ouyang *et al*., 2022).

Ahora bien, convertir potencial tecnológico en poder militar exige vencer fricciones internas. La introducción de IA en organizaciones complejas obliga a definir quién valida los modelos, cómo se gobiernan los datos, qué sesgos se aceptan y cuáles se mitigan, y cómo se preserva el control humano sobre decisiones críticas. El valor estratégico de la IA puede degradarse si se usa sin comprensión de sus límites o si se aplica de forma superficial como mera automatización de productos. Se ha señalado que, incluso cuando la IA apoya tareas concretas, su utilidad depende de la calidad de los datos, de la claridad de los objetivos de empleo y de la capacidad del usuario para interpretar resultados sin convertirlos en dogmas (Bender *et al*., 2021).

En el nivel operacional, estas consideraciones son especialmente relevantes porque el planeamiento integra incertidumbre, adversarios adaptativos y restricciones políticas. Se ha señalado que la IA, aplicada al arte operacional, puede actuar como catalizador de cambios en la forma de planear y conducir operaciones, pero su contribución real depende de cómo se traduzca en procesos de decisión concretos y de cómo se integre en la cultura del Estado Mayor (Garat, 2023). En consecuencia, la relación entre IA, poder militar y competencia estratégica no se reduce a la adquisición de sistemas, sino a la capacidad de convertirlos en ventajas de decisión sostenidas.

En este marco, una organización que consigue analizar con mayor profundidad en el mismo tiempo, o mantener consistencia en sus criterios bajo presión, obtiene una ventaja operativa incluso sin cambios en el orden de batalla. La ventaja se amplifica cuando la organización aprende: la trazabilidad permite identificar qué supuestos fallaron, qué criterios pesaron de forma indebida y qué señales fueron interpretadas de manera errónea. Esa capacidad de aprendizaje acelerado es, en sí misma, un componente de poder militar, porque reduce la probabilidad de repetir errores y aumenta la adaptabilidad en ciclos sucesivos.

A la vez, la IA introduce vulnerabilidades estratégicas. Si el adversario puede degradar datos, manipular señales, inducir patrones falsos o explotar dependencias del modelo, la ventaja puede invertirse. Además, la presión por decidir más rápido puede llevar

a aceptar resultados opacos sin el contraste necesario. Por ello, la IA debe concebirse como apoyo a la decisión y no como sustituto del juicio del comandante; su función es ampliar la comprensión del problema y facilitar la evaluación de alternativas, preservando la responsabilidad y el control humanos (Garat, 2023).

Además, el valor estratégico de la IA se incrementa cuando se considera el carácter conjunto y, con frecuencia, multinacional de las operaciones. En un entorno aliado, el planeamiento requiere un lenguaje común, criterios compartidos y procedimientos estandarizados para que la evaluación de alternativas sea comparable y comprensible entre componentes. La doctrina aliada proporciona ese marco, pero la incorporación de herramientas de IA obliga a asegurar que los modelos respeten supuestos doctrinales, que los resultados sean comunicables y que el proceso conserve coherencia entre escalones y cuarteles generales (NSO, 2023). En términos prácticos, una misma herramienta puede generar valor solo si sus productos son aceptados, interpretados y utilizados de forma consistente por un equipo multinacional.

En este punto, la IA puede aportar una ventaja adicional: ampliar el número de iteraciones de análisis sin incrementar de forma proporcional el tiempo del Estado Mayor (Palantir, 2025). La investigación sobre *wargaming* recomienda superar enfoques excesivamente manuales y avanzar hacia métodos que permitan explorar más opciones, registrar supuestos y comparar resultados con mayor rigor (NATO, 2022). En la medida en que un adversario sea capaz de ejecutar ciclos de análisis y adaptación más rápidos, la competencia estratégica tenderá a premiar a quien logre sostener ese ritmo sin degradar la calidad del juicio. Por eso, la IA debe evaluarse no solo por su rendimiento técnico, sino por su contribución a procesos decisorios repetibles, auditables y útiles.

Por último, la competencia estratégica también se juega en la confianza institucional. La IA puede reforzar el mando si aporta claridad, coherencia y trazabilidad, pero puede erosionarlo si introduce opacidad o si desplaza la responsabilidad sin control. En seguridad nacional, el reto no es únicamente desarrollar capacidades, sino gobernarlas y emplearlas de modo que aumenten la ventaja y reduzcan riesgos (Allen y Chan, 2017). En la práctica operacional, esto exige que el comandante entienda qué asume el modelo, qué no puede ver y qué incertidumbre permanece. Solo así la IA se convierte en poder militar real y sostenible (Scharre, 2023). Ese equilibrio entre velocidad, transparencia y

control humano define la diferencia entre una ventaja decisiva y una dependencia operativa vulnerable potencial.

2.2 Impacto de la inteligencia artificial en el planeamiento operacional OTAN

El planeamiento operacional en el marco OTAN se apoya en un proceso estructurado que permite transformar una situación compleja en una línea de acción coherente, coordinada y justificable. La COPD describe un enfoque que combina análisis, generación de alternativas, confrontación y comparación antes de la decisión del comandante, y que exige coherencia entre supuestos, criterios y productos del Estado Mayor (Kwok y Lim, 2011). Sobre esa arquitectura, la IA puede introducir mejoras relevantes si se integra como apoyo al trabajo del Estado Mayor y no como sustituto del juicio.

El primer impacto potencial aparece en la fase de comprensión del problema. El planeamiento operacional exige construir una apreciación compartida del entorno, identificar factores decisivos y actualizar la comprensión a medida que cambia la situación. Herramientas de IA pueden apoyar la fusión de información procedente de fuentes heterogéneas, resaltar patrones o anomalías y ayudar a priorizar qué información es operativamente relevante. En un entorno con gran volumen de datos, esta capacidad puede reducir la carga cognitiva y mejorar la velocidad con la que el Estado Mayor pasa de la información al conocimiento útil (Ruiz, 2021).

El segundo impacto se relaciona con la generación de líneas de acción. En la práctica, el tiempo y los recursos limitan el número de alternativas que el Estado Mayor puede desarrollar y refinar. La IA puede apoyar la exploración de un conjunto mayor de variantes, ayudando a identificar combinaciones de acciones, secuencias y medidas de coordinación que cumplan restricciones y aprovechen oportunidades. Este apoyo no elimina la necesidad de creatividad y juicio, pero puede servir como mecanismo para ampliar el espacio de búsqueda y evitar que el proceso se ancle demasiado pronto en una opción preferida.

El tercer impacto, especialmente relevante, se sitúa en la confrontación. La COPD incorpora el *wargaming* como mecanismo para evaluar la interacción con el adversario y detectar riesgos, decisiones críticas y puntos de fricción (Tinnirello, 2018).

Sin embargo, la investigación sobre *wargaming* destaca que los enfoques tradicionales consumen tiempo, dependen de la experiencia de los participantes y tienden a limitar el número de iteraciones posibles (NATO, 2022). La IA puede complementar este proceso ejecutando iteraciones adicionales bajo supuestos explícitos, registrando resultados y facilitando comparaciones entre trayectorias de enfrentamiento. Se ha señalado que plataformas habilitadas por IA pueden acelerar la exploración de opciones en contextos tácticos, una lógica que, adaptada con cautela, resulta valiosa para el nivel operacional en términos de consistencia y trazabilidad (Tarraf *et al*., 2020).

El cuarto impacto se aprecia en la comparación de líneas de acción y en la síntesis para la decisión. La doctrina OTAN exige que el Estado Mayor presente recomendaciones basadas en criterios y en una valoración clara de riesgos, ventajas y costes (DOPE, 2024a). Herramientas de IA pueden ayudar a mantener consistencia en la aplicación de criterios, a documentar cómo se ponderan factores bajo presión y a producir representaciones comparables para el comandante. De este modo, el producto final no es solo más rápido, sino más explicable.

Ahora bien, el impacto positivo depende de condiciones de integración. En primer lugar, los modelos deben alinearse con el marco doctrinal para que sus resultados sean interpretables por equipos conjuntos y multinacionales; en un cuartel general aliado, la confianza se construye con transparencia sobre supuestos y limitaciones. En segundo lugar, la gobernanza de datos y la ciberresiliencia son críticas: el planeamiento es tan fiable como la información que alimenta los modelos, y un adversario buscará degradar o manipular señales. En tercer lugar, el control humano debe permanecer explícito: la IA debe apoyar el juicio, no desplazarlo, y el comandante debe poder aceptar, modificar o rechazar recomendaciones con fundamento (Farnell *et al.*, 2024).

En suma, la IA puede impactar el planeamiento operacional OTAN allí donde el proceso es más sensible a tiempo, complejidad y consistencia: comprensión situacional, generación de alternativas, confrontación y comparación. Su integración debe centrarse en reforzar productos del Estado Mayor, mejorar la trazabilidad y ampliar el análisis dentro del marco doctrinal, manteniendo la responsabilidad y el control humanos como requisitos inalterables (Bossio, 2023).

Desde el punto de vista organizativo, integrar IA en un Cuartel General implica ajustar rutinas de trabajo y responsabilidades. Para que un producto asistido por IA sea útil, debe existir un flujo claro de preparación de datos, parametrización de supuestos, revisión de resultados y comunicación al decisor. Esto requiere formación específica para que el personal comprenda qué hace el modelo, qué no hace y qué incertidumbres permanece. También exige procedimientos de validación y control de calidad, de modo que los resultados sean reproducibles y coherentes entre turnos y secciones. La literatura sobre *wargaming* subraya que la utilidad crece cuando se registran supuestos y se normaliza el formato de resultados, facilitando comparación y aprendizaje (US Army, 2023). En el ámbito operacional, se ha señalado que la transformación no es meramente técnica, sino cultural: incorporar IA significa reforzar la disciplina analítica del Estado Mayor y mejorar su capacidad de adaptación bajo presión (Goecks y Waytewich, 2022). Cuando estas condiciones se cumplen, la IA actúa como multiplicador de análisis y no como autoridad.

3 Impacto de la IA en la confrontación

La confrontación de líneas de acción es el momento en que el planeamiento deja de ser una lista de tareas y pasa a modelar la interacción con un adversario que aprende (Araya y King, 2022). En la práctica, el *wargaming* permite anticipar reacciones, detectar decisiones críticas y estimar riesgos operacionales conjuntos, pero sufre limitaciones de tiempo, de recursos y de consistencia cuando el escenario es complejo y el ciclo de decisión se acelera (Ministerio de Defensa, 2023). La inteligencia artificial puede ampliar el número de iteraciones, mantener supuestos explícitos y registrar resultados de manera trazable, siempre bajo control humano. El valor no está en «adivinar» el futuro, sino en mejorar la calidad del juicio del Estado Mayor.

3.1 El rol de la IA en la confrontación

La confrontación o «Wargaming» en el planeamiento operacional representa un proceso en el que se enfrentan las COA propias con las del oponente (OCOA). La secuencia en la confrontación consiste en simular secuencialmente, en tres turnos, la interacción entre las fuerzas propias y enemigas: en el primer turno, las fuerzas propias ejecutan una acción operacional; en el segundo,

el adversario reacciona conforme a su OCOA y, en el tercer turno, las fuerzas propias desarrollan una contra reacción. Este ciclo permite evaluar la solidez de cada COA ante respuestas adversarias y afinar su diseño antes de su selección final (Wong *et al*., 2019).

Tradicionalmente, esta confrontación está marcada por un alto sesgo personal. Los modelos de *wargaming* manuales están principalmente basados en los conocimientos, experiencia y juicio de los analistas y comandantes. Este proceso se considera vulnerable cuando el analista aun teniendo un conocimiento y juicio óptimo, carece de experiencia suficiente para afrontar el proceso de confrontación con garantías. Esta situación provoca que el proceso se vuelva aún más vulnerable a la subjetividad, lo que puede llevar a decisiones no óptimas y a un planeamiento menos efectivo (Tarraf *et al*., 2020).

En estos casos, la IA emerge como una herramienta clave para reducir esta subjetividad. Esta tecnología permite rellenar el vacío de la inexperiencia, proporcionando unos análisis rigurosos basados en grandes volúmenes de datos y modelos de predicción. Mediante el uso de algoritmos avanzados y datos verificables, la IA puede ayudar a estructurar el proceso de toma de decisiones en general, y de la confrontación en particular (Russell y Norvig, 2020). De este modo, la tecnología no solo optimiza la confrontación de COA, sino que también actúa como un multiplicador del conocimiento, nivelando el desempeño de los analistas y minimizando el impacto negativo de la falta de experiencia.

La IA ayudará a gestionar la falta de tiempo y el análisis de grandes volúmenes de datos. Los analistas como parte del planeamiento de operaciones, están sometidos a un estrés de tiempo significativo. Estas limitaciones de tiempo pueden dificultar el desarrollo y la selección de una decisión óptima. Además, debe gestionar una gran carga de información, no solo propia sino también del adversario y otros actores del entorno, así como otros factores (Coomber, 2009). En este contexto, la IA ofrece una alta capacidad de procesar grandes cantidades de información en segundos. Esto no solo optimiza la toma de decisiones bajo presión, sino que también reduce la posibilidad de errores humanos y sesgos, permitiendo una evaluación más precisa y fundamentada.

En el siguiente epígrafe, se llevará a cabo el estudio desarrollado de la confrontación de COA empleando IA. La investigación se ha desarrollado bajo la ambientación del ejercicio de alta inten-

sidad Constellatia, parte del Curso de Estado Mayor de las FAS españolas (CEMFAS) (DOPE, 2024b). Para tratar de demostrar la objetividad empírica del resultado, se ha adoptado un enfoque basado en la teoría de los juegos, utilizando el algoritmo Minimax con poda Alfa-Beta (Gómez, 2016). Mediante este enfoque, se analizará en qué medida la IA puede mejorar la confrontación de COA, evaluando su impacto en la precisión, la rapidez del análisis y la optimización de los recursos humanos.

Para la investigación se tomarán las COA y OCOA desarrolladas por cinco grupos de trabajo del CEMFAS. Dichas COA serán enfrentadas con la línea de acción del oponente más peligrosa (MDOCOA) y la línea de acción del oponente más probable (MLOCOA), con el objetivo de identificar no solo la viabilidad táctica y estratégica de cada opción, sino también los riesgos, limitaciones y oportunidades que surgen en el proceso (US Army, 2023). En el último epígrafe del capítulo, se desarrollarán los resultados de ambos métodos (tradicional e IA) así como su comparación.

Se analizará también cómo la IA influye en la gestión del tiempo y la optimización de la carga de trabajo. En este sentido, se estudiará la implicación en la carga hombre-hora, así como el personal necesario para realizar el *wargame*. Para ello, se tomará como punto de referencia de inicio de cálculo de tiempos la finalización del desarrollo de las COA. Con respecto a la posible optimización de la carga de trabajo hombre-hora, se han tomado como participantes los veintiséis miembros del curso de Estado Mayor que formaban parte de los JOPG, ya que estos forman parte del *wargame* como miembros en alguna de las células (Red, Blue, Green, White, registradores o personal de apoyo) (Zhang, Liu y Yuan, 2024).

La aplicación de la IA en la confrontación de las líneas de acción a nivel operacional sigue en desarrollo (Knack y Powell, 2023). A pesar de las inversiones billonarias en el impulso de la inteligencia artificial (Comisión Europea, 2025) su tecnología no se ha integrado en la etapa de análisis de este capítulo. Hasta la fecha del fin del marco temporal (31 diciembre 2024), los esfuerzos se han centrado en la automatización de tareas logísticas, el análisis de inteligencia y la mejora de la toma de decisiones tácticas (Palantir, 2024). A continuación, se detallará el proceso de confrontación empleando la IA describiendo la metodología empleada y el desarrollo de cada fase.

3.2 Confrontación optimizada con IA

El avance de la tecnología ha permitido el desarrollo de sistemas de simulación y apoyo a la decisión que integran modelos de IA de última generación (Vestner, 2023). La herramienta empleada en esta investigación combina procesamiento de lenguaje natural y algoritmos de optimización para generar, confrontar y refinar líneas de acción (COA) en tiempo casi real, lo que reduce tiempos de análisis y facilita iteraciones sucesivas (Chance *et al*., 2023). Su arquitectura se orienta a asistir al comandante en la confrontación de COA integrando información doctrinal, histórica y operacional en un proceso iterativo de optimización.

El modelo se entrena con información general y se especializa mediante fine-tuning con documentos doctrinales, informes militares y escenarios históricos de *wargaming*. Así incorpora terminología y lógicas propias del planeamiento, pudiendo generar opciones coherentes para fuerzas propias y anticipar reacciones enemigas (Brown *et al*., 2020). La doctrina también se integra mediante aprendizaje en contexto: a partir de la información proporcionada por el analista, el modelo ajusta su evaluación a los supuestos, restricciones y guías facilitadas, comportándose como un GPT (transformador generativo preentrenado) adaptado a operaciones militares (Goecks y Waytowich, 2024).

Este diseño permite que sus respuestas no dependan de reglas fijas, sino del reconocimiento de patrones extraídos de casos previos y de la lógica doctrinal. Además, destaca la velocidad de procesamiento y la capacidad de adaptación para reevaluar confrontaciones con retroalimentación del analista o cambios en los supuestos (Goecks *et al*., 2023).

Esta tecnología puede analizar escenarios, documentación e interpretar COA/OCOA para aplicarlas a la confrontación. Estudios recientes señalan que los grandes modelos de lenguaje pueden aproximar procesos de toma de decisiones humanas en conflictos simulados (Roberts *et al*., 2024), lo que posibilita evaluar dinámicamente una COA propia frente a una opción del adversario (OCOA) en un entorno simulado de texto e imágenes e identificar desenlaces plausibles (US Army War College, 2023). El valor práctico radica en generar confrontaciones en segundos y ajustar la evaluación de forma ágil, de manera que, si el comandante introduce cambios o directrices adicionales, el sistema pueda

recalcular de inmediato el enfrentamiento y actualizar el apoyo a la decisión (Goecks *et al*., 2023).

El método se articula en un ciclo iterativo de cuatro fases: conocimiento, análisis, refinamiento y resultados (figura 1). En la fase de conocimiento, se alimenta a la IA con productos del planeamiento. Como mínimo se introducen el CUOE completo, la directiva de Planeamiento Estratégico (SPD), el diseño operacional y el diseño de la maniobra de las COA. Además, se asignan medidas de efectividad (MoE) a cada efecto mediante indicadores que cuantifican el éxito esperado (Richardson, 2004). Esta entrada es decisiva porque proporciona una base sólida sobre la que construir un análisis consistente y reutilizable en iteraciones posteriores.



Figura 1. Fases ciclo confrontación optimizada con IA (Fuente: Elaboración propia)

En la siguiente fase, de análisis, la IA evalúa alternativas de enfrentamiento adaptando el *wargame* secuencial tradicional a tres niveles: acción propia (turno 1), reacción adversaria más probable y más peligrosa (turno 2) y contrarreacción propia (turno 3). Esta secuencia acción-reacción-contrarreacción recoge el núcleo doctrinal del *wargaming* aliado (NSO, 2019). A diferencia del método tradicional, en el que las acciones y reacciones se deliberan por el grupo de planeamiento (UK MoD, 2021), aquí la IA puede proponer opciones para ambos bandos con base en patrones doctrinales, datos históricos e inteligencia contextual (HQ DoA, 2019). En consecuencia, el sistema no solo evalúa

decisiones humanas: puede generar nuevas opciones operativas y contrastarlas, apoyándose en principios doctrinales y una lógica empírica (Coutts *et al*., 2022).

El enfoque admite variaciones respecto al *wargaming* clásico. Puede invertirse la secuencia e iniciar el turno 1 con una acción del adversario, lo que resulta valioso en operaciones no cinéticas, en misiones de mantenimiento de la paz o cuando fuerzas propias se hallan en defensiva y el adversario conserva la iniciativa. Además, el procesamiento permite alargar la confrontación más allá de tres turnos. Complementariamente, la IA puede generar árboles de decisión de ramas dinámicas, lo que facilita considerar un número elevado de resultados potenciales, evaluar alternativas de forma más exhaustiva y determinar combinaciones con mayor probabilidad de éxito (NATO STO, 2022).

La investigación aplica la confrontación por Condiciones Decisivas (DC), como ejemplifica la figura 2. La IA construye un árbol de decisión apoyándose en teoría de juegos (ITNL, 2005) y en la lógica doctrinal. En los turnos secuenciales los jugadores conocen lo ocurrido y la posición en el árbol, lo que se formaliza como información perfecta (Sokri, 2022). Esta estructura permite explorar combinaciones masivas: en el caso práctico, una DC generó 71 760 combinaciones y, al iterar sobre varias DC, el volumen total asciende a cientos de miles. Para gestionar la complejidad, el sistema optimiza mediante poda alfa-beta, descartando ramas con baja aportación decisional y concentrando el análisis en trayectorias más prometedoras (Quevedo y Quevedo, 2021).

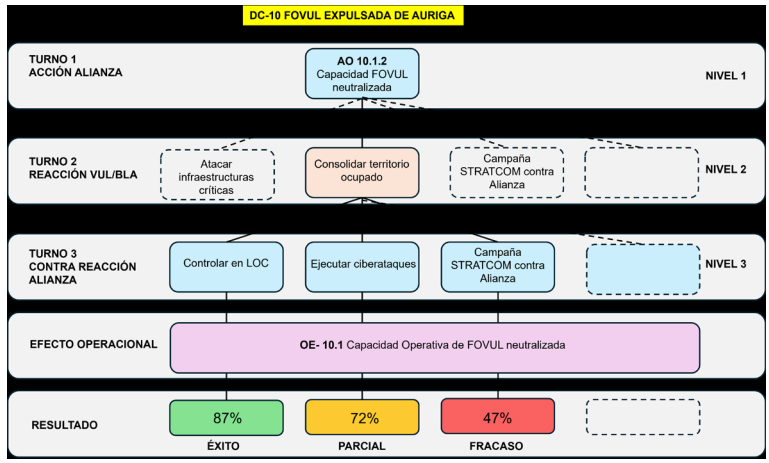


Figura 2. Esquema método optimizado IA. Fuente: elaboración propia

Cada combinación se evalúa por sus efectos sobre el entorno operacional. Para cada secuencia, la IA asigna un valor porcentual según los MoE y clasifica el resultado como éxito, éxito parcial o fracaso; corresponde al comandante fijar umbrales de aceptabilidad conforme al riesgo asumible y criterios doctrinales (UK MoD, 2021). El sistema representa capacidades, requisitos y vulnerabilidades, pondera actitudes y propósitos y valora acciones (Dupuy, 1979). Por ejemplo, si la actitud del adversario es defender «a toda costa» una zona ocupada, el valor de acciones orientadas a defensa de zona o protección de instalaciones puede incrementarse un 20 % para reflejar esa prioridad (Lawrence, 2017). Además, se introduce el desgaste: cada empleo de una capacidad reduce proporcionalmente su tasa de éxito posterior, modelando la degradación progresiva.

La fortaleza del enfoque iterativo reside en el ajuste dinámico de estrategias. Tras la evaluación inicial, el sistema produce un informe con porcentajes de éxito por DC; si una acción supera el 85 % se considera exitosa, entre 60 % y 85 % parcialmente exitosa y por debajo del 60 % fracaso. Esa clasificación activa el refinamiento, con interacción entre usuario e IA para modificar supuestos, sincronización, recursos y guías del comandante. El esquema es aplicable tanto al planeamiento como a la conducción de operaciones, permitiendo ajustar planes conforme evoluciona la situación (De Rosa, 2022). En esa interacción se busca sinergia entre el arte operacional del usuario y la evaluación cuantitativa del sistema, facilitando la identificación de mejoras y recomendaciones específicas.

En la fase final, se presentan resultados del análisis y del refinamiento como conclusiones, observaciones y sugerencias para perfeccionar alternativas (Ruestchmann, 2022). Se determinan necesidades adicionales de capacidades o fuerzas y sincronización imprescindible, se analizan riesgos y oportunidades frente a cada OCOA y se derivan ramas y secuelas, puntos de decisión respaldados por CCIR y ajustes de misiones a mandos componentes (DOPE, 2024a). En conjunto, la integración de IA se plantea como un cambio relevante: reduce parte de la subjetividad y del tiempo del análisis manual (Alberts y Hayes, 2007) y apoya una asignación más eficiente de recursos mediante iteraciones rápidas basadas en evidencia empírica (Palantir, 2025). Finalmente, los productos generados se comparan con los resultados obtenidos por los JOPG del CEMFAS durante el ejercicio Constellatia para validar si el enfoque asistido por IA reduce tiempos, mejora

la calidad y aumenta la objetividad del proceso, frente al método tradicional (Swedint, 2016).

3.2.1 Caso práctico confrontación con IA

En este epígrafe, se aplica de manera práctica la IA a la etapa de confrontación dentro del planeamiento operacional, usando como ambientación el ejercicio de alta intensidad Constellatia desarrollado en el CEMFAS (Ritter, 2018). El caso busca mostrar cómo un sistema de IA puede apoyar el *wargaming* en la confrontación COA vs. OCOA, qué entradas documentales requiere, qué productos analíticos genera y cómo facilita el refinamiento iterativo de una línea de acción. Para ello, se emplean documentos generados por uno de los grupos de planeamiento (JPOG) y la investigación se centra en dos COA, denominadas CEPO y APOCALIPSIS, enfrentadas a la MDOCOA.

La confrontación se ejecuta mediante el método por condiciones decisivas, que descompone el problema operacional en hitos críticos y permite evaluar de forma estructurada el avance hacia los objetivos. Aunque el estudio completo consideró varias condiciones decisivas, aquí se representan los resultados sobre una: la condición decisiva 10 (DC-10), «Expulsión de FOVUL de Auriga». El caso práctico se desarrolla siguiendo un ciclo de interacción entre un analista y la IA, que comprende: contextualización y carga documental, verificación de supuestos, análisis por turnos (acción-reacción-contra reacción) y, si procede, refinamiento iterativo.

El primer paso consiste en contextualizar el sistema. El usuario describe el escenario, el rol analítico que debe adoptar la IA y las tareas a desarrollar. Para dotar de base documental al análisis, el analista introduce un conjunto de documentos estructurados esenciales: el CUOE completo, el Strategic Warning Order (SWO), el SACEUR Strategic Assessment (SSA), la Guía de Planeamiento del comandante (CPG) y la SPD. A esa base se añade el diseño operacional, que integra objetivos operacionales, condiciones decisivas, efectos y acciones, junto con la organización operativa y el esquema de maniobra de ambas COA. La finalidad de esta fase no es únicamente «alimentar» el modelo, sino delimitar con precisión el marco de decisiones y las restricciones operacionales que condicionan la confrontación.

Con la base establecida, la fase de análisis inicia con la descripción de la DC-10. La situación se formula en formato narrativo,

explicitando qué acciones ejecutará la Alianza, qué efectos se buscan con cada acción y qué Medidas de Efectividad (MoE) permitirán valorar el logro de esos efectos. En paralelo, se describen las acciones probables del adversario según capacidades y objetivos de su OCOA (Nonnenmacher, 2004). Además, se permite que la IA proponga acciones adicionales del adversario cuando detecta alternativas plausibles no contempladas, siempre dentro de los límites del escenario y de la lógica de capacidades. Esta combinación de «entrada guiada» y «exploración asistida» persigue ampliar el espacio de opciones sin perder control sobre la validez del modelo.

Una vez validada y aclarada la información, se inicia el núcleo del *wargaming*: la secuencia acción-reacción-contrareacción. En el caso analizado, el turno 1 contempla veintitrés acciones aliadas; el turno 2 define veinte reacciones adversarias posibles para cada acción y el turno 3 reúne 156 opciones de contra reacción de la Alianza. Este diseño produce un espacio teórico de más de 71 000 combinaciones. Explorar exhaustivamente ese espacio de forma manual sería inviable; por ello, el sistema aplica un enfoque de teoría de juegos mediante el algoritmo minimax, combinado con poda alfa-beta, para descartar ramas con resultados inferiores y concentrar el análisis en alternativas con mayor potencial (Krivokuća, 2019). El efecto práctico es reducir el esfuerzo computacional y, al mismo tiempo, mantener una lógica de decisión consistente con la competencia entre voluntades.

El output principal se entrega como una tabla exportable (.csv) que recoge probabilidades de éxito de acciones concretas y de secuencias, facilitando trazabilidad y posterior explotación (figura 3). Tras la poda, el caso de la DC-10 confrontando CEPO frente a la MDOCOA sintetiza las 71 760 combinaciones teóricas en una tabla de 2380 filas, agrupando las alternativas más relevantes para la decisión (Berwick, 2011). La tabla no solo resume resultados, sino que permite identificar qué acciones tienden a sostenerse ante reacciones específicas y qué contra reacciones son más eficaces para recuperar iniciativa.

Junto con el producto proporcionado, la IA entrega un comentario analítico en lenguaje natural que describe los principales riesgos y oportunidades operacionales que pueden emerger, y señala dónde la secuencia tiende a degradarse (por ejemplo, puntos de ruptura logísticos o ventanas de vulnerabilidad). La IA acompaña también la tabla con recomendaciones operacionales: informa de probabilidades de éxito asociadas a cada acción, propone una

Acción - Alianza (CEPO)	Reacción - MDOCOA	Contra Reaccón - Alianza (CEPO)	MoE (%)	Resultado
Limpiar el Área ocupada por la FOVUL	Mantener Áreas de denegación	Auditar y bastionar sistemas CIS control IC	65	Parcial
			44	
Atacar posiciones defensivas de FOVUL	Lanzar campañas de STRATCOM	Destruir aeronaves con capacidad AAR VUL	48	Fracaso
			90	
Inutilizar CIAP	Mantener Áreas de denegación	Destruir unidades logísticas de FOVUL	76	Parcial
			96	

Figura 3. Muestra de la tabla de presentación de resultados. Fuente: elaboración propia con datos de la IA)

secuencia óptima a seguir y señala cuáles no alcanzan un umbral mínimo de éxito fijado por el analista (por ejemplo, 85 %). En ese punto, el analista decide el siguiente paso: si considera suficiente la tasa de éxito, puede dar por concluida la confrontación y pasar a otra condición decisiva; si desea mejorar el desempeño, activa la fase de refinamiento iterativo (Soler, 2024).

El refinamiento funciona como un bucle: el usuario examina resultados iniciales, introduce ajustes o nuevas hipótesis operacionales (cambios en sincronización, reasignación de recursos, variación de secuencias, incorporación de apoyos) y la IA reprocesa el problema adaptando el análisis hasta proponer un modelo optimizado más ajustado al entorno.

La evaluación de cada iteración se hace con una tasa de éxito ponderada construida a partir de las MoE. La ponderación se realiza con criterios objetivos definidos para cada efecto deseado, de modo que la evaluación agregue resultados parciales sin perder trazabilidad sobre qué efectos y acciones impulsan el desempeño. Una función adicional del sistema es mostrar la evolución de la tasa de éxito iteración tras iteración, lo que facilita valorar el impacto de cada cambio, detectar estancamientos y decidir si conviene redefinir hipótesis o insistir en la misma línea de ajustes. Así, la confrontación deja de ser una «fotografía» y pasa a ser un proceso de mejora controlada.

La evolución de CEPO en la DC-10 ejemplifica el proceso (figura 4). La evaluación inicial presenta un desempeño moderado: éxito medio del 40 %, éxito parcial del 35 % y fracaso del 25 %. La IA vincula parte de ese rendimiento a dificultades de ejecución por interrupción de líneas logísticas por parte de la OCOA y a una capacidad de adaptación limitada frente a reacciones enemigas. Tras aplicar modificaciones sugeridas, la primera iteración incrementa el éxito al 55 %, reduce el éxito parcial al 30 % y baja el fracaso al 15 %. Aun con la mejora, el diagnóstico sugiere que persisten vulnerabilidades en la fase de consolidación de objetivos, lo que exige ajustes adicionales orientados a sostener los efectos conseguidos y no solo a alcanzar el objetivo inmediato.

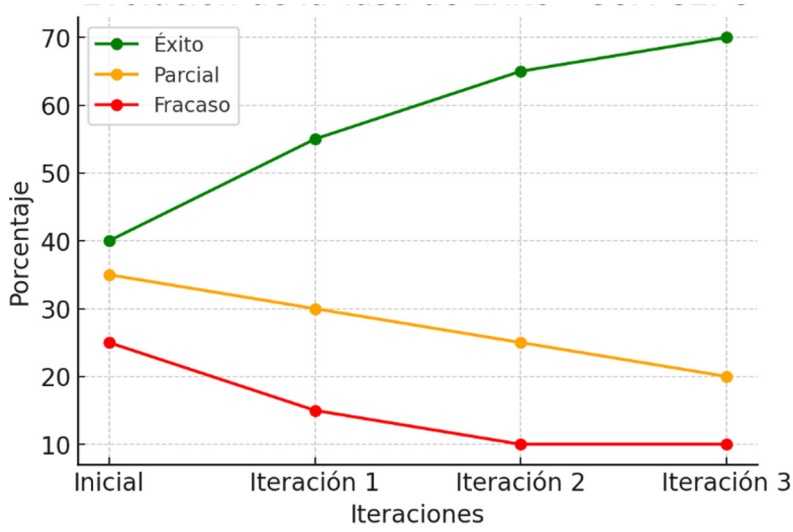


Figura 4. Evolución de la Tasa de éxito de DC-10 COA CEPO. Fuente: elaboración propia con datos de IA

La segunda optimización se centra en mejorar sincronización y consolidación de operaciones. Para reducir tiempos de respuesta ante contraofensivas, la IA recomienda incrementar la sincronización entre maniobras ofensivas y defensivas, buscando una mejor alineación entre el ataque sobre el adversario y la consolidación del terreno. Este ajuste pretende cerrar ventanas de vulnerabilidad en la transición entre fases y facilitar respuestas más rápidas a contraataques. Además, propone reforzar operaciones en profundidad mediante ataques de precisión y acciones que degraden la estructura de mando adversaria, reduciendo su capacidad de reconstitución. De manera complementaria, se sugiere

acompañar el esfuerzo cinético con INFOOPS y STRATCOM para contrarrestar desinformación, erosionar la cohesión y afectar la capacidad de movilización y respuesta del adversario (IEEE, 2020). En conjunto, estas modificaciones buscan mejorar progresivamente el desempeño, coherente con la lógica de iteración y optimización propia de enfoques basados en teoría de juegos.

El ciclo de mejora se repite hasta que el analista considera alcanzada una tasa de éxito suficiente. Completado el proceso, se pasa a la fase de validación y extracción de conclusiones. En esta etapa, se presentan resultados definitivos con puntuaciones basadas en MoE, visualizaciones que reflejan tendencias y conclusiones derivadas del proceso, ya sea por COA o en formato comparativo (Khimeche y De Champs, 2004). Además, el sistema puede ofrecer una primera comparación de cómo se comportan las COA frente a distintas OCOA, lo que amplía el valor del análisis más allá de un único enfrentamiento y favorece el contraste temprano entre alternativas (Lamparth *et al*., 2024). La salida final, por tanto, no es solo un listado de acciones, sino una combinación de evidencia cuantificada y razonamiento estructurado sobre riesgos, oportunidades y secuencias preferibles.

En conjunto, el caso práctico pretende demostrar empíricamente que integrar IA en la confrontación COA vs. OCOA optimiza la toma de decisiones al combinar inteligencia artificial, MoE y teoría de juegos. El enfoque tiende a mejorar precisión y objetividad al desplazar parte de la valoración hacia métricas definidas ex ante y ponderadas de manera trazable. Desde el punto de vista técnico, el uso de minimax con poda alfa-beta hace viable el análisis a gran escala al reducir el árbol de decisiones y concentrar la atención en líneas de acción con mayor calidad potencial (Sokri, 2022). A nivel operativo, el refinamiento iterativo permite identificar riesgos y oportunidades de forma sistemática y ajustar maniobras, recursos y apoyos para incrementar la probabilidad de éxito, en línea con enfoques que destacan el valor del *wargaming* asistido para mejorar coherencia y eficacia de la ejecución (Caffrey, 2022).

En síntesis, el caso práctico muestra una lógica de empleo realista: la IA no sustituye el *wargaming*, sino que lo refuerza. Aporta iteraciones adicionales, estandariza resultados y mejora la trazabilidad, mientras el analista conserva la función de interpretar, cuestionar y decidir. Esta combinación permite que la confrontación sea más exigente y eficiente dentro del ciclo de planeamiento, sin sacrificar la responsabilidad inherente del

comandante, condición central del mando y control en el nivel operacional.

3.3 Resultados comparativos modelo tradicional vs IA

El proceso de confrontación ha evolucionado con la introducción de IA. Mientras que el método tradicional se apoya en la experiencia y el juicio de los analistas, el modelo basado en IA se sustenta en optimización computacional y en medidas de efectividad cuantificables (MoE). En este epígrafe, se comparan ambos enfoques según rapidez, precisión/objetividad y eficiencia de personal. Conviene considerar que el Grupo de Planeamiento (JOPG) del método tradicional integraba personal de los tres ejércitos y la Guardia Civil, y que parte del equipo no tenía experiencia previa en planeamiento operacional.

La diferencia más visible es el tiempo. El método tradicional requiere aproximadamente cincuenta minutos por condición decisiva; aplicado a trece condiciones decisivas, equivale a unas 10,83 horas por analista. En contraste, la IA analiza más de setenta mil combinaciones en menos de treinta minutos, incluidas iteraciones y refinamientos dentro del mismo ciclo (Goecks y Waytowich, 2024). La dedicación con IA se estimó en 6,5 horas por analista, reduciendo alrededor del 40 % la fase de ejecución (figura 5). Si se suma el tiempo de preparación y se multiplica por el personal necesario, el total pasa de 333,67 horas en el método tradicional a ciento dos horas con IA, lo que supone una disminución del 69,4 %. Esta ganancia es coherente con precedentes que integraron IA (p. ej., CADET) en procesos de planeamiento, donde se obtuvieron planes detallados en ~20 minutos frente a ~16 horas-persona del proceso manual, sin degradar la calidad (Rasch *et al*., 2002).

En recursos humanos, el método tradicional precisó de veintiséis oficiales organizados en células RED, BLUE, WHITE, GREEN y apoyo. El método optimizado opera con doce personas y roles definidos para maximizar la interacción hombre-máquina (Wong *et al*., 2019): jugadores por célula que introducen decisiones y contrastan *outputs*; un responsable técnico que mantiene la arquitectura y mitiga el efecto «caja negra»; perfiles de gestión de datos y análisis; facilitación digital para evitar fricciones tecnológicas y apoyo especializado por dominios (logística, ciber, *targeting*, etc.). Esta reducción (-53,8 %) aporta un doble beneficio: disminuye el personal total implicado y libera oficiales de tareas

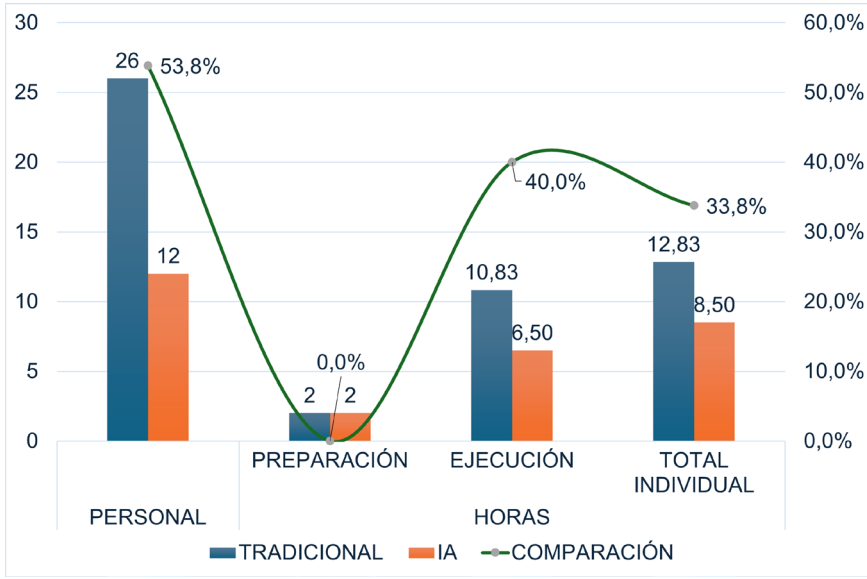


Figura 5. Comparación tiempo invertidos. Fuente: elaboración propia con datos de IA

repetitivas para redirigirlos hacia análisis crítico, planeamiento futuro o control de calidad doctrinal (Knack y Powell, 2023).

La precisión y la profundidad del análisis mejoran por la capacidad iterativa. La figura 5 muestra la evolución de las tasas de éxito por COA antes y después de optimizaciones, evidenciando el efecto positivo en «CEPO» y «APOCALIPSIS». A partir del análisis de MoE, el modelo con IA incrementa la proporción de resultados en niveles de «Éxito» frente al enfoque tradicional. Además, permite iterar el proceso decenas de veces y aplicar ajustes de inmediato: tras tres ciclos, «CEPO» pasa de 40 % a 70 % y «APOCALIPSIS» de 50 % a 80 %, lo que sugiere mayor capacidad para afinar la sincronización de acciones y efectos hacia la condición decisiva objetivo (Reynolds, 2024).

En visualización y comprensión, la IA presenta resultados en tablas, histogramas, diagramas de árbol y comparativos de MoE, facilitando detectar patrones de éxito, vulnerabilidades y acciones de mayor impacto. En el método tradicional, estos productos suelen construirse manualmente tras cada sesión, con mayor consumo de tiempo y riesgo de error interpretativo (Scott y Michell, 2023).

En cuanto a objetividad, el método tradicional se apoya en juicios subjetivos e interpretaciones doctrinales, con mayor exposición a sesgos cognitivos cuando falta experiencia (NATO ACT, 2017). El enfoque con IA integra doctrina, datos históricos y modelos simulados y emplea árboles de decisión con algoritmo minimax y poda alfa-beta (DeBerry *et al*., 2022). Esta aproximación está alineada con Código de buenas prácticas (COBP) de la OTAN, que define que el análisis en los *wargames* debe ser objetivo y riguroso. Asimismo, mejora trazabilidad y reproducibilidad al registrar la lógica de decisión y permitir auditoría y réplica del análisis ante cambios del entorno. También incrementa la flexibilidad operativa al facilitar modificaciones en tiempo real de escenarios y reacciones adversarias.

Ahora bien, los resultados deben interpretarse con prudencia. Una mejora de tasa de éxito no equivale a predicción, sino a desempeño bajo supuestos explícitos. Si los supuestos son erróneos, el resultado puede ser engañoso, aunque sea consistente. Por ello, el valor del enfoque asistido no está en la «certeza», sino en la disciplina analítica. Se ha señalado que la IA aporta valor operativo cuando refuerza el juicio humano y no cuando lo reemplaza.

4 Impacto de la IA en la comparación de líneas de acción

4.1 El rol de la IA en la comparación de líneas de acción

La comparación de líneas de acción es el cierre analítico del planeamiento antes de que el mando seleccione la alternativa recomendada. En esa fase, se ordenan prioridades, se ponderan criterios y se elige la opción con mejor equilibrio entre eficacia, riesgo y sostenibilidad. La inteligencia artificial aporta velocidad, consistencia y trazabilidad cuando se integra con un método multicriterio y se mantiene el control humano. Al descargar trabajo mecánico, el Estado Mayor puede dedicar más tiempo a contrastar supuestos, explicar la recomendación y anticipar objeciones. Ese refuerzo es especialmente útil en entornos multinacionales, donde la doctrina exige justificar cada paso y comparar alternativas con criterios comunes claros (HQ DoA, 2019). En el enfoque tradicional, el grupo de planeamiento parte de criterios definidos por el mando y valora cada alternativa en función de esos criterios. El resultado se suele sintetizar en matrices de decisión y

productos visuales que facilitan el debate y la exposición, como tablas ponderadas o representaciones gráficas de fortalezas y debilidades (Schmitt, 2015). Esta estructura aporta disciplina, pero destaca la acumulación de un «doble sesgo»: el sesgo del comandante al ponderar criterios (intuiciones, presiones externas, cultura organizacional) y el sesgo de los analistas al puntuar COA (familiaridad doctrinal, calidad de la información disponible o sesgos cognitivos inconscientes) (Williams, 2011). Como ambos procesos son multiplicativos (peso × puntuación), el sesgo tiende a amplificarse y puede distorsionar la realidad, afectando a la decisión.

En este contexto, la inteligencia artificial introduce una innovación significativa. Mediante modelos de procesamiento del lenguaje natural entrenados en doctrina OTAN, literatura militar, lecciones identificadas y escenarios históricos, la IA puede apoyar un razonamiento experto más estructurado, transparente y verificable (Garat, 2023). Su propósito no es sustituir el juicio del comandante, sino ampliar su capacidad de análisis, minimizar sesgos, mejorar la trazabilidad y reducir la carga cognitiva, aportando explicaciones de por qué una ponderación o una valoración propuesta resulta razonable a la luz de la evidencia disponible. Este apoyo es especialmente útil en entornos multinacionales, donde la calidad del producto depende de que el razonamiento sea entendible para audiencias con procedencias y culturas operativas diferentes (HQ DoA, 2019).

Una vía práctica de actuación es combinar la IA con métodos multicriterio como el Proceso Analítico Jerárquico (AHP). Este método descompone el problema en niveles, obliga a comparar criterios por pares y transforma preferencias cualitativas en prioridades cuantificables, incorporando, además, un control de coherencia interna (Saaty, 1980). En lugar de preguntar «cuánto pesa cada criterio» de forma directa, se pregunta «qué criterio es más importante entre dos y en qué grado». Al repetir ese ejercicio para todos los pares, se obtiene una jerarquía de pesos que refleja la intención del comandante de manera más estructurada. Frente a asignaciones directas e intuitivas, la IA puede fundamentar esas comparaciones con datos doctrinales, históricos o contextuales extraídos automáticamente de repositorios complejos, reforzando la base empírica del análisis (Farmer, 2022).

Este apoyo reduce debilidades habituales del método tradicional. La primera es la variabilidad entre equipos: dos Estados Mayores distintos pueden ponderar de forma diferente a partir del mismo

conjunto de criterios si no existe una disciplina explícita de comparación. La segunda es el sesgo de disponibilidad: bajo presión, se tiende a sobredimensionar el criterio más visible o el riesgo más reciente, aunque no sea el más decisivo. La tercera es la fragilidad argumental: cuando una autoridad o un actor externo cuestiona la recomendación, el equipo necesita explicar con precisión qué supuestos, qué pesos y qué valoraciones conducen a la conclusión. La IA no elimina esos riesgos, pero puede mitigarlos al exigir que cada comparación quede registrada y al ofrecer explicaciones consistentes para los valores asignados (Vestner, 2024).

Además, la IA puede reducir la carga de trabajo del Estado Mayor. La comparación de líneas de acción en operaciones complejas suele requerir varias iteraciones, productos intermedios y coordinación entre secciones. Automatizar cálculos, generar tablas y producir justificaciones homogéneas permite concentrar el esfuerzo humano en decisiones de fondo: si el criterio está bien definido, si el peso refleja la intención del comandante y si la valoración de cada alternativa es coherente con los resultados de la confrontación.

El rol de la IA, por tanto, no es «elegir» la mejor línea de acción, sino sostener un proceso comparativo más disciplinado, repetible y fácil de explicar. Su contribución se mide por la consistencia de las ponderaciones, la claridad de las justificaciones y la capacidad de repetir el análisis cuando cambian supuestos o restricciones. En un entorno de planeamiento exigente, esa combinación mejora la calidad de la recomendación y refuerza la legitimidad del producto final ante el comandante y ante la organización.

4.2 Comparación de líneas de acción optimizada con IA

La fase de comparación de COA obliga a jerarquizar prioridades operativas en un marco de incertidumbre parcial, tiempo limitado y multiplicidad de variables interdependientes. El empleo de técnicas de decisión multicriterio tiene como objetivo reducir la incertidumbre en contextos donde se deben comparar varias alternativas (COA) bajo criterios múltiples (Hellin, 2020).

El método AHP, desarrollado por Saaty en los años setenta, destaca por su capacidad para descomponer problemas complejos en estructuras jerárquicas. Este hecho permite una comparación clara y coherente entre diferentes alternativas o líneas de acción

(COA) (Saaty, 1980). En el ámbito militar, su aplicabilidad ha sido validada tanto en procesos de adquisición (Ruiz, 2021) como en operaciones, integrar la IA en este proceso no altera su lógica estructural, sino que incrementa su potencia mediante el procesamiento masivo de datos doctrinales, históricos, técnicos y contextuales, facilitando decisiones con mayor evidencia empírica y justificación trazable (Garat, 2023).

A diferencia de modelos puramente cuantitativos, el AHP permite la integración de juicios cualitativos del decisor, que son transformados en valores numéricos a través de comparaciones por pares (Kwok y Lim, 2011). Esta versatilidad lo convierte en una herramienta potente para jerarquizar líneas de acción, atendiendo a criterios definidos por el comandante, tales como bajas, rapidez, flexibilidad, disuasión o protección de civiles.

Sin embargo, su implementación manual adolece de varios problemas: está sujeta a sesgos cognitivos, puede consumir tiempo considerable en situaciones de presión operativa y presenta limitaciones en cuanto a la gestión de grandes volúmenes de datos doctrinales (William, 2011). En este contexto, la integración de la IA con el AHP da lugar a un modelo híbrido que maximiza las fortalezas de ambas aproximaciones: la estructuración jerárquica del AHP y la capacidad de análisis, predicción y evaluación automatizada de la IA elevando la calidad, precisión y robustez de la decisión adoptada (Bossio, 2023).

El proceso de comparación optimizada con IA se estructura en cuatro etapas consecutivas. En la primera etapa se define y representa el problema, a continuación, se evalúan los criterios o subcriterios, dividiéndose en las subetapas de ponderación y valoración de criterios. Seguidamente, se evalúan las alternativas para por último obtenerse la jerarquización final (Saaty, 1980). En cada fase, la IA actúa como sistema de apoyo experto, asistiendo en la recopilación de información, aplicación del AHP y generación de resultados explicables y trazables para el comandante. En esta integración hombre-máquina, reside el verdadero salto cualitativo de la toma de decisiones (Reynolds, 2024).

A continuación, se definirán cada una de estas etapas y como la IA se incorpora a las mismas. En la Etapa 1 (figura 6), de formulación del problema, se descompone el problema de decisión en su jerarquía lógica: objetivo, criterios, subcriterios (si los hubiera) y alternativas (Ruiz, 2021). El objetivo general es seleccionar la COA óptima para cumplir la misión. Los criterios son definidos

por el comandante, y pueden basarse en doctrina (COPD, PDC-5), experiencia previa o condiciones del entorno. Las alternativas son las COA propuestas por el JOPG tras la fase de desarrollo: en

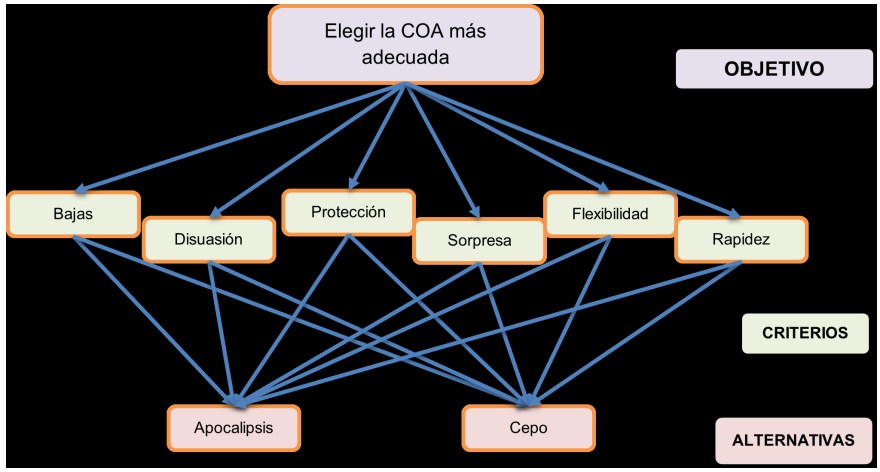


Figura 6. Etapa 1. Selección de alternativas y criterios. Fuente: elaboración propia

el caso práctico del ejercicio CONSTELLATIA, se trabajará con las COA APOCALIPSIS y CEPO.

La IA puede asistir en esta fase sugiriendo criterios que históricamente han sido relevantes en operaciones similares, así como subcriterios derivados, por ejemplo, descomponiendo «bajas» en bajas propias, civiles o de fuerzas aliadas. Esto asegura una representación más completa del problema, especialmente útil en escenarios complejos y multinacionales (DeBerry *et al*., 2024).

La Etapa 2 de evaluación de criterios se realiza la ponderación de los criterios. En el contexto militar, esta ponderación debe reflejar fielmente las prioridades operacionales del comandante. Para lograrlo, se aplica el método AHP utilizando la IA como sistema de apoyo de juicio experto. A través de una matriz de comparación por pares, se valoran las relaciones relativas de importancia entre cada par de criterios (Marks, 2008). La IA actúa como evaluador experto al aplicar reglas doctrinales, aprendizaje histórico y contexto operacional para proponer valores iniciales, detectar incoherencias y justificar los pesos resultantes.

En el método AHP, los criterios se comparan dos a dos preguntándose cuál de los dos es más importante y en qué medida. Esta comparación se realiza utilizando la escala de Saaty, que va del

1 (igual importancia) al 9 (importancia extrema de un criterio sobre otro). Por ejemplo, si el criterio «bajas propias» se considera fuertemente más importante que «rapidez de ejecución», se asignará un valor de 5 en la celda correspondiente. La celda simétrica de la matriz tomará el valor recíproco (1/5). Este procedimiento se repite para todos los pares de criterios.

Para una comparación con n criterios, se construye una matriz cuadrada n x n, siendo cada elemento a_ij la importancia del criterio i respecto al j. Una vez completada, se normaliza cada columna de la matriz dividiendo cada valor por la suma de su columna, y luego se promedia cada fila para obtener el vector de prioridades o pesos relativos. Esta técnica garantiza una distribución coherente de los pesos en función de las comparaciones realizadas (Vargas, 2021).

Para validar la coherencia de estas comparaciones, se aplica el cálculo del Índice de Consistencia (CI) y del Ratio de Consistencia (CR). El CI mide la desviación respecto a una matriz perfectamente coherente. El CR compara este valor con un índice aleatorio (RI) basado en el número de criterios. Si CR < 0.10, se considera que los juicios son aceptablemente coherentes. En caso contrario, se deben revisar las comparaciones realizadas. Este control garantiza que la ponderación no solo refleja las prioridades, sino que lo hace de manera lógica y justificable (Vafaei *et al*., 2020).

La integración de IA en esta fase consiste en delegar a un modelo entrenado en doctrina militar (por ejemplo, COPD, AJP-5) la función de evaluador experto. Gracias a su capacidad para emular un panel de expertos virtuales, puede realizar múltiples rondas de comparación por pares, identificando patrones de consenso y eliminando valores atípicos (Goecks *et al*., 2023). Esta funcionalidad amplía la robustez del sistema y permite reducir la influencia de sesgos individuales. Además, la IA puede detectar inconsistencias, calcular automáticamente el CR y proponer ajustes precisos para mejorar la coherencia, ahorrando tiempo y reduciendo errores humanos.

La Etapa 3 de evaluación de las COA consiste en valorar cómo se comporta cada COA frente a los criterios previamente ponderados. La IA realiza esta función procesando datos provenientes de doctrinas OTAN, simulaciones operacionales, resultados históricos (Lawrence, 2017), indicadores de adiestramiento, cohesión y efectividad (MOE y MOP), y evalúa cada combinación COA-criterio manteniendo la escala de comparación por pares.

Cada puntuación se justifica doctrinalmente y es trazable por parte del comandante. Esto elimina el sesgo del analista y asegura consistencia en todos los escenarios en coordinación con las prioridades del comandante. Este sistema permite que la valoración no dependa de forma exclusiva del juicio humano, sino que sea el resultado de un análisis multifuente, trazable y empíricamente fundamentado (Svoboda y Lande, 2024). La IA actúa, así, como un asesor operacional virtual que combina conocimiento doctrinal, histórico y predictivo, elevando la calidad de la comparación entre COA.

Por último, en la Etapa 4 la IA emite la clasificación jerarquizada de cada COA. Igualmente se incluye una ficha técnica de cada una, donde detalla el cumplimiento de cada criterio, sus riesgos asociados, medidas de mitigación y propuestas de refinamiento si fuera necesario. Esta salida permite una toma de decisión informada, racional y transparente.

La trazabilidad del proceso IA+AHP constituye una ventaja clave en entornos OTAN. El planeamiento multinacional exige justificar cada paso del análisis. Además, este enfoque es escalable: permite integrar más criterios, analizar más COA y realizar simulaciones rápidas bajo distintas premisas, aportando flexibilidad al planeamiento (Reynolds, 2024).

4.2.1 Caso práctico comparación líneas de acción con IA

En un Cuartel General, cuando el tiempo aprieta y la incertidumbre manda, el momento de comparar COA suele ser el punto donde una buena intuición puede salvar una operación… o donde un sesgo silencioso puede inclinar una decisión sin que nadie lo perciba. En este epígrafe, se aplica de manera práctica el modelo hibrido IA+AHP a la etapa de comparación de COA. Al igual que en la fase de confrontación, se toma como base el ejercicio de alta intensidad CONSTELLATIA.

En el caso analizado, se trabajó con dos líneas de acción que perseguían los mismos objetivos operacionales, pero diferían en la forma de alcanzarlos. Una de ellas, denominada APOCALIPSIS, se caracterizaba por una maniobra indirecta y envolvente, con énfasis en la sincronización de fuegos, la decepción y la acción simultánea en varios dominios. La otra, CEPO, proponía una acción más directa, orientada a la concentración de fuerzas y al aprovechamiento del impulso operacional mediante un esfuerzo prioritario en el eje central. La diferencia esencial no era el fin, sino el perfil de riesgo, el ritmo y las dependencias de coordinación.

El estudio se desarrolla siguiendo cuatro etapas metodológicas: representar el problema, ponderar criterios, evaluar alternativas y jerarquizar el resultado final. Cada etapa se refuerza con capacidades analíticas de la IA, entrenada con un corpus doctrinal y técnico amplio (más de dos mil documentos). Con ello se busca que la comparación no dependa únicamente de la intuición del equipo de planeamiento, sino de una base más empírica y defendible.

La primera etapa consiste en construir una jerarquía decisional simple (figura 6): arriba, el objetivo global («seleccionar la mejor COA»); debajo, seis criterios definidos por el comandante y, en el nivel inferior, las dos alternativas. Aunque el AHP permite introducir niveles intermedios y subcriterios para descomponer problemas complejos, se optó por la versión más simple para replicar el procedimiento doctrinal y facilitar una comparación objetiva entre enfoques (Kasperczyk y Knickel, 2022).

Con el marco definido, la segunda etapa se centra en la ponderación de los criterios aplicando la técnica AHP asistida por IA. Se construye una matriz de comparación por pares siguiendo la escala de Saaty: criterio contra criterio, estableciendo cuál pesa más y en qué grado. La aportación de la IA en esta fase es ayudar a convertir intuiciones en comparaciones justificadas, apoyándose en doctrina OTAN, lecciones identificadas, información contextual aportada por inteligencia (J2), antecedentes históricos y simulaciones coherentes con el entorno. La clave no es solo asig-

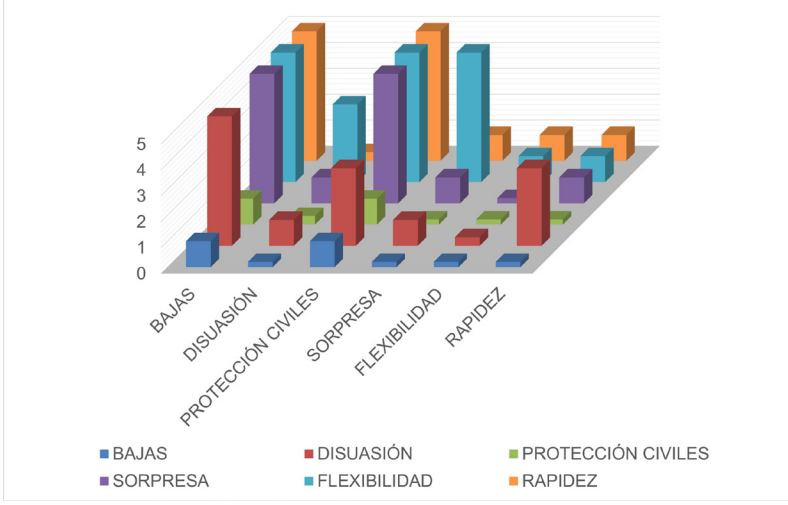


Figura 7. Matriz comparada por pares. Fuente: elaboración propia con datos de la IA

nar números, sino sostenerlos con razones verificables dentro del marco operativo y doctrinal disponible (figura 7).

El control de consistencia tuvo aquí un papel práctico. Una matriz de comparaciones puede resultar aparentemente razonable y, sin embargo, contener contradicciones. El índice de consistencia obliga a revisar comparaciones si la estructura lógica no se sostiene, lo que protege al proceso de preferencias arbitrarias (Salomon y Gomes, 2024). La IA facilita esta revisión porque identifica qué pares generan la inconsistencia y propone ajustes mínimos para recuperar coherencia, de modo que el resultado conserve el sentido original del mando.

Un ejemplo ayuda a entender cómo se traduce ese apoyo en decisiones concretas. En el escenario del ejercicio, el criterio de protección de civiles o bajas propias adquirió un peso dominante, por su impacto en la continuidad del esfuerzo y en la legitimidad política de la operación. La IA vinculó esa prioridad a doctrina aliada y a lecciones de campañas recientes, donde el coste humano condicionó el margen de maniobra y la aceptación pública (CCOE, 2024). De forma similar, la valoración de criterios asociados a sorpresa y disuasión se apoyó en precedentes de presencia avanzada aliada, en los que la percepción del compromiso influye en el cálculo del oponente (Palavenis, 2024). Estas referencias no sustituyeron el juicio del equipo, pero facilitaron coherencia y consenso. Además, permitió justificar por escrito cada preferencia inicial y revisar rápidamente comparaciones inconsistentes.

La tercera etapa comparó las dos líneas de acción respecto a cada criterio. Este paso es el puente entre la intención del mando y la realidad del escenario: obliga a declarar, criterio a criterio, cuál alternativa ofrece mejor desempeño y en qué grado. La IA se empleó como asistente para fundamentar cada valoración, devolviendo una explicación basada en evidencia del propio escenario, en referencias doctrinales y registros históricos de operaciones similares, lo que reduce el riesgo de asignar números sin contexto.

En términos operacionales, la fase permitió distinguir entre ventajas de diseño y ventajas circunstanciales. Una línea de acción puede parecer superior porque promete rapidez, pero si su éxito depende de supuestos frágiles, esa rapidez puede traducirse en vulnerabilidad. Por el contrario, una alternativa más lenta puede ser preferible si mantiene flexibilidad, reduce exposición y sostiene legitimidad del esfuerzo. El método obliga a hacer explícitas

estas compensaciones y a vincularlas con pesos de criterios previamente definidos, evitando que la discusión se convierta en un intercambio de impresiones.

El modelo generó un vector de prioridades para las alternativas, resultado de las comparaciones por criterios y de los pesos

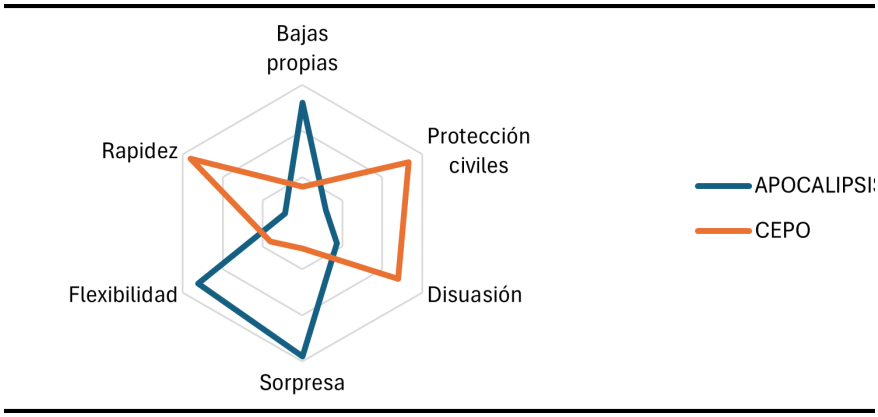
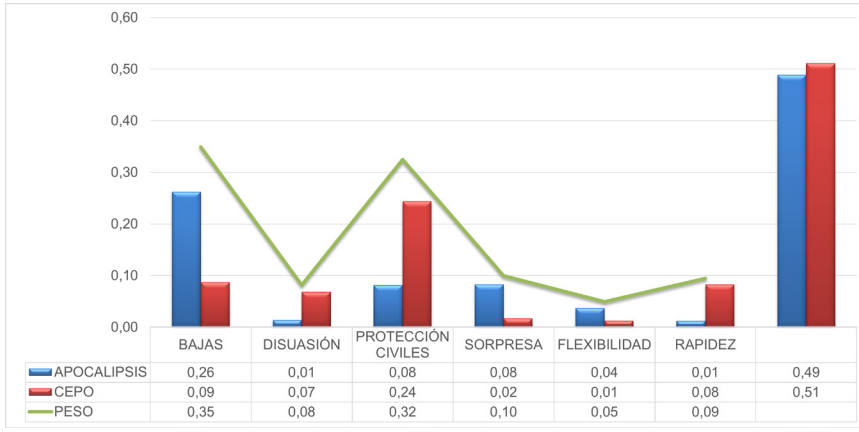


Figura 8. Vector propio de las líneas de acción. Fuente: elaboración propia con datos de IA

obtenidos (figura 8). Este vector, que puede interpretarse como una preferencia global, no es un veredicto automático, es un producto trazable que muestra cuánto contribuye cada criterio al resultado final.

La cuarta etapa convierte todo lo anterior en una recomendación cuantificada: la síntesis ponderada donde se multiplica el desempeño relativo de cada COA en cada criterio (Etapa 3) por el peso de ese criterio (Etapa 2) y se suman los productos para cada alternativa (Vargas, 2010). Este cálculo integra las preferencias del comandante (expresadas en pesos) con la evaluación comparativa de alternativas, generando una puntuación total de adecuación global a los objetivos operacionales. La figura 9 presenta la matriz de síntesis con valores ponderados. Con la finalización de esta cuarta etapa, se cierra el ciclo del modelo AHP asistido por IA.

En la práctica, la comparación asistida por IA aportó tres mejoras observables. La primera fue velocidad con disciplina, en la que se redujo el tiempo dedicado a construir matrices y a recalcular pesos, sin perder el control de consistencia. La segunda fue coherencia, el proceso mantuvo un hilo lógico entre intención del



	BAJAS	DISUASIÓN	PROTECCIÓN CIVILES	SORPRESA	FLEXIBILIDAD	RAPIDEZ	
APOCALIPSIS	0,26	0,01	0,08	0,08	0,04	0,01	0,49
CEPO	0,09	0,07	0,24	0,02	0,01	0,08	0,51
PESO	0,35	0,08	0,32	0,10	0,05	0,09	

Figura 9. Jerarquización de las líneas de acción. Fuente: elaboración propia con datos de IA

comandante, pesos de criterios, valoraciones por criterio y resultado. La tercera fue capacidad de explicación, cada valor asignado podía vincularse a una justificación y, por tanto, defenderse ante preguntas críticas.

También se identificaron límites que condicionan el empleo. El modelo puede amplificar errores si los criterios están mal definidos, si las valoraciones se alimentan con supuestos incorrectos o si la evidencia del escenario es incompleta. Por eso, el control del analista se mantuvo en tres puntos: validación del conjunto de criterios, revisión de comparaciones por pares y contraste de valoraciones de alternativas. El sistema apoya, pero la responsabilidad de aceptar un peso o una valoración sigue siendo del equipo y del mando.

Un aspecto relevante fue el efecto sobre el debate del grupo de planeamiento. Con el enfoque tradicional, parte del tiempo se consume en acordar pesos y en reconstruir por qué se asignó una puntuación. Con el enfoque asistido, el debate se desplazó hacia preguntas de fondo: qué criterio refleja mejor la intención del mando, qué riesgos son inaceptables y qué medidas mitigadoras podrían cambiar la valoración de una alternativa. En ese sentido, la IA no añadió una capa tecnológica, sino un mecanismo para centrar el tiempo del grupo de planeamiento en juicio y decisión.

Finalmente, el caso práctico mostró que el resultado más valioso no es el *ranking* en sí, sino la claridad sobre sus causas. Cuando la jerarquía favorece a una alternativa, el equipo puede ver si la razón es una ventaja sostenida en criterios clave o una dependencia excesiva de un único criterio. Esta lectura permite refinar

la alternativa seleccionada y preparar la argumentación para su presentación. En un entorno aliado, donde la recomendación debe ser entendible por diferentes actores, esa trazabilidad refuerza la legitimidad del proceso y mejora la calidad de la directiva posterior (CCOE, 2024).

4.3 Resultados comparativos modelo tradicional vs IA

La elección de la mejor COA es uno de los momentos más críticos del proceso de planeamiento operacional. El contraste entre el método tradicional y el modelo asistido por IA se aprecia, ante todo, en la forma de construir y sostener la recomendación.

En el enfoque tradicional, la comparación se basó en una matriz ponderada donde el equipo asigna valores a cada alternativa conforme a criterios definidos por el mando y, a partir de esa síntesis, el comandante decide. En este modelo, la COA APOCALIPSIS fue seleccionada como la más adecuada, al obtener una puntuación total de 66 puntos frente a los 41 de la COA CEPO.

La comparación se realizó según los seis criterios seleccionados por el comandante. Cada criterio recibió un peso asignado subjetivamente, y cada COA fue valorada del 1 al 3 según su rendimiento en ese criterio. Al multiplicar el peso por la puntuación y sumar los resultados, APOCALIPSIS obtuvo una ventaja significativa. Esta metodología, si bien estructurada, está fuertemente condicionada por el juicio humano, lo que introduce un doble sesgo: el del comandante al ponderar los criterios, y el de los analistas al valorar las alternativas. Dado que ambos elementos se multiplican, el sesgo se ve también amplificado, pudiendo distorsionar el resultado final.

Por el contrario, el modelo híbrido propuesto en este trabajo combina el método AHP con IA, permitiendo una asignación empírica de pesos y valoraciones a partir de análisis doctrinal, evaluación cuantitativa y antecedentes operativos. En este modelo, los criterios se ponderan mediante comparaciones por pares fundamentadas en datos doctrinales y contextuales (COPD, AJP-5, historial de combates, potencia de combate relativa, evaluación de capacidades de las fuerzas implicadas, etc.) (Torres, 2009). De igual modo, las COA se comparan según cada criterio con una base empírica y reproducible.

Al aplicar este modelo al caso CONSTELLATIA, los resultados se invierten. La COA CEPO obtiene una puntuación final de 0,5105

frente al 0,4895 de APOCALIPSIS. La diferencia es estrecha, pero relevante (figura 10). Este resultado se explica principalmente por la distinta ponderación de los criterios. Por un lado, el modelo tradicional dio una prioridad máxima al criterio de bajas propias (40 % del peso), seguido del criterio de disuasión y protección de civiles (20 % de peso cada uno). Por otro lado, el modelo AHP+IA

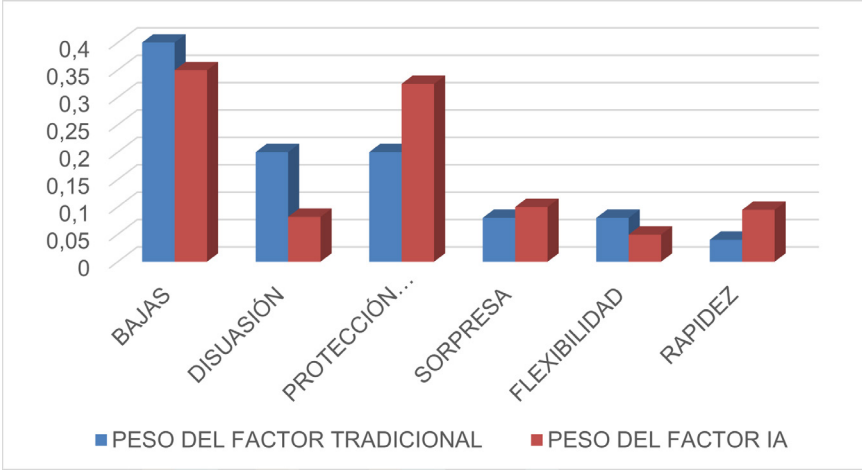


Figura 10. Comparación criterios ambos modelos. Fuente: elaboración propia

equilibra la importancia entre bajas y protección de civiles, otorgando a estos dos criterios un peso relativo del 60 % del total. Esta redistribución se justifica en base a experiencias recientes en conflictos urbanos e híbridos, donde la rapidez y la protección civil tienen un impacto directo sobre la legitimidad y sostenibilidad de la operación (Lawrence, 2017).

Asimismo, en el modelo tradicional se valora a APOCALIPSIS como más favorable en la mayoría de los criterios, mientras que en el modelo AHP+IA, CEPO sobresale en disuasión, protección civil y rapidez, tres criterios decisivos en el contexto de CONSTELLATIA, donde la explotación del *momentum* operacional y la consolidación del control territorial son claves para alcanzar la estabilidad de la región. La IA fundamenta esta valoración en datos objetivos sobre el despliegue de fuerzas, niveles de adiestramiento, probabilidad de éxito de cada COA y simulaciones doctrinales.

En síntesis, la comparación entre ambos modelos revela el valor añadido que aporta la integración de IA al proceso de decisión militar. No solo se consigue una mayor objetividad y trazabilidad, sino que se facilita la comprensión de por qué una COA es más adecuada que otra, permitiendo al comandante tomar una decisión informada y fundamentada en datos. Este caso práctico valida empíricamente la utilidad del modelo propuesto y abre la puerta a su incorporación doctrinal futura en el planeamiento operacional de la Alianza.

5 Conclusiones

El planeamiento operacional se sostiene sobre una tensión permanente, la necesidad de decidir con rapidez y la obligación de justificar esas decisiones con rigor, especialmente cuando la operación es conjunta y multinacional. En ese marco, la inteligencia artificial no aparece como un atajo que reemplace el juicio del mando, sino como un multiplicador de análisis cuando se integra en métodos ya aceptados. La experiencia descrita muestra que su valor crece cuando se emplea para ampliar iteraciones, reducir trabajo mecánico y mantener un registro trazable de supuestos, decisiones y resultados, en línea con las exigencias doctrinales del proceso.

En la confrontación, el aporte principal se sitúa en la capacidad de explorar más trayectorias de enfrentamiento sin consumir el tiempo del Estado Mayor. El *wargaming* tradicional sigue siendo insustituible para construir entendimiento compartido, identificar decisiones críticas y captar matices del adversario, pero se ve limitado por el número de iteraciones posibles y por la variabilidad inherente a sesiones sucesivas. La asistencia de IA permite ejecutar rondas adicionales bajo supuestos comunes, registrar patrones de fallo y orientar el debate humano hacia los puntos donde el plan es más frágil. En vez de competir con el *wargaming*, lo refuerza, convierte la confrontación en un ciclo más repetible, donde cada ajuste se evalúa y queda documentado.

En la comparación, el beneficio es aún más visible porque se apoya en un método formal. El Proceso Analítico Jerárquico ofrece un marco que traduce la intención del mando en pesos de criterios y obliga a comparar alternativas con disciplina, incorporando un control de coherencia interna. Cuando la IA se integra como asistente experto, puede acelerar la construc-

ción de matrices, proponer comparaciones iniciales coherentes con doctrina y contexto, y devolver explicaciones estructuradas que facilitan la rendición de cuentas. El resultado no es una «decisión automática», sino una recomendación más fácil de explicar: se ve qué criterios determinan el *ranking* y qué cambios de prioridad serían necesarios para invertirlo.

La lección operativa más importante es que la IA aporta valor cuando aumenta la capacidad de explicación del proceso, no cuando promete certeza. La comparación de líneas de acción, por definición, trabaja con incertidumbre. Por ello, el indicador de calidad no es que el modelo «acierte» el futuro, sino que el Estado Mayor pueda defender por qué recomienda una alternativa, qué riesgos acepta y qué supuestos considera críticos. Ese enfoque encaja con la cultura doctrinal del planeamiento, que exige coherencia, transparencia y capacidad de revisión cuando cambian restricciones o se reciben nuevas directrices.

Al mismo tiempo, el empleo introduce condiciones de prudencia. Un sistema capaz de producir matrices, pesos y gráficos con rapidez puede amplificar errores si se alimenta con criterios ambiguos, supuestos implícitos o datos incompletos. La calidad de entrada es, por tanto, una responsabilidad del equipo, definir criterios sin solapes, explicitar restricciones, validar comparaciones por pares y contrastar valoraciones con productos del propio planeamiento. Los controles del método, como el índice de consistencia, ayudan a detectar incoherencias, pero no reemplazan la verificación humana del sentido operacional. En esta integración hombre-máquina reside la garantía de que la velocidad no degrade el rigor.

El caso de Constellatia permite extraer una implicación práctica adicional: la IA desplaza el esfuerzo del grupo de planeamiento desde la producción hacia la interpretación y análisis. Cuando los cálculos y los productos intermedios se generan con más rapidez, se gana tiempo para discutir lo importante: si los criterios reflejan la intención del comandante, si las medidas mitigadoras cambian el perfil de riesgo, o si la alternativa seleccionada depende de supuestos frágiles. Este desplazamiento es especialmente valioso en ejercicios y operaciones donde el ritmo obliga a iterar varias veces. En términos de mando, significa más tiempo para juicio, y menos para tareas de oficina.

Por otro lado, la trazabilidad de un modelo basado en comparaciones por pares facilita explicar por qué un criterio pesa más,

cómo se valoró una alternativa y qué evidencia lo sustenta. Esa transparencia reduce fricción entre secciones y entre naciones porque convierte desacuerdos difusos en discrepancias concretas, se debate un peso o una comparación, no un resultado global opaco. Además, al conservar un registro de entradas y salidas, el equipo puede repetir el análisis cuando cambian premisas sin volver a empezar, lo que mejora la continuidad del proceso de planeamiento.

Desde la perspectiva de transformación, el empleo de IA en confrontación y comparación se alinea con el impulso de modernización doctrinal y de gestión del conocimiento. La doctrina nacional y aliada subraya la necesidad de integrar información de múltiples dominios y de sostener decisiones con productos coherentes.

Cabe destacar que teniendo en cuenta el nivel de desarrollo tecnológico actual no se pretende que la IA reemplace la decisión humana. Su papel es el de un «multiplicador cognitivo», ofreciendo capacidad de análisis ampliada, pero siempre bajo la supervisión y validación humana. Sin embargo, es coherente afirmar que la capacidad de aprendizaje de la IA hace posible que se reduzcan los tiempos de refinamiento dentro del ciclo de decisión. El caso práctico validó la utilidad del modelo propuesto, demostrando su fiabilidad y superioridad frente al enfoque tradicional en términos de objetividad y fundamentación de la decisión.

Un último aspecto es la gobernanza del dato y del modelo. La utilidad de la IA depende de que las entradas sean pertinentes, estén controladas y puedan auditarse. En *wargaming* analítico, se insiste en capturar datos de las iteraciones para comparar resultados y mejorar modelos. Del mismo modo, el apoyo con IA exige definir fuentes autorizadas y trazabilidad de cada salida.

En conjunto, los resultados sostienen una tesis sencilla: la inteligencia artificial incrementa la calidad del planeamiento cuando se integra en la disciplina del proceso, no cuando se usa como sustituto. En confrontación, amplía iteraciones y revela patrones; en comparación, aporta coherencia y capacidad de explicación; en ambos casos, libera tiempo para el juicio profesional del Estado Mayor y mejora de forma evidente la calidad, rapidez, objetividad y precisión de la toma de decisiones. El valor último no es la automatización, sino la mejora de la decisión.

Bibliografía

Alberts, D. S. y Hayes, R. E. (2007). Planning: Complex Endeavors [en línea]. CCRP. [Consulta: 2026]. Disponible en: http://www.dodccrp.org/events/12th_ICCRTS/Papers/105.pdf

Allen, G. C. y Chan, T. (2017). Artificial Intelligence and National Security [en línea]. Belfer Center for Science and International Affairs, Harvard Kennedy School. [Consulta: 2026]. Disponible en: https://www.belfercenter.org

Araya, D. y King, M. (2022). The Impact of Artificial Intelligence on Military Defence and Security. *CIGI Papers*. N.º 263.

Asarta Cuevas, A. (2021). El nivel operacional. Monografías 149 [en línea]. Madrid, Ministerio de Defensa, Centro Conjunto de Desarrollo de Conceptos. [Consulta: 2026]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monograf_a_149_el_nivel_operacional.pdf

Bender, E. M. et al. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? [en línea]. FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. [Consulta: 2026]. Disponible en: https://dl.acm.org/doi/10.1145/3442188.3445922

Berwick, R. (2011). Game trees, minimax, & alpha-beta search. Recitation 3, 6.034 Artificial Intelligence [en línea]. Massachusetts Institute of Technology. [Consulta: 2026]. Disponible en: https://web.mit.edu/6.034/wwwbob/handout3-fall11.pdf

Bossio Ballesteros, V. E. (2023). La Inteligencia Artificial en el Ámbito Militar: Una Herramienta Relevante y Útil [en línea]. Revista Seguridad y Poder Terrestre. 2(3), pp. 53-61. [Consulta: 2026]. Disponible en: https://ceeep.mil.pe/2023/10/26/la-inteligencia-artificial-en-el-ambito-militar-una-herramienta-relevante-y-util/

Brown, T. et al. (2020). Language Models are Few-Shot Learners [en línea]. OpenAI. [Consulta: 2026]. Disponible en: https://arxiv.org/pdf/2005.14165.pdf

Burrell, J. (2016). How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms [en línea]. Big Data & Society. 3(1), pp. 1-12. [Consulta: 2026]. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2660674

Caffrey, M. (2022). Wargaming vs. Modeling and Simulation: Ancient Roots, Modern Overlap, Recent Friction and Potential Synergies [en línea]. En: *STO-TR-SAS-139 – NATO Analytical*

War Gaming: Innovative Approaches for Data Capture, Analysis and Exploitation. Capítulo 9. NATO Science and Technology Organization. [Consulta: 2026]. Disponible en: https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-SAS-139/$$TR-SAS-139-ALL.pdf

Carrasco, B. (2024). La Armada dotará de gemelos digitales a los submarinos S-80, fragatas F-100 y cazaminas [en línea]. Infodefensa. [Consulta: 2026]. Disponible en: La Armada dotará con gemelos digitales a los submarinos S80, las fragatas F100 y los cazaminas

Chance, G. *et al*. (2023). Using AI in Wargaming Simulation as a Multi-Domain Decision Support Tool. NATO Science and Technology Organization.

CIMIC Centre of Excellence (CCOE). (2024). *CIMIC Handbook. Civil-Military Cooperation Centre of Excellence* [en línea]. [Consulta: 2026]. Disponible en: https://www.cimic-coe.org/handbook-entries/welcome-to-the-cimic-handbook/

Comisión Europea. (2025). La UE pone en marcha la iniciativa InvestAI para movilizar 200.000 millones de euros [en línea]. Comisión Europea. [Consulta: 2026]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_25_467

Coomber, N. (2009). COA Wargaming is No Black Art [en línea]. Army Technology. [Consulta: 2026]. Disponible en: https://www.army-technology.com/features/feature50512/

Coutts, A., Williams, P. y Knoll, J. (2022). Enabling Analytical Wargaming Through Operations Analysis [en línea]. En: NATO Analytical War Gaming – Innovative Approaches for Data Capture, Analysis and Exploitation. Final Report of the Research Task Group SAS-139. STO-TR-SAS-139. NATO Science and Technology Organization. [Consulta: 2026]. Disponible en: https://costsofwar.watson.brown.edu/sites/default/files/papers/Crawford-Civilian-Death-and-Injury-Iraq.pdf

Crawford, N. C. (2011). Civilian Death and Injury in Iraq, 2003-2011 [en línea]. Watson Institute for International and Public Affairs, Brown University. [Consulta: 2026]. Disponible en: https://scholar.afit.edu/cgi/viewcontent.cgi?article=6043&context=etd

DeBerry, C. et al. (2022). The Wargame Commodity Course of Action Automated Analysis Method [en línea]. En: NATO Science and Technology Organization. NATO Analytical Wargaming – Innovative Approaches for Data Capture, Analysis and

Exploitation (STO-TR-SAS-139). [Consulta: 2026]. Disponible en: Home | NATO Science and Technology Organization

De Rosa, F. (2022). A Perspective on Automation and Autonomy for Analytical Wargaming [en línea]. En: NATO Analytical War Gaming: Innovative Approaches for Data Capture, Analysis and Exploitation. Capítulo 4. STO-TR-SAS-139. NATO Science and Technology Organization. Disponible en: https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-SAS-139/$$TR-SAS-139-ALL.pdf

DOPE. (2024a). *Libro Asignatura 13. Planeamiento de Operaciones Conjuntas*. (Adaptado a la COPD v 3.1 de 13 de octubre de 2023). XXVI Curso de Estado Mayor de las Fuerzas Armadas Españolas. Madrid, Centro Superior de Estudios de la Defensa Nacional (CESEDEN).

—. (2024b). *Ejercicio Constellatia 1.ª Fase 2025. Documentación operativa*. XXVI Curso de Estado Mayor de las Fuerzas Armadas Españolas. Madrid, Centro Superior de Estudios de la Defensa Nacional (CESEDEN).

Dupuy, T. N. (1979). Numbers, Predictions and War: Using History to Evaluate Combat Factors and Predict the Outcome of Battles. Indianapolis, Bobbs-Merrill.

Farmer, M. S. (2022). Four-Dimensional Planning at the Speed of Relevance: Artificial-Intelligence-Enabled Military Decision-Making Process [en línea]. Military Review. Army University Press, pp. 64-73. [Consulta: 2026]. Disponible en: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2022/

Farnell, R. y Coffey, K. (2024). AI's New Frontier in War Planning: How AI Agents Can Revolutionize Military Decision-Making [en línea]. Belfer Center for Science and International Affairs. [Consulta: 2026]. Disponible en: https://www.belfercenter.org/research-analysis/ais-new-frontier-war-planning-how-ai-agents-can-revolutionize-military-decision

Fernández Diz, A. (2024). El juego de la guerra (wargaming) y su inevitable importancia en el presente y en el futuro de nuestras fuerzas armadas [en línea]. Academia de las Ciencias y Artes Militares. [Consulta: 2026]. Disponible en: https://www.acami.es/wp-content/uploads/2024/11/El-juego-de-la-guerra-y-las-fuerzas-armadas-web.pdf

Garat González, J. M. (2023). La inteligencia artificial como factor de transformación de las operaciones militares en el nivel

operacional [en línea]. En: Monografía 158. Selección de los ocho mejores trabajos de fin de curso del XXIV CEMFAS y el mejor trabajo de fin de curso del XVI CSIFAS en el año escolar 2022-2023 impartido en el CESEDEN. Madrid, Ministerio de Defensa, Escuela Superior de las Fuerzas Armas. [Consulta: 2026]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monog rafia_158_xxiv_cemfas.pdf

Goecks, V. y Waytowich, N. (2022). COA-GPT: Transformadores Generativos Preentrenados para el Desarrollo Acelerado del Curso de Acción en Operaciones Militares [en línea]. University of Maryland. [Consulta: 2026]. Disponible en: arXiv:2402.01786v2 [cs.AI].

Goecks, V. G. *et al*. (2023). On games and simulators as a platform for development of artificial intelligence for command and control. *Journal of Defense Modeling and Simulation*. 20(4), pp. 495-508. DOI: 10.1177/15485129221083278

Gómez Gómez, C. (2016) *Tutor de algoritmos de juegos: Adversarial Search Tutor* [trabajo fin de grado] [en línea]. Universidad de Málaga. [Consulta: 2026]. Disponible en: http://hdl.handle.net/10630/12713

Grupo Ético Comisión Europea. (2018). *Declaración sobre Inteligencia Artificial, Robótica y Sistemas Autónomos* [en línea]. [Consulta: 2026]. Disponible en: https://data.europa.eu/doi/10.2777/531856

Hellín Vegas, A. (2020). Estudio de posibles implementaciones en el BMS (Battle Management System) [trabajo fin de grado] [en línea]. Universidad de Zaragoza. [Consulta: 2026]. Disponible en: https://zaguan.unizar.es/record/101057/files/TAZ-TFG-2020-4423.pdf

HQ Department of the Army (HQ DoA). (2019). ATP 2-01.3 Intelligence Preparation of the Battlefield/Battlespace [en línea]. US Army. [Consulta: 2026]. Disponible en: https://home.army.mil/wood/application/files/8915/5751/8365/ATP_2-01.3_Intelligence_Preparation_of_the_Battlefield.pdf

Instituto Español de Estudios Estratégicos (IEEE). (2020). Implicaciones del ámbito cognitivo en las operaciones militares [en línea]. Ministerio de Defensa de España, CESEDEN. [Consulta: 2026]. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf

Khimeche, L. y Champs, P. de. (2004). M&S in Decision Support for Course of Action Analysis: APLET [en línea]. En: *RTO-MP-MSG-028 – Modelling and Simulation to Address NATO's New and Existing Military Requirements, Koblenz*. Alemania, NATO Research and Technology Organisation. [Consulta: 2026]. Disponible en: https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/RTO-MP-MSG-028/MP-MSG-028-04.pdf

Knack, A. y Powell, R. (2023). Artificial Intelligence in Wargaming: An evidence-based assessment of AI applications [en línea]. CETaS Research Reports. [Consulta: 2026]. Disponible en: https://cetas.turing.ac.uk/publications/artificial-intelligence-wargaming

Krivokuća, M. (2019). Minimax with Alpha-Beta Pruning in Python [en línea]. Stack Abuse. [Consulta: 2026]. Disponible en: https://stackabuse.com/minimax-and-alpha-beta-pruning-in-python/

Kwok, Y. F. y Lim, H. S. (2011). Using Analytic Hierarchy Process with Operations Analysis in Project Evaluation [en línea]. Defence Science and Technology Agency (DSTA). [Consulta: 2026]. Disponible en: https://www.dsta.gov.sg/docs/default-source/dsta-programmes/using-analytic-hierarchy-process-with-operations-analysis-in-project-evaluation.pdf

Instituto Tecnológico de Nuevo Laredo (ITNL). (2005). Minimax [en línea]. [Consulta: 2026]. Disponible en: https://nlaredo.tecnm.mx/takeyas/Apuntes/inteligencia%20artificial/Apuntes/tareas_alumnos/Minimax/Minimax(2005-II-A).pdf

Lamparth, M. et al. (2024). Human vs. Machine: Behavioral Differences Between Expert Humans and Language Models in Wargame Simulations [en línea]. arXiv:2403.03407v1 [cs.CY]. [Consulta: 2026]. Disponible en: https://arxiv.org/abs/2403.03407v1

Lawrence, C. A. (2017). *War by Numbers: Understanding Conventional Combat*. Potomac Books.

Marks, H. A. (2008). Robust Sensitivity Analysis of Courses of Action Using an Additive Value Model [en línea]. Air Force Institute of Technology. [Consulta: 2026]. Disponible en: https://scholar.afit.edu/etd/2813/

Ministerio de Defensa. (2023). *PDC-5. Planeamiento de las operaciones*. Madrid, Ministerio de Defensa, Estado Mayor de la Defensa.

—. (2024). *PDC-01(B). Doctrina para el Empleo de las Fuerzas Armadas*. Ministerio de Defensa, Secretaría General Técnica.

Minutolo, V. (2021). Use of Analytic Hierarchy Process Modeling in the Military Decision-Making Process for Course of Action Evaluation and Unit Cohesion [en línea]. En: Proceedings of 7th International Symposium on the Analytic Hierarchy Process. Bali. [Consulta: 2026]. Disponible en: https://www.researchgate.net/publication/351446225_USE_OF_ANALYTIC_HIERARCHY_PROCESS_MODELING_IN_THE_MILITARY_DECISION_MAKING_PROCESS_FOR_COURSE_OF_ACTION_EVALUATION_AND_UNIT_COHESION

Nantes, E. A. (2019). Método Analytic Hierarchy Process para la toma de decisiones: repaso de la metodología y aplicaciones [en línea]. Investigación Operativa. 27(46), pp. 54-73. [Consulta: 2026]. Disponible en: https://repositoriodigital.uns.edu.ar/handle/123456789/6060

NATO. (2017). The NATO Alternative Analysis Handbook. 2.ª ed. Norfolk, Allied Command Transformation [en línea]. [Consulta: 2026]. Disponible en: https://www.act.nato.int/wp-content/uploads/2023/05/alta-handbook.pdf

NATO Science and Technology Organization (STO). (2022). NATO Analytical War Gaming – Innovative Approaches for Data Capture, Analysis and Exploitation. Final Report of the Research Task Group SAS-139 [en línea]. [Consulta: 2026]. Disponible en: https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-SAS-139/$$TR-SAS-139-ALL.pdf

NATO Standardization Office (NSO). (2019). *Allied Joint Doctrine for the Planning of Operations. AJP-05*. Edition A, Version 2. NSO.

—. (2023). Comprehensive Operations Planning Directive (COPD) v3.1. NSO.

Nonnenmacher, W. (2004). An Expert System Based Approach to Analyse the Underlying Structure of a Multilateral Crisis [en línea]. En: *RTO NMSG Symposium on "Modelling and Simulation to Address NATO's New and Existing Military Requirements". RTO-MP-MSG-028*. Koblenz. [Consulta: 2026]. Disponible en: https://publications.sto.nato.int/publications/

STO%20Meeting%20Proceedings/RTO-MP-MSG-028/MP-MSG-028-$$ALL.pdf

Ouyang, L. et al. (2022). Training language models to follow instructions with human feedback [en línea]. arXiv:2203.02155v1 [cs.CL]. [Consulta: 2026]. Disponible en: https://arxiv.org/abs/2203.02155

Palantir Technologies. (2025). Gotham [en línea]. Palantir Technologies. [Consulta: 2026]. Disponible en: https://www.palantir.com/platforms/gotham/

Palavenis, D. (2024). NATO Enhanced Forward Presence in the Baltics: The Nexus Between the Host and the Framework Nation [en línea]. Security and Defence Quarterly. 49(1), 74-97. [Consulta: 2026]. Disponible en: https://www.researchgate.net/publication/386042637_NATO_enhanced_forwar_presence_in_the_Baltics_The_nexus_between_the_host_and_the_framework_nation

Quevedo, J. R. y Quevedo, E. G. (2021). Árbol de juegos: Del algoritmo Minimax con poda α-β al algoritmo Montecarlo Tree Search. Fuerza bruta vs. Aleatoriedad [en línea]. Formación del Profesorado e Investigación en Educación Matemática XIII, pp. 169-203. [Consulta: 2026]. Disponible en: https://accedacris.ulpgc.es/bitstream/10553/121232/1/183-602-1-PB.pdf

Rasch, R., Kott, A. y Forbus, K. D. (2002). AI on the Battlefield: An Experimental Exploration [en línea]. Proceedings of the Eighteenth National Conference on Artificial Intelligence (AAAI-02). Association for the Advancement of Artificial Intelligence, pp. 878-884. [Consulta: 2026]. Disponible en: https://cdn.aaai.org/AAAI/2002/AAAI02-134.pdf

Reynolds, I. J. (2024). *AI Enabled Command in the United States: Rhetorical Contestation and Solving the Problems of Speed and Knowledge in War* [tesis doctoral inédita]. Washington D.C., American University.

Richardson, H. (2004). *Measures of Effectiveness (MOE) and Effects-Based Operations (EBO) in the Headquarters ARRC. The Cornwallis Group IX: Analysis for Stabilization and Counter-Terrorist Operations*. Canadian Peacekeeping Press. [Consulta:2026]. Disponible en: https://www.abebooks.co.uk/Cornwallis-Group-Analysis-Stabilization-Counter-Terrorist-Operations/31907322697/bd

Ritter, C. (2018). NATO School Crisis Management Exercise Scenario [en línea]. En: 18th International Kyiv Week "Reshaping NATO's Porture for 21th Century Challnge". Course Guide. NATO Defense College, NATO School Oberammergau y Universidad Nacional de Defensa de Ucrania. [Consulta: 2026]. Disponible en: https://nuou.org.ua/assets/documents/booklet-int-week-eng-2018.pdf

Ruestchmann, P. (2022). Applying AI and Automation to Wargaming: An Overview of Opportunities with a Focus on Intelligent Components [en línea]. En: NATO Analytical War Gaming – Innovative Approaches for Data Capture, Analysis and Exploitation. Final Report of the Research Task Group SAS-139. STO-TR-SAS- 139. NATO Science and Technology Organization. [Consulta: 2026]. Disponible en: https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-SAS-139/$$TR-SAS-139-ALL.pdf

Ruiz López, C., (2021). *Métodos cuantitativos de ayuda a la decisión*. Zaragoza, Universidad de Zaragoza.

Roberts, J., Moore, K. y Fischer, D. (2024). Do Large language models learn humans-like strategic preferences? [en línea] Tennessee, Vanderbilt University. Disponible en: https://arxiv.org/pdf/2404.08710

Russell, S. y Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*. Pearson.

Saaty, T. L. (1980). The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. Nueva York, McGraw-Hill (Decision Making Series).

Sáez, J. E. (2023). Interacción de un estado mayor en el proceso de planeamiento operacional [en línea]. Revista Fuerza Aérea-EUA. 5(1), pp. 29-36. [Consulta: 2026]. Disponible en: https://www.airuniversity.af.edu/Portals/10/JOTA/journals/Volume-5_Issue-1/05-Saez_s%20(2).pdf

Scharre, P. (2023). Four Battlegrounds: Power in the Age of Artificial Intelligence. Nueva York, W.W. Norton & Co.

Schmitt, J. F. (2015). A Practical Guide for Developing and Writing Military Concepts. En*: U.S. Army Command and General Staff College Press, Art of War Papers*. Fort Leavenworth, U.S. Army Combined Arms Center.

Scott, B. y Michell, A. (2023). Enhancing Situational Understanding through Integration of Artificial Intelligence in Tactical

Headquarters. *Military Review*. Army University Press, pp. 74-83.

Sokri, A. (2022). How and When Game Theory Can Be Used for Wargaming [en línea]. En: NATO Analytical War Gaming – Innovative Approaches for Data Capture, Analysis and Exploitation. Final Report of the Research Task Group SAS-139. STO-TR-SAS-139. NATO Science and Technology Organization. [Consulta: 2026]. Disponible en: https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-SAS-139/$$TR-SAS-139-ALL.pdf f

Soler, D. (2024). ¿Qué es el refinamiento iterativo en los modelos de lenguaje? [en línea]. KeepCoding. [Consulta: 2026]. Disponible en: https://keepcoding.io/blog/que-es-el-refinamiento-iterativo

Svoboda, I. y Lande, D. (2024). Enhancing Multi-Criteria Decision Analysis with AI: Integrating Analytic Hierarchy Process and GPT-4 for Automated Decision Support [en línea]. arXiv:2402.07404v1 [cs.AI]. [Consulta: 2026]. Disponible en: https://arxiv.org/abs/2402.07404

Swedish Armed Forces International Centre (Swedint). (2016). *Handbook: Excerpts of UN Country Report* [material docente; escenario ficticio de Constellatia]. Kungsängen: Swedish Armed Forces International Centre].

Tarraf, D. C. et al. (2020). An Experiment in Tactical Wargaming with Platforms Enabled by Artificial Intelligence [en línea]. Santa Mónica, RAND Corporation. [Consulta: 2026]. Disponible en: https://www.rand.org/pubs/research_reports/RRA423-1.html

Tinnirello, M. (2018). Offensive Realism and the Insecure Structure of the International System: Artificial Intelligence and Global Hegemony [en línea]. En: Artificial Intelligence Safety and Security. Taylor & Francis. [Consulta: 2026]. Disponible en: https://www.academia.edu/download/61798975/AI_and_the_insecure_structure_of_the_international_system20200115-3603-6mns66.pdf

UK MoD. (2021). Allied Joint Doctrine for the Planning of Operations. Edition B, Version 1 [en línea]. Ministry of Defence. [Consulta: 2026]. Disponible en: https://assets.publishing.service.gov.uk/media/6054d017e90e0724be025a8f/20210310-AJP_5_with_UK_elem_final_web.pdf

US Army. (2023). Military Decision-Making Process (MDMP) [en línea]. Center for Army Lessons Learned [Consulta: 2026]. Disponible en: https://api.army.mil/e2/c/downloads/2023/11/17/f7177a3c/23-07-594-military-decision-making-process-nov-23-public.pdf

US Army War College. (2023). *Campaign Planning Handbook: Academic Year 2023* [en línea]. [Consulta: 2026]. Disponible en: https://usawc-ssi-media.s3.us-east-1.amazonaws.com/misc/AY24-Campaign-Planning-Handbook.pdf

US DoD. (2018). Summary of the 2018 Department of Defense Artificial Intelligence Strategy [en línea]. Washington, D.C., Department of Defense. [Consulta: 2026]. Disponible en: https://media.defense.gov/2019/feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf

—. (2023). Data, Analytics, and Artificial Intelligence Adoption Strategy [en línea]. Washington, D.C., Department of Defense. [Consulta: 2026]. Disponible en: https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

Vafaei, N., Ribeiro, R. A., y Camarinha-Matos, L. M. (2020). Selecting Normalization Techniques for the Analytical Hierarchy Process [en línea]. En: 11th Doctoral Conference on Computing, Electrical and Industrial Systems (DoCEIS). Costa de Caparica, pp. 43-52. [Consulta: 2026]. Disponible en: https://inria.hal.science/hal-03741563/document

Vargas, R. V. (2010). Using the analytic hierarchy process (ahp) to select and prioritize projects in a porfolio. Paper presented at PMIR Global Congress 2010. Washington D. C., Newtown Square, Project Management Institute.

Vargas, L. G. (2021). Understanding the Analytic Hierarchy Process [en línea]. Technometrics. 63(4), pp. 400-411. [Consulta: 2026]. Disponible en: https://www.tandfonline.com/doi/full/10.1080/00401706.2021.1904744

Vestner, T. (2024). From Strategy to Orders: Preparing and Conducting Military Operations with Artificial Intelligence [en línea]. En: Geiß, R. y Lahmann, H. (eds.). Research Handbook on Warfare and Artificial Intelligence. Edward Elgar Publishing. [Consulta: 2026]. Disponible en: https://dam.gcsp.ch/files/misc/military-operations-working-paper-v2

Williams, B. S. (2011). Heurísticas y sesgos en la toma de decisiones militares [en línea]. Military Review. Army University

Press, pp. 52-64. [Consulta: 2026]. Disponible en: https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20110228_art009SPA.pdf

Wong, Y. H. et al. (2019). Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action [en línea]. Santa Mónica, RAND Corporation. [Consulta: 2026]. Disponible en: https://www.rand.org/pubs/research_reports/RR2227.html

Yongfu, Z., Yang, L. y He, Y. (2024). Un método para la identificación de nodos clave en un sistema de objetivos operacionales basado en juegos de guerra [en línea]. Revista de Simulación de Sistemas. 36(11), pp. 2654-2661. [Consulta: 2026]. Disponible en: https://www.china-simulation.com/EN/10.16182/j.issn1004731x.joss.23-0947

Capítulo noveno

Capacidades militares de Arabia Saudí para la defensa de infraestructuras críticas en su litoral marítimo

Patricio Adrián Alisi

Resumen

La seguridad de las infraestructuras críticas asociadas al sistema energético saudí se ha convertido en un factor central del equilibrio estratégico en Oriente Medio. La elevada dependencia del Reino de activos situados en su franja costera, así como de corredores marítimos esenciales para el comercio global, lo expone de manera particular a amenazas asimétricas y a dinámicas de guerra por delegación. En este contexto, actores estatales y no estatales han demostrado la capacidad de generar efectos estratégicos significativos mediante acciones desarrolladas en la denominada zona gris.

El trabajo analiza el entorno de seguridad regional en el que opera Arabia Saudí, prestando especial atención a la rivalidad con Irán y al papel del movimiento hutí como vector de presión indirecta. A partir de este marco, se examina la evolución del instrumento militar saudí desde 2016, en particular en los dominios naval, aéreo, antimisiles y cibernético, y su contribución a la protección de activos estratégicos y rutas marítimas clave.

El estudio concluye que Arabia Saudí ha avanzado hacia una postura disuasiva más integrada y resiliente, aunque persisten

limitaciones estructurales que obligan al Reino a complementar sus capacidades militares con alianzas estratégicas, cooperación internacional y un enfoque multidominio orientado a la protección de intereses vitales en un entorno regional altamente volátil.

Palabras clave

Liderazgo regional, Seguridad energética global, Amenazas híbridas, Disuasión regional, Control del dominio marítimo.

Saudi Arabia's Military Capabilities for the Defence of Critical Infrastructure Along Its Maritime Coastline

Abstract

The security of critical infrastructure associated with the Saudi energy system has become a central factor in the strategic balance of the Middle East. The Kingdom's high dependence on assets located along its coastal strip, as well as on maritime corridors essential to global trade, exposes it in particular to asymmetric threats and to dynamics of proxy warfare. In this context, state and non-state actors have demonstrated the ability to generate significant strategic effects through actions carried out in the so-called grey zone.

This study analyses the regional security environment in which Saudi Arabia operates, paying special attention to its rivalry with Iran and to the role of the Houthi movement as an indirect pressure vector. Building on this framework, it examines the evolution of the Saudi military instrument since 2016—particularly in the naval, air, missile-defence, and cyber domains—and its contribution to the protection of strategic assets and key maritime routes.

The study concludes that Saudi Arabia has progressed toward a more integrated and resilient deterrent posture, although structural limitations persist that compel the Kingdom to complement its military capabilities with strategic alliances, international cooperation, and a multidomain approach aimed at protecting vital interests in a highly volatile regional environment.

Key words

Regional leadership, Global energy security, Hybrid threats, Regional deterrence, Maritime domain control.

Lista de abreviaturas

OTAN	Organización del Tratado del Atlántico Norte.
SAMI	Industria militar árabe.
MMSC	Buques de combate multipropósito.
THAAD	Terminal de defensa de área de gran altitud.
UCAV	Vehículo aéreo de combate no tripulado.
GAMI	Autoridad General de Industrias Militares.

1 Introducción

La protección de las infraestructuras críticas constituye en la actualidad un elemento esencial de la seguridad nacional de los Estados y un factor determinante de la estabilidad regional e internacional. En entornos estratégicos caracterizados por la volatilidad, la creciente competencia entre actores estatales y no estatales y el empleo cada vez más frecuente de estrategias híbridas, la defensa de activos vinculados al ámbito marítimo adquiere una relevancia particular. Esta importancia se ve acentuada cuando dichos activos sustentan funciones económicas, energéticas y logísticas de alcance global, cuya interrupción tendría efectos sistémicos más allá del ámbito estrictamente nacional.

Arabia Saudí ocupa una posición central en este contexto debido a su papel como uno de los principales exportadores mundiales de petróleo, sustentado en infraestructuras críticas situadas en su litoral del golfo Arábigo y del mar Rojo, así como en su dependencia estructural de rutas marítimas clave para el comercio energético internacional. La proximidad de pasos estratégicos como los estrechos de Ormuz y Bab al Mandeb incrementa de manera significativa su exposición a riesgos y amenazas. Desde la perspectiva de la teoría del poder marítimo de Alfred Thayer Mahan, quien afirmaba que «el control de las rutas marítimas y la proyección naval son fundamentales para garantizar el desarrollo económico y la seguridad nacional» (Sumida, 2006), esta realidad explica el interés saudí en ejercer un control implícito sobre dichos puntos geoestratégicos y sobre su entorno marítimo inmediato.

Desde un punto de vista teórico, este análisis se apoya en los conceptos de disuasión y proyección del poder como pilares fundamentales de la estrategia de seguridad contemporánea. La disuasión, entendida no solo en términos nucleares, sino también convencionales, busca elevar los costes potenciales y reducir la probabilidad de éxito de una agresión. Este enfoque resulta especialmente relevante en escenarios regionales marcados por amenazas asimétricas, dinámicas de guerra por delegación[71] y una elevada ambigüedad estratégica. A ello se suma la lógica del control del dominio marítimo, que resalta la importancia de las

[71] Acción donde se apoya militarmente a un gobierno o a un actor armado no estatal en contra de un rival estratégico.

rutas de comunicación marítima, la libertad de navegación y la presencia naval sostenida como instrumentos clave para garantizar tanto la seguridad nacional como la estabilidad económica.

En ese orden de ideas, la evolución del entorno de seguridad regional, marcada por la rivalidad estratégica con Irán y por la actuación de actores delegados como la milicia hutí en Yemen, ha puesto de manifiesto la vulnerabilidad de estas infraestructuras frente a amenazas asimétricas, ataques de precisión y operaciones en la denominada zona gris[72]. Los ataques contra instalaciones energéticas, así como el hostigamiento al tráfico marítimo comercial, han evidenciado la necesidad de superar enfoques defensivos tradicionales y de avanzar hacia una arquitectura de seguridad más integrada, resiliente y de características multidominio.

En respuesta a este escenario, Arabia Saudí ha impulsado desde 2016 un proceso sostenido de transformación de sus capacidades militares, enmarcado en los objetivos de la Visión 2030. Este plan estratégico, como señala el Gulf Research Centre (2023: 14),

> «abre el Reino al mundo particularmente en la asociación con organizaciones internacionales para implementar industrias militares a nivel local, invirtiendo en materiales disponibles y capacitación de empleados para liderar los procesos de investigación y desarrollo».

En este contexto, dicho proceso ha otorgado una atención prioritaria a la defensa del litoral marítimo y a la protección de infraestructuras críticas mediante la modernización de las fuerzas navales, el refuerzo de la defensa aérea y antimisiles, el desarrollo de capacidades de vigilancia, inteligencia y reconocimiento, así como la consolidación de alianzas estratégicas con socios internacionales.

El presente artículo examina estas capacidades desde una perspectiva estratégica y operacional, analizando en qué medida la evolución del instrumento militar saudí contribuye a la protección de infraestructuras críticas en su entorno marítimo y a la construcción de una postura disuasiva creíble frente a amenazas estatales y no estatales. El objetivo es ofrecer una aproximación analítica y divulgativa que permita comprender el papel de la defensa marí-

[72] La «zona gris» hace referencia a un ámbito entre la paz y la guerra donde se emplean tácticas no convencionales (como ciberataques, propaganda o guerra por delegación) para influir sin desencadenar un conflicto abierto.

tima saudí tanto en el equilibrio de seguridad regional como en la preservación de la seguridad energética internacional.

2 Dialéctica de voluntades entre Arabia Saudí, Irán y los rebeldes hutíes

2.1 La proyección asimétrica de la amenaza hutí y su impacto sobre la seguridad estratégica saudí

La intervención militar saudí en Yemen en 2015 alteró de manera sustancial el equilibrio de fuerzas del conflicto, al debilitar de forma significativa la capacidad ofensiva convencional de los rebeldes hutíes asentados principalmente en la región de Sa'dah. Esta presión militar obligó a dichos actores a adaptar sus métodos operativos, evolucionando desde una confrontación limitada al espacio territorial yemení hacia una doctrina de proyección ofensiva más allá de sus fronteras, dirigida tanto contra objetivos situados en territorio saudí como contra infraestructuras y líneas de navegación en su entorno marítimo inmediato.

Así mismo, la persistente inestabilidad en dicha nación continúa representando una amenaza directa para la seguridad del Reino de Arabia Saudí. Así lo señalan diversos analistas y responsables militares de la región, quienes advierten sobre el progresivo incremento de la capacidad de las milicias hutíes para atacar infraestructuras y perturbar el tráfico marítimo en áreas de elevado valor estratégico. Con el paso del tiempo, esta amenaza se ha materializado en acciones de carácter claramente asimétrico, planificadas con cuidado y ejecutadas en momentos de especial sensibilidad política o mediática para el Reino.

De hecho, numerosos ataques se produjeron en fechas próximas a eventos internacionales relevantes organizados por Arabia Saudí, lo que sugiere una planificación orientada no solo a provocar daños materiales, sino también a generar un impacto psicológico significativo y una amplia repercusión internacional. Esta lógica se manifiesta, asimismo, en la naturaleza y el alcance de los medios empleados, ya que se ha documentado el uso de drones de largo alcance y misiles balísticos capaces de alcanzar objetivos situados a cientos de kilómetros del punto de lanzamiento, incluyendo instalaciones energéticas, zonas urbanas y nodos logísticos clave. La literatura especializada aporta evidencia concreta de estas capacidades, pues Michael Tanchum

(2019: 2) subraya que «para los ataques del 2019 contra las dos estaciones de bombeo de la refinería de Saudi Aramco se utilizaron drones con un alcance de hasta 1.400 kilómetros», mientras que Hariyani *et al*. (2022: 123) remarcan que «en 2021, sobre la ciudad de Jazan, se emplearon misiles balísticos y drones, armas que inclusive provocaron incendios en una universidad local».

Aunque, en apariencia, estas hostilidades podrían interpretarse como un enfrentamiento bilateral entre Arabia Saudí y los rebeldes hutíes, un análisis estratégico más profundo revela la intervención de un tercer actor fundamental: la República Islámica de Irán. Si bien Teherán no ha reconocido oficialmente un apoyo directo a las milicias hutíes, existen múltiples indicios que apuntan a su implicación indirecta, entre ellos el empleo de armamento de fabricación iraní y la interceptación de cargamentos de misiles, cohetes y explosivos con destino a Yemen, procedentes tanto de territorio iraní como de rutas marítimas asociadas.

Este esquema responde a una lógica de guerra por delegación, mediante la cual Irán proyecta su influencia regional a través de actores no estatales, reduciendo los costes políticos y militares de una confrontación directa. Para Arabia Saudí, esta dinámica incrementa de forma notable la complejidad de su entorno de seguridad, al combinar amenazas estatales y no estatales dotadas de capacidades tecnológicas cada vez más sofisticadas.

En este contexto, las infraestructuras críticas saudíes, en particular aquellas vinculadas al sector energético y al litoral marítimo, adquieren una relevancia estratégica prioritaria. La vulnerabilidad ya demostrada de estos activos, junto con el considerable impacto económico de alcance global que puede derivarse de su afectación, los convierte en objetivos de alto valor dentro de una dialéctica de confrontación estratégica. Dicha dinámica puede entenderse como una interacción deliberada entre actores estatales y no estatales orientada a influir en la conducta del adversario mediante señales y acciones dotadas de significado político. En este sentido, y como parte del Método de Toma de Decisiones en Condiciones de Incertidumbre, Cal *et al*. (2016: 31) conceptualizan este tipo de interacciones como «procesos comunicativos en los que las acciones funcionan como mensajes: entre aliados, para coordinar posiciones, y entre adversarios, para disputar intereses y negociar el equilibrio del conflicto».

Para Arabia Saudí, esta realidad configura un desafío de carácter estructural: la necesidad de proteger intereses vitales frente a

amenazas persistentes que se sitúan deliberadamente por debajo del umbral del conflicto convencional. Esta presión constante obliga al Reino a concebir su estrategia de seguridad no como una respuesta puntual o episódica, sino como un proceso continuo de adaptación, en el que la protección de las infraestructuras críticas y la defensa del espacio marítimo adquieren una centralidad creciente.

2.2 Intereses estratégicos y racionalidad de Arabia Saudí

Para comprender la respuesta saudí frente a este entorno de amenazas, resulta imprescindible analizar la estructura de intereses que orienta su proceso de toma de decisiones. A partir del estudio de su conducta política, de las declaraciones oficiales y de las acciones emprendidas por el Reino, pueden identificarse dos intereses estratégicos de máxima jerarquía que condicionan su comportamiento en el ámbito regional y de seguridad.

El primero de ellos es la consolidación de una posición de liderazgo regional. Arabia Saudí aspira a ejercer una hegemonía reconocida en Oriente Medio que le permita proteger sus intereses nacionales y desempeñar un papel central en la gestión y resolución de disputas interestatales. Esta ambición se manifiesta en una densa red de alianzas internacionales, entre las que destacan su relación estratégica con Estados Unidos, una cooperación económica y tecnológica cada vez más estrecha con China y una política exterior marcadamente pragmática, caracterizada por apoyos diferenciados en escenarios de elevada complejidad, como el persistente conflicto entre Israel y Palestina. En este sentido, la intervención militar en Yemen debe entenderse también como un instrumento orientado a reforzar dicho estatus regional y a proyectar capacidad de liderazgo más allá de sus fronteras inmediatas (Muhammad Lukman, 2024: 509).

Esta concepción amplia del liderazgo regional y explica por qué Riad interpreta cualquier amenaza dirigida contra sus infraestructuras energéticas como un desafío directo a su posición estratégica. Los ataques contra refinerías, puertos, plantas desalinizadoras o nodos logísticos clave no son percibidos únicamente como agresiones de carácter táctico, sino como intentos deliberados de erosionar su credibilidad, su capacidad de disuasión y su imagen como garantizador de la estabilidad regional.

Asimismo, la centralidad de este interés condiciona la evaluación saudí de los riesgos asociados a una posible escalada militar. La

estrecha interdependencia entre seguridad, estabilidad económica y legitimidad internacional induce al Reino a adoptar una postura generalmente prudente, evitando conflictos abiertos de alta intensidad que puedan comprometer sus objetivos de desarrollo a largo plazo, en particular, aquellos vinculados al ambicioso programa de reformas estructurales recogido en la Visión 2030[73].

El segundo interés estratégico fundamental es la construcción de un entorno regional más estable y previsible. En esta línea, Mnekhir (2023: 104) subraya que «en los últimos años, el Reino saudí ha impulsado acercamientos diplomáticos y, de manera puntual, militares con el régimen de los ayatolás, como parte de un esfuerzo más amplio orientado a la pacificación de Oriente Medio». Este enfoque combina iniciativas diplomáticas con el refuerzo de alianzas regionales e internacionales, sin renunciar al fortalecimiento de sus capacidades militares defensivas como elemento disuasorio frente a amenazas persistentes.

Junto con estos intereses estratégicos primarios, Arabia Saudí mantiene una serie de intereses de menor jerarquía, aunque estrechamente vinculados a su seguridad nacional. Entre ellos, y como se refleja en la tabla 1, destacan la producción y comercialización de hidrocarburos, la diversificación económica promovida por la Visión 2030, la protección de las infraestructuras críticas y la garantía de la seguridad del recurso hídrico, particularmente relevante en un contexto de vulnerabilidad climática y demográfica.

En lo que respecta a las infraestructuras estratégicas, su protección constituye un eje central de la política de defensa saudí y se traduce en un incremento sostenido de capacidades militares. Este esfuerzo responde a la necesidad de obtener resultados concretos frente a amenazas reales y recurrentes, y refleja un enfoque de disuasión convencional orientado a contrarrestar tanto a actores estatales como no estatales, incluso en un entorno regional caracterizado por la proliferación de capacidades operativas avanzadas y la creciente posibilidad de actuación en entornos multidominio.

Finalmente, y a pesar del progresivo reequilibrio del interés estratégico estadounidense hacia la región del Indo-Pacífico,

[73] La Visión 2030 de Arabia Saudí es un proyecto que apunta al desarrollo de la industria no petrolera del país para reducir la dependencia excesiva de los productos derivados del petróleo (Alam *et al., 2023)*.

Arabia Saudí continúa apoyándose en una sólida red de alianzas con su principal socio estratégico y con diversos países miembros de la OTAN. Esta arquitectura de seguridad sustenta, además, su apuesta por el desarrollo de una industria de defensa nacional, concebida no solo como un instrumento de autonomía estratégica, sino también como un pilar para asumir un papel de liderazgo en el sector de la defensa a escala global de cara al horizonte 2030 (Wezeman, 2018).

INTERESES			
Nombre del interés	**Descripción**	**Jerarquía**	**Orden**
Hegemonía regional	Dominio saudí en la región	Mayor	1
Estabilidad regional	Situación de equilibrio y paz en Medio Oriente	Mayor	2
Hidrocarburos	Producción y comercialización de petróleo	Menor	3
Plan Visión 2030	Plan integral económico reduciendo dependencia del petróleo	Menor	4
Infraestructuras críticas	Defensa de infraestructuras vitales para la nación	Menor	5
Recurso hídrico	Gestión de recurso escaso	Menor	6
Gobierno yemení	Intervención contra grupo Hutí	Menor	7
Incremento poder militar	Adquisición de armamento	Menor	8
Líneas marítimas	Libre navegación marítima en mares y estrechos aledaños	Menor	9
Relaciones con EE.UU. Y China	Mantenimiento de relaciones con países hegemónicos	Menor	10
Relaciones con Israel	Mantenimiento de Status Quo regional	Menor	11
Consejo de Cooperación del Golfo	Alianza política y económica regional	Menor	12

Tabla 1. Intereses mayores y menores de Arabia Saudí. Fuente propia

2.3 Intereses estratégicos y racionalidad de Irán

Por su parte, y como se detalla en la tabla 2, la racionalidad estratégica iraní se articula en torno a dos intereses estratégicos de máxima jerarquía que condicionan de forma estructural su comportamiento regional y su interacción con Arabia Saudí. El análisis de su discurso político, de su doctrina de seguridad y de sus patrones de actuación permite identificar con claridad estos ejes fundamentales de su toma de decisiones.

El primero de ellos es la aspiración a ejercer una hegemonía regional, en abierta competencia con Arabia Saudí por el lide-

razgo político y religioso en Oriente Medio. Esta rivalidad hunde sus raíces en factores históricos, ideológicos y confesionales y se ha intensificado desde la revolución islámica de 1979. De Carlos (2021: 13) señala que «tras la caída del Sha de Persia, ambos países mantienen una rivalidad sostenida por el liderazgo regional, basada en dos interpretaciones opuestas del islam», lo que ha contribuido a configurar una confrontación de carácter estructural y de largo plazo.

Un pilar central de esta ambición hegemónica es la demostración de fuerza, estrechamente vinculada a la lógica de la disuasión estratégica, incluida su dimensión nuclear. La ambigüedad deliberada que rodea al programa nuclear iraní actúa como un multiplicador de poder, permitiendo a Teherán disuadir tanto a adversarios regionales como extrarregionales, al tiempo que refuerza su capacidad de negociación frente a presiones diplomáticas, económicas o militares procedentes del exterior. Esta estrategia persigue, además, elevar el umbral de respuesta de sus oponentes y limitar su margen de maniobra en escenarios de escalada controlada.

El segundo interés estratégico fundamental de Irán es la expansión de su influencia ideológica y política en el entorno regional. Este objetivo se sustenta en la diseminación del islam chií[74] y en la promoción de un modelo revolucionario que trasciende las fronteras nacionales y cuestiona el orden regional existente. En este sentido, Moniri, Fallahzadeh y Eftekhari (2020: 107) sostienen que «la base de este proceso consiste en difundir una idea de revolución que conducirá a la salvación de todas las naciones». La materialización de este interés se produce, de manera preferente, a través del apoyo sostenido a actores no estatales afines, que operan como instrumentos de proyección indirecta de poder y como vectores de influencia en múltiples escenarios geopolíticos.

Junto con estos intereses estratégicos primarios, Irán mantiene una serie de intereses y capacidades de menor jerarquía que, en conjunto, representan amenazas directas o indirectas para la seguridad saudí y, en particular, para la protección de sus infraestructuras críticas. Entre ellos, destacan el desarrollo y perfeccionamiento de su programa nuclear, el liderazgo, financiación

[74] La diseminación ideológica chií hace referencia a la estrategia de Irán de expandir su influencia mediante la promoción de su modelo teocrático y lazos religiosos en países de mayoría o presencia chiita.

y adiestramiento de grupos armados aliados, la conducción de conflictos por delegación y la ejecución de operaciones cibernéticas de carácter ofensivo contra objetivos estatales y no estatales.

En lo que respecta al empleo de estas últimas capacidades, Irán tiende a operar deliberadamente en un espacio de ambigüedad estratégica situado por debajo del umbral del conflicto armado convencional, es decir, dentro de la zona gris. En este ámbito, Teherán recurre a operaciones asimétricas, encubiertas o de baja atribución que le permiten imponer costes graduales a sus adversarios, erosionar su percepción de seguridad y preservar la negación plausible de su implicación directa, evitando así una confrontación abierta que podría resultar política, económica y militarmente excesiva.

INTERESES			
Nombre del interés	**Descripción**	**Jerarquía**	**Orden**
Hegemonía regional	Dominio iraní en la región	Mayor	1
Revolución islámica	Exportación ideología islámica Chií	Mayor	2
Programa nuclear	Enriquecimiento de uranio para fines bélicos	Menor	3
Gas y petróleo	Producción y comercialización de gas y petróleo	Menor	4
Liderazgo grupos rebeldes	Apoyo a Hamás y Hutíes	Menor	5
Recurso hídrico	Gestión de recurso escaso	Menor	6
Eliminación Israel	Eliminación del Estado para beneficio palestino	Menor	7
Relaciones con Rusia y China	Mantenimiento de relaciones con paises hegemónicos	Menor	8
Control Estrecho Ormuz	Control de líneas de comunicación marítima	Menor	9
Guerra proxy	Empleo de Hutíes contra Arabia Saudí	Menor	10
Ciberataques ofensivos	Empleo ciberespacio como herramienta de desestabilización geopolítica	Menor	11
BRICS	Alianza política y económica	Menor	12

Tabla 2. Intereses mayores y menores de Irán. Fuente propia

2.4 Intereses estratégicos y racionalidad Hutí

La racionalidad estratégica del movimiento rebelde hutí, conocido como Ansar Allah, se articula en torno a un interés central claramente definido: la aspiración de ejercer el liderazgo político de Yemen desde una perspectiva chií, alineada ideológica y estra-

tégicamente con el modelo promovido por la República Islámica de Irán. En este sentido, Lukman (2024: 516) destaca que «su único plan es convertir a dicha nación en un Estado revisionista tal como lo es la República de Irán». De este modo, el grupo no se limita a la mera disputa por el poder interno, sino que persigue una transformación profunda y estructural del Estado yemení, orientada a alterar de manera sostenida el equilibrio regional existente.

Este objetivo estratégico principal, y como se visualiza en la tabla 3, se ve reforzado por una serie de intereses secundarios que consolidan y sostienen sus planes de actuación. Entre ellos, destacan la difusión de la ideología chií zaidí en distintos espacios de Oriente Medio, los beneficios económicos derivados del control de rutas comerciales y recursos vinculados al tráfico y comercio del petróleo, la posesión, administración y defensa de territorio dentro de Yemen y la estrecha relación política, logística y paramilitar mantenida con Irán. En conjunto, estos elementos configuran una compleja red de incentivos políticos, económicos y estratégicos que contribuye a la continuidad operativa y a la expansión progresiva del movimiento hutí.

En este proceso, y en un plano de mayor alcance, el grupo rebelde Partidario de Dios u oficialmente Ansar Allah, ha identificado las infraestructuras críticas saudíes como un instrumento particularmente eficaz de presión política y militar. Si bien este objetivo se sitúa en un nivel de interés secundario respecto de sus aspiraciones políticas fundamentales, su relevancia estratégica resulta considerable. La capacidad de amenazar o atacar instalaciones clave del sector energético saudí no solo expresa el rechazo ideológico del grupo hacia el liderazgo suní regional, sino que, además, genera efectos directos sobre la economía del Reino de Arabia Saudí y, por extensión, sobre los mercados internacionales de energía. Tal como subraya Tanchum (2019: 3), «la desarticulación de dichos objetivos claves generaría un impacto tanto local como internacional en lo que a la exportación de crudo respecta», lo que da cuenta de la magnitud y alcance de los efectos que potenciales ataques podrían desencadenar.

La explotación deliberada de esta vulnerabilidad introduce, además, un elemento de disuasión indirecta y de proyección de poder que amplifica el impacto del movimiento hutí más allá del escenario estrictamente yemení. Esta dinámica evidencia una racionalidad estratégica que combina de manera coherente objetivos ideológicos, territoriales y económicos con acciones de alto

impacto regional, reforzando el papel de Ansar Allah como un actor no estatal con una superlativa capacidad de influir en la estabilidad del entorno de seguridad del Golfo.

INTERESES			
Nombre del interés	**Descripción**	**Jerarquía**	**Orden**
Liderazgo Chií en Yemen	Liderazgo chiíta dentro del Estado	Mayor	1
Ideología chiita zaidiya	Diseminación de ideología en Yemen	Menor	2
Petróleo	Beneficios de la importación y exportación del recurso	Menor	3
Territorio	Posesión territorial en Yemen	Menor	4
Apoyo de Irán	Promoción de la revolución árabe	Menor	5
Causa palestina	Defensa de los derechos palestinos contra Israel	Menor	6
Mar rojo y estrecho Bal al Mandeb	Control de líneas de comunicación marítima en apoyo a Hamas	Menor	7
Infraestructuras críticas saudíes	Desarticulación de economía saudí	Menor	8
Guerra Proxi	Materialización intereses propios e iraníes	Menor	9

Tabla 3. Intereses mayores y menores de la milicia hutí. Fuente propia

2.5 Emotividad de los tres actores. Factores y estilos de liderazgo en la toma de decisiones

Además de la racionalidad estratégica basada en intereses y objetivos, la conducta de los Estados y actores no estatales en escenarios de alta tensión se encuentra fuertemente condicionada por factores emocionales y perceptivos. Estos elementos influyen de manera directa en la disposición a escalar o desescalar un conflicto y permiten comprender por qué actores con capacidades similares adoptan comportamientos estratégicos diferenciados frente a amenazas análogas.

Desde esta perspectiva, el análisis del comportamiento estratégico puede apoyarse en tres variables fundamentales, que, como Cal *et al.* (2016: 90) subrayan, permiten clasificar a los actores como halcones[75] o palomos[76]. Estas tres variables refieren por un lado al grado de determinación en la toma de decisiones, a

[75] Los halcones atribuyen valores altos a los intereses de jerarquía mayor propios con tendencia a la imposición, buscando el dominio de la cuestión estratégica.

[76] Los palomos se comportan contrariamente a los halcones, con tendencia a la negociación.

la aversión al riesgo frente a las posibles consecuencias de una acción y finalmente al nivel de empatía estratégica, entendida como la capacidad de anticipar la reacción del adversario y de considerar sus intereses, percepciones y líneas rojas.

En el caso de Arabia Saudí, el examen de estas variables revela un patrón de comportamiento propio de un actor tipo palomo, caracterizado por una elevada determinación política, combinada con una marcada aversión al riesgo y una significativa capacidad de empatía estratégica. Esta combinación configura a un actor que, si bien está dispuesto a emplear el poder militar para defender sus intereses vitales, muestra una clara preferencia por evitar escaladas incontroladas que puedan derivar en conflictos regionales abiertos de alta intensidad.

En detalle, la elevada determinación saudí se manifiesta en su disposición a intervenir militarmente cuando percibe amenazas directas a su seguridad nacional, como ocurrió en Yemen, así como en su sostenido esfuerzo por modernizar y ampliar sus capacidades defensivas. Cerioli (2023: 288) recalca que «la guerra en Yemen desde 2015 y el masivo plan de reforma socioeconómica de la Visión 2030 son claros ejemplos de esta actitud proactiva». No obstante, esta firmeza se ve equilibrada por una alta aversión al riesgo, especialmente en lo relativo a daños colaterales, impactos económicos y repercusiones internacionales que puedan afectar su imagen, su estabilidad interna o su papel como proveedor energético global.

Asimismo, Arabia Saudí ha evidenciado una creciente empatía estratégica, reflejada en su disposición a articular el uso de la fuerza con iniciativas diplomáticas orientadas a la reducción de tensiones, incluso con adversarios históricos. En este marco, la monarquía saudí ha desarrollado vínculos con Israel con impacto en el orden regional (Nawaz, 2022: 178), así como procesos de acercamiento a Qatar e Irán, orientados a comprender sus intereses y a promover la estabilidad y la paz en la región (Mnekhir, 2023: 111). Este enfoque persigue preservar márgenes de maniobra política y evitar escenarios de confrontación directa que puedan comprometer sus objetivos de desarrollo a largo plazo.

A diferencia de Arabia Saudí, el Estado iraní presenta un perfil claramente asociado a un comportamiento tipo halcón, caracterizado por una alta determinación, una baja aversión al riesgo y una limitada empatía hacia otros actores, especialmente hacia aquellos que no comparten su visión ideológica y estratégica.

La determinación iraní se manifiesta en su disposición a implicarse de forma activa y sostenida en escenarios de conflicto cuando estos favorecen la expansión de su influencia política, militar y religiosa. Teherán actúa con firmeza cuando percibe que sus objetivos geopolíticos pueden verse reforzados, apoyando a actores afines y promoviendo dinámicas de confrontación indirecta que consoliden su papel como potencia regional (Paunic, 2016: 85).

Al mismo tiempo, Irán muestra una reducida aversión al riesgo. La percepción de que su capacidad disuasoria, particularmente en el ámbito nuclear, actúa como freno a posibles agresiones externas le permite asumir costes y riesgos que otros Estados evitarían. Esta confianza relativa disminuye su temor a una escalada directa, al considerar que el precio de un conflicto abierto resultaría excesivamente elevado para sus adversarios.

Por último, la política exterior iraní evidencia una baja empatía estratégica hacia el resto de actores regionales, especialmente hacia aquellos que no comparten su proyecto ideológico (González Gómez del Miño, 2019: 191). Esta escasa consideración por los intereses ajenos refuerza una conducta pragmática y confrontativa, en la que prevalece la consecución de objetivos propios sobre la búsqueda de consensos duraderos.

Dentro de esta dinámica triangular, y aunque en un espectro más limitado, el movimiento rebelde hutí presenta un comportamiento estratégico con rasgos similares a los de la República Islámica de Irán. Su actuación se caracteriza por una elevada determinación, una baja aversión al riesgo y una escasa empatía estratégica, lo que se traduce en una marcada disposición a asumir costes elevados con tal de infligir daño a sus adversarios. En este sentido, Congosto (2020: 141) sostiene que «el grupo insurgente no teme ante la intervención saudí ni a las coaliciones formadas posteriormente para la operación denominada Tormenta Decisiva, procurando incluso desgastar a estas fuerzas para mantener sus intereses».

Este perfil explica la recurrencia de ataques contra infraestructuras críticas, centros urbanos y líneas de navegación, incluso cuando dichas acciones conllevan un alto riesgo de represalias. Para los hutíes, el empleo de medios asimétricos como drones y misiles cumple no solo una función paramilitar, sino también política y simbólica, al proyectar una imagen de resistencia y capacidad de desafío frente a un adversario tecnológicamente superior.

Por último, el análisis conjunto de los intereses y comportamientos de los actores revela un patrón definido de relaciones estratégicas, en el que Arabia Saudí compite tanto con Irán como con el movimiento hutí, especialmente en términos de liderazgo regional y seguridad. En contraste, Irán y los hutíes mantienen una relación cooperativa basada en intereses estratégicos compartidos y en una lógica de proyección indirecta de poder destinada a limitar la influencia saudí. Este entramado genera un entorno de seguridad volátil, en el que la protección de las infraestructuras críticas saudíes se consolida como eje central de la estrategia nacional frente a dinámicas de competencia interestatal, guerra por delegación y amenazas asimétricas.

Para actores caracterizados por una baja aversión al riesgo, como Irán y el movimiento hutí, la explotación de estas dimensiones emocionales forma parte integral de su doctrina. La selección de objetivos altamente visibles y de elevado impacto mediático responde a una lógica de presión psicológica orientada a erosionar la confianza del adversario en su capacidad de control. Arabia Saudí, consciente de esta dinámica, ha incorporado progresivamente mecanismos de gestión del riesgo y de comunicación estratégica destinados a minimizar el impacto emocional de este tipo de acciones y a preservar la coherencia de su respuesta.

2.6 Equilibrios y asimetrías de poder en el triángulo Arabia Saudí-Irán-hutíes

El análisis de la dialéctica estratégica entre Arabia Saudí, Irán y el movimiento hutí pone de manifiesto una compleja red de relaciones de poder basada en dependencias cruzadas entre intereses mayores y menores. En este contexto, el poder no se expresa únicamente a través de capacidades militares convencionales, sino también mediante la capacidad de condicionar los objetivos estratégicos del adversario y limitar su margen de maniobra.

2.6.1 Relaciones de poder. Arabia Saudí frente a la disuasión nuclear y la proyección indirecta iraní

La relación entre Irán y Arabia Saudí se caracteriza por una asimetría significativa de poder, en la que los, como se visualiza en la tabla 4, intereses estratégicos fundamentales del Reino, en particular el liderazgo regional y la estabilidad de su entorno de seguridad se ven condicionados por la capacidad iraní de emplear

instrumentos de poder de carácter indirecto. Esta dinámica otorga a Teherán una influencia relevante sobre el cálculo estratégico saudí, al limitar su margen de maniobra y reforzar una lógica de disuasión estructural de largo alcance.

Uno de los principales factores explicativos de esta asimetría es la capacidad nuclear iraní, o, más precisamente, la ambigüedad estratégica que rodea a su programa nuclear, la cual actúa como un multiplicador de poder. Este elemento incrementa la percepción de vulnerabilidad saudí frente a un liderazgo regional percibido como potencialmente agresivo y condiciona las decisiones estratégicas de Riad. A ello se suma el liderazgo que ejerce Irán sobre una red de actores no estatales, lo que le permite proyectar poder de manera indirecta, sostenida y con costes limitados, sin asumir los riesgos de una confrontación directa. En conjunto, la ambigüedad nuclear iraní y su influencia sobre grupos armados generan una doble presión sobre los principales intereses estratégicos saudíes, ampliando significativamente el margen de poder iraní en la región. En este sentido, el enriquecimiento de uranio con potenciales fines bélicos adquiere un rol central en la relación bilateral, al profundizar la percepción de amenaza del Reino e incentivar incluso el debate sobre el fortalecimiento de su propia disuasión nuclear (Chen, 2017: 21).

En este marco, las aspiraciones saudíes de consolidar un entorno regional más estable y previsible se ven erosionadas por la actividad de grupos armados apoyados por Irán, particularmente en el escenario yemení. La guerra por delegación desarrollada desde este teatro de operaciones, junto con otros focos de inestabilidad regional, reduce las posibilidades de alcanzar una estabilidad duradera, al menos en el corto y medio plazo, e incrementa la presión constante sobre los activos estratégicos del Reino.

Otro factor relevante en esta relación de poder es el empleo de capacidades cibernéticas ofensivas por parte de Irán, desarrolladas en el ámbito de la zona gris, que permiten infligir daños significativos sin cruzar el umbral del conflicto armado convencional. Para Arabia Saudí, este tipo de amenazas representa un desafío particular debido a su impacto potencial sobre infraestructuras críticas altamente digitalizadas. Un ejemplo paradigmático de esta dinámica fue el ataque cibernético de 2012 contra Saudi Aramco, que inutilizó decenas de miles de sistemas informáticos y evidenció la vulnerabilidad del sector energético frente a operaciones encubiertas. Diversos autores atribuyen este ataque a grupos de mercenarios cibernéticos que facilitan la proyección

de poder iraní en el ciberespacio, como el grupo autodenominado Espada Cortante de la Justicia, responsable también del ataque contra la compañía gasífera qatarí RasGas mediante el uso del virus Shamoon[77], que inutilizó aproximadamente treinta mil ordenadores (Connell, 2014: 7).

No obstante, la relación de poder entre ambos Estados no es completamente unidireccional. Irán también presenta dependencias estratégicas respecto de Arabia Saudí, aunque de menor intensidad. La red de alianzas internacionales del Reino, en particular su relación estratégica con Estados Unidos, su creciente interacción económica con China y su posicionamiento en escenarios regionales clave, limita las aspiraciones iraníes de alcanzar una hegemonía regional sin oposición. Asimismo, la adquisición sostenida de material militar avanzado de origen estadounidense por parte de Arabia Saudí actúa como un factor de contención frente a la proyección de poder iraní, configurando un equilibrio inestable

[77] Shamoon es un *malware* destructivo usado en ataques cibernéticos, particularmente contra empresas energéticas en Oriente Medio. Borra datos de los sistemas infectados,

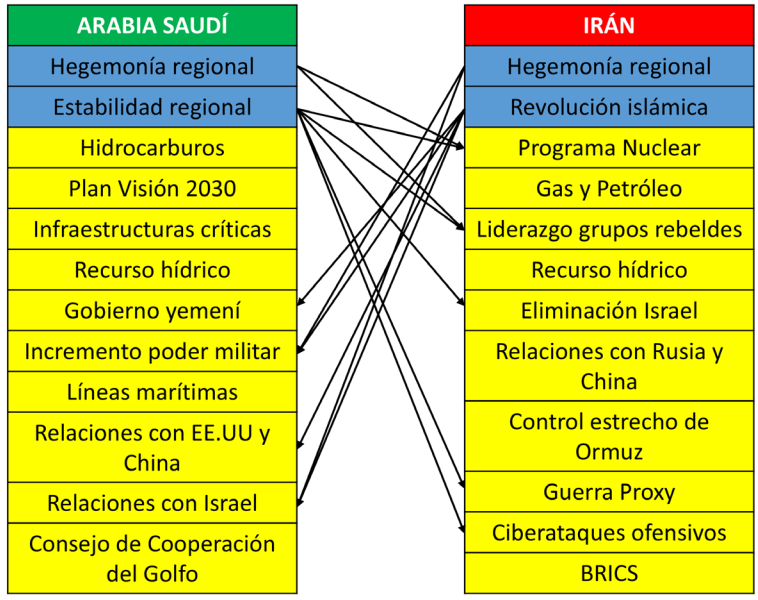


Tabla 4. Relaciones de poder entre Arabia Saudí e Irán. Fuente propia

provocando grandes interrupciones operativas.

que restringe el margen de acción de Teherán en Oriente Medio (Jahandad y Mustafa 2023: 99).

2.6.2 Relaciones de poder entre Arabia Saudí y los hutíes: presión indirecta y vulnerabilidad estratégica

Por su parte, la relación entre Arabia Saudí y el movimiento hutí se inscribe en el marco de un conflicto indirecto y asimétrico, en el que un actor no estatal, respaldado política y militarmente por Irán, ha logrado incrementar de manera progresiva su capacidad de presión sobre una potencia regional consolidada.

Pese a los esfuerzos saudíes por contener y neutralizar a la milicia yemení, las acciones recientes de los hutíes han elevado de forma sensible su capacidad de influencia estratégica. Los ataques dirigidos contra infraestructuras energéticas y, de manera especialmente relevante, contra buques comerciales que transitan por el estrecho de Bab al Mandeb han tenido un impacto directo sobre la seguridad marítima regional y sobre las cadenas globales de suministro, afectando de forma significativa y sostenida a los intereses mayores saudíes.

Esta capacidad de interferir en un punto crítico del comercio internacional otorga al movimiento hutí un poder desproporcionado respecto a su naturaleza no estatal, incrementando la presión estratégica sobre Riad y ampliando los costes económicos, políticos y de seguridad asociados al conflicto.

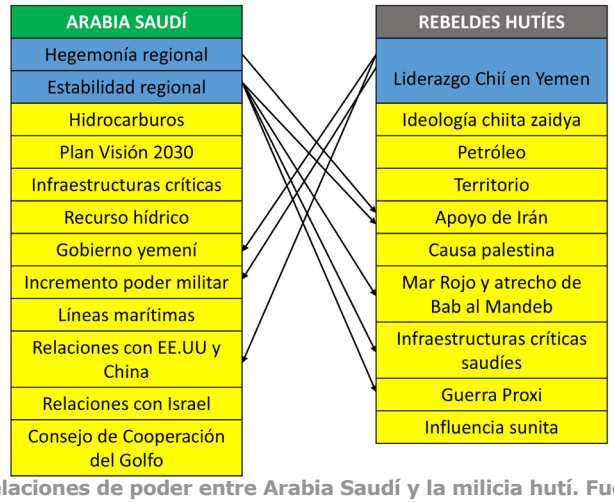


Tabla 5. Relaciones de poder entre Arabia Saudí y la milicia hutí. Fuente propia

Sin embargo, esta relación no es completamente unidireccional. Las capacidades militares saudíes, reforzadas por décadas de inversión en armamento avanzado, así como su objetivo estratégico de promover un gobierno yemení funcional y estable, limitan las aspiraciones hutíes de ejercer un control total y duradero sobre Yemen. Las capacidades militares adquiridas por la nación Saudí en sistemas de armas avanzados particularmente de procedencia estadounidense han facilitado su participación en conflictos regionales que, en cierto grado, pueden inclusive plantear una estrategia de delegación por parte de Estados Unidos, ejecutada a través del Reino saudí frente al principal actor del eje chií (Chen, 2017: 18).

2.6.3 El poder en la alianza Irán-Hutí: cooperación estratégica y guerra por delegación

A diferencia de las relaciones analizadas anteriormente, el vínculo entre Irán y el movimiento hutí se fundamenta en una cooperación estratégica de carácter mutuamente beneficioso. Para Teherán, el apoyo sostenido a Ansar Allah refuerza su liderazgo regional y amplía de forma significativa su capacidad de influencia indirecta en la península arábiga, permitiéndole proyectar poder sin incurrir en los costes de una confrontación directa. Para los hutíes, esta relación proporciona un respaldo financiero, militar e ideológico indispensable para sostener su lucha armada, mantener su cohesión interna y consolidar su control territorial en amplias zonas de Yemen.

Esta interdependencia se articula en torno a una convergencia ideológica de carácter chií y a una serie de intereses estratégicos compartidos, lo que convierte a esta alianza en un elemento central del eje de poder regional liderado por Irán y en un instrumento clave de su estrategia de proyección indirecta.

En resumen, el conjunto de estas dinámicas de poder entre los tres actores da lugar a un sociograma en el que Irán emerge como el actor con mayor capacidad de influencia, seguido por el movimiento hutí en un plano secundario pero efectivo. Arabia Saudí, pese a su considerable peso económico y militar, se ve condicionada por estas relaciones, especialmente en los ámbitos de la seguridad energética, la estabilidad regional y la competencia por el liderazgo político y religioso en Oriente Medio.

Estas circunstancias deben ser consideradas cuidadosamente por el Reino saudí a la hora de diseñar y ajustar sus futuras decisiones

estratégicas, en un entorno regional crecientemente marcado por la competencia indirecta mediante la guerra por delegación y la persistencia de amenazas asimétricas.

2.7 Situación estratégica actual y dinámica del conflicto

Según Cal *et al*. (2016: 114), el nivel actual de la cuestión puede analizarse a partir del concepto de graduación, entendido como una relación bilateral de carácter jerárquico entre los intereses mayores y menores de distintos actores, la cual se manifiesta en la conducta estatal mediante grados que oscilan entre el intercambio, de naturaleza cooperativa, o la imposición, de carácter marcadamente competitivo.

El análisis de los intereses en este escenario competitivo indica que la interacción entre las partes se sitúa en un grado de distracción, caracterizado por la prevalencia de intereses secundarios de Irán y del movimiento hutí que inciden de forma indirecta pero constante sobre los intereses prioritarios de la monarquía saudí. Esta configuración deriva en la adopción de estrategias orientadas a desviar la atención del adversario y a generar confusión en torno a la jerarquía de intereses, enfrentando objetivos de alto valor estratégico de un actor con intereses de menor rango del otro.

En definitiva, y a la luz de este análisis estratégico, en un contexto regional marcado por una relativa contención de los conflictos abiertos, puede afirmarse que, si Irán decidiera avanzar con mayor determinación hacia la consecución de sus intereses estratégicos mayores, sus opciones para debilitar a Arabia Saudí serían limitadas en número, pero potencialmente muy eficaces. En un escenario de este tipo, la reactivación de la guerra por delegación a través de grupos armados aliados y la intensificación de las operaciones en el ciberespacio se perfilan como las alternativas más viables y plausibles.

Ambas líneas de acción se desarrollarían previsiblemente en el ámbito de la zona gris. Irán ha demostrado en numerosas ocasiones su capacidad para operar con soltura en este entorno, delegando la ejecución de acciones hostiles en terceros actores y manteniendo, al mismo tiempo, un margen significativo de negación plausible que dificulta la atribución directa y la respuesta proporcional.

Esta habilidad quedó especialmente demostrada entre 2010 y 2012, cuando la República Islámica respondió a una serie de ciberataques dirigidos contra su programa nuclear y su industria energética, así como a las sanciones económicas impuestas por la comunidad internacional. Durante ese periodo, Teherán lanzó ataques cibernéticos contra instituciones financieras estadounidenses con vínculos con capital saudí, evidenciando su capacidad para emplear el ciberespacio como un instrumento de presión estratégica indirecta, tanto en clave defensiva como ofensiva, y como complemento a otras formas de disuasión.

No obstante, aunque las amenazas asociadas a la guerra por delegación y a las operaciones cibernéticas representan los riesgos más probables para Arabia Saudí, el Reino no puede ignorar el peso de los factores emocionales y de las posturas más radicalizadas presentes en el escenario estratégico regional. En situaciones de alta tensión, los actores caracterizados por una elevada determinación y una baja aversión al riesgo, también denominados halcones, tienden a privilegiar la confrontación y la imposición sobre la contención, incluso cuando ello implica asumir costes elevados y riesgos significativos.

La presencia de este tipo de dinámicas introduce un elemento adicional de incertidumbre en el entorno de seguridad saudí y refuerza la necesidad de disponer de capacidades de defensa robustas, flexibles y capaz de operar en ambientes del multidominio, orientadas principalmente a la protección de infraestructuras críticas y a la seguridad del litoral marítimo, que constituyen objetivos prioritarios en cualquier estrategia de presión indirecta dirigida contra el Reino.

3 Infraestructuras críticas y pasos marítimos del sistema energético saudí

3.1 Vulnerabilidad sistémica y valor estratégico de las infraestructuras energéticas saudíes

El concepto de infraestructura crítica ha adquirido en las últimas décadas una relevancia creciente dentro de los estudios de seguridad y defensa, hasta convertirse en un eje central del análisis estratégico contemporáneo. De Felice, Baffo y Petrillo (2022: 1) definen a las infraestructuras críticas como:

> «los recursos materiales, servicios, sistemas de tecnologías de la información, redes y activos de infraestructura que, de ser dañados o destruidos, causarían graves repercusiones en las funciones cruciales de la sociedad, incluida la cadena de suministro, la salud, la seguridad y el bienestar económico o social del Estado y la población».

En Estados altamente dependientes de sectores estratégicos concretos, como el energético en el caso saudí, esta vulnerabilidad se amplifica y adquiere una dimensión sistémica.

A diferencia de otros activos militares, las infraestructuras críticas presentan una doble condición: son indispensables para el funcionamiento del Estado y, al mismo tiempo, intrínsecamente vulnerables debido a su visibilidad, localización fija y dependencia tecnológica. Esta combinación las convierte en objetivos preferentes dentro de estrategias híbridas y de guerra por delegación, donde actores estatales y no estatales buscan maximizar el impacto con recursos limitados.

En el ámbito marítimo, esta vulnerabilidad se ve reforzada por la concentración espacial de instalaciones estratégicas y por la dependencia de corredores de tránsito estrechos. La defensa de estas infraestructuras, por tanto, exige un enfoque integral que combine capacidades militares, medidas de protección física, sistemas de vigilancia y cooperación internacional.

En particular, la posición geográfica del Reino, entre el golfo Arábigo y el mar Rojo, le otorga una ventaja geoeconómica excepcional. Desde sus costas, se articula una densa red de puertos, refinerías, plantas industriales y tendidos submarinos que sostienen su condición de principal exportador mundial de petróleo. Sin embargo, esa misma centralidad convierte a estas infraestructuras en objetivos estratégicos especialmente sensibles en un entorno regional volátil.

A esta vulnerabilidad estructural se suma la dependencia de dos pasos marítimos críticos: el estrecho de Ormuz y el estrecho de Bab al Mandeb. Ambos actúan como auténticas vías del comercio energético global, conectando las costas saudíes con los principales mercados internacionales. De igual manera, cualquier interrupción en estos corredores tendría un impacto inmediato sobre el tráfico marítimo, las cadenas logísticas y los precios de la energía.

En particular, el estrecho de Bab al Mandeb se ha convertido en un foco creciente de inestabilidad. Desde sus márgenes, el movimiento hutí ha intensificado acciones de hostigamiento contra buques civiles mediante drones y misiles, obligando a numerosas navieras a modificar rutas y generando disrupciones a escala global.

En este contexto, la protección de las infraestructuras críticas saudíes y de dichas arterias marítimas, no puede entenderse como un desafío abstracto o meramente técnico, sino como una cuestión central de seguridad nacional con implicaciones regionales y globales. La combinación de alta dependencia energética, exposición marítima y presión de actores hostiles configura un entorno en el que cada instalación adquiere un valor estratégico singular.

3.2 La arquitectura energética de las costas saudíes

En el sector oriental del país, se concentran algunas de las instalaciones más relevantes del sistema energético mundial. Entre ellas, destaca el complejo portuario y de refinado de Ras Tanura, la mayor terminal petrolera del planeta. Desde este enclave, se procesan y exportan hasta 6,5 millones de barriles diarios, una cifra equivalente a cerca del 7 % de la demanda mundial de crudo. Para dimensionar su magnitud, Ras Tanura puede exportar en poco más de tres semanas un volumen similar al total anual de productos petrolíferos exportados por países industrializados de tamaño medio. Como referencia y según datos obtenidos de Statista (2025) en el año 2023 el Reino de España exportó aproximadamente 20,9 millones de toneladas de productos petrolíferos, que equivale a un poco más de 131,4 millones de barriles en un año, lo que lleva a concluir que Tanura posee la capacidad de alcanzar ese número en tan solo veintidós días.

Más al norte, en la ciudad de Jubail, se encuentra el Puerto Industrial Rey Fahd, considerado el mayor *hub*[78] industrial de Oriente Medio. Este complejo alberga refinerías de última generación como SATORP y SASREF, capaces de procesar conjuntamente más de 750 000 barriles diarios Satorp (2024). Su importancia no reside solo en el volumen de producción, sino en su papel dentro de la estrategia saudí de diversificación económica y de

[78] Denominación que se le otorga a un centro logístico dedicado a gestionar todas las operaciones vinculadas al transporte, organización, envío y distribución de productos, tanto a nivel nacional como internacional.

generación de productos de alto valor añadido, en línea con los objetivos de la Visión 2030.

A estos nodos se suma el puerto de Ras Al-Khair, inaugurado en 2016 y concebido como el puerto industrial más moderno del país. En su portal, Basenton (2023) expresa que

> «el puerto cuenta con catorce atracaderos y con una capacidad de exportación que alcanza los 35 millones de toneladas de diversos productos, dotado además de tecnología de vanguardia para el transporte y la manipulación de mercancías de todo tipo».

Su conexión directa por ferrocarril con las regiones mineras del interior lo convierte en un punto clave para la exportación de minerales y productos industriales, ampliando el perfil económico del Reino más allá del petróleo.

Junto con estas instalaciones visibles, existe una infraestructura menos perceptible pero igualmente crítica, ellos son los sistemas submarinos que conectan yacimientos *offshore* como Zuluf, Marjan y Safaniya con la costa. Estos campos, que albergan reservas de decenas de miles de millones de barriles (El economista, 2025), dependen de complejas redes de tuberías y cables submarinos para su funcionamiento. La interrupción de cualquiera de estos elementos tendría efectos inmediatos sobre la producción y exportación de crudo.

En este mismo entorno, se ubica la planta desalinizadora de Ras Al-Khair, la mayor del mundo. Según datos de (Water Partners, 2024) esta planta produce 1036 millones de litros de agua por día y su desarticulación significaría un gran problema para toda la sociedad. En una región donde el agua es un recurso estratégico escaso, esta instalación representa un activo crítico cuya pérdida tendría consecuencias sociales y económicas de gran alcance.

Por su parte, la costa occidental saudí presenta un perfil de riesgo diferente, pero no menos significativo. Por el mar Rojo transita cerca del 15 % del comercio marítimo mundial, lo que convierte a sus puertos en nodos esenciales del sistema logístico global.

El puerto Rey Fahd de Yambú es uno de los principales centros de exportación de productos petroquímicos del país y un punto de escala clave en las rutas entre Occidente y Asia. A pesar de la distancia[79] que la separa respecto a la capital de Yemen, ya ha sido

[79] Aproximadamente mil doscientos kilómetros.

objeto de ataques con drones, lo que demuestra la capacidad de los hutíes para proyectar fuerza a larga distancia y seleccionar objetivos de alto valor simbólico y económico.

Más al sur, el puerto y refinería de Yeda constituye uno de los mayores centros logísticos saudíes. Elentably (2015) destaca que «este punto logístico es uno de los principales puertos saudíes en términos de volumen de carga y manipulación de insumos con capacidad para albergar 58 barcos dentro de sus 11,2 kilómetros de longitud». Su proximidad al eje Bab al Mandeb – canal de Suez lo convierte en un posible objetivo especialmente sensible. Los ataques sufridos en 2022, que provocaron incendios en depósitos de crudo, evidenciaron la vulnerabilidad de estas instalaciones frente a amenazas asimétricas.

Finalmente, el puerto y refinería de Jazan representa quizá el caso más crítico desde el punto de vista de la seguridad. Situado a escasos ciento noventa kilómetros de Saadá[80], bastión hutí en Yemen y a menos de trescientass millas náuticas del estrecho de Bab al Mandeb, este complejo combina una elevada capacidad de refinado con una exposición directa a ataques con misiles y drones. Su importancia como puerta de entrada de importaciones



Figura 1. Magnitud del incendio en uno de los depósitos de la refinería en Jeddah (The Guardian, 2022)

[80] Esta ciudad es uno de los bastiones principales desde donde se cree se han efectuado la mayoría de los lanzamientos de misiles y drones hacia el sur saudí.

africanas refuerza su valor estratégico y, al mismo tiempo, su atractivo como objetivo.

3.3 La dimensión marítima de la seguridad de las infraestructuras críticas saudíes

En conjunto, dichas infraestructuras conforman el esqueleto energético y económico de Arabia Saudí. Su emplazamiento mayoritariamente costero y la fuerte dependencia de corredores marítimos estratégicos las sitúan dentro del alcance de amenazas tanto convencionales como no convencionales, en particular aquellas asociadas a actores no estatales.

Este contexto explica la inversión sostenida del Reino en capacidades de defensa aérea, naval y en sistemas de protección de infraestructuras críticas. Sin embargo, estas iniciativas trascienden la mera defensa física: forman parte de una estrategia de disuasión más amplia orientada a garantizar la continuidad de los flujos energéticos globales y a la búsqueda de una consolidación de los ya identificados intereses mayores. La credibilidad de esta postura disuasiva es, por tanto, un componente esencial de su política de seguridad y de su proyección geopolítica.

En ese marco, la seguridad de las infraestructuras estratégicas saudíes no se limita a puertos, refinerías o complejos industriales, sino que también depende de un factor tan decisivo como frágil: el control de los pasos marítimos clave. Estos estrechos y corredores concentran una porción significativa del comercio energético mundial y, al mismo tiempo, constituyen algunos de los puntos más vulnerables del sistema global, donde incidentes localizados pueden generar efectos desproporcionados a escala regional e internacional.

En el caso de Arabia Saudí, y como ya fue resaltado, los estrechos de Ormuz, que da acceso al golfo Arábigo, y de Bab al-Mandeb, situado en la salida meridional del mar Rojo, adquieren una relevancia estratégica fundamental, ya que ambos funcionan como auténticas arterias por las que transita el petróleo saudí con destino a los mercados internacionales.

3.4 El estrecho de Ormuz: un paso sin alternativa

El estrecho de Ormuz es uno de los espacios marítimos más sensibles del planeta. Por él transitan los buques que conectan

los puertos saudíes del golfo Arábigo con el resto del mundo, en un entorno caracterizado por un tráfico intenso y altamente concentrado.

Su principal vulnerabilidad radica en un hecho tan simple como crítico: la inexistencia de una ruta alternativa viable. En consecuencia, y conforme a los marcos legales internacionales establecidos por el derecho del mar, los buques que transitan por esta vía deben hacerlo a través de aguas territoriales de Irán y Omán. En su tramo navegable más estrecho, el corredor cuenta con apenas dos kilómetros de ancho, una característica que lo vuelve especialmente susceptible a interrupciones derivadas de bloqueos físicos, actos de sabotaje o incluso la colocación de minas marítimas (Zulkifli, Ridzuan y Ariffin, 2023: 24).

Si bien el derecho internacional garantiza el derecho de paso en tránsito de los buques a través de los estrechos, la realidad operacional resulta considerablemente más compleja. Irán, ubicado en la ribera norte, ejerce un control implícito sobre este espacio al haber desarrollado una doctrina militar sustentada en tácticas asimétricas. En un escenario de escalada, dichas capacidades podrían materializarse en el empleo de misiles, drones, embarcaciones rápidas o minas marítimas, con el objetivo de hostigar o incluso paralizar el tráfico comercial.

La sola posibilidad de una interrupción prolongada en Ormuz tendría consecuencias inmediatas sobre los precios del petróleo. Por este motivo, el estrecho ha atraído históricamente la atención de potencias externas, en especial de Estados Unidos, cuya presencia naval busca garantizar la libertad de navegación. Esta dinámica, sin embargo, también alimenta tensiones recurrentes con Teherán, reforzando la percepción de Ormuz como uno de los puntos más volátiles del sistema energético global.

3.5 Bab al Mandeb: la amenaza desde la inestabilidad

Si Ormuz representa el riesgo de un bloqueo estatal, Bab al Mandeb encarna la amenaza de la inestabilidad crónica. Este estrecho conecta el mar Rojo con el océano Índico a través del golfo de Adén y constituye un eslabón esencial entre los mercados de Asia, Europa y América. En términos económicos, el estrecho vincula los mercados de América, Asia y Europa. González Laxe

(2024: 57) recalca que «sus dimensiones de 64 millas náuticas de longitud, una anchura máxima de 16 millas y una profundidad de 300 metros, refuerzan su papel como arteria clave del comercio global».

A diferencia de otros pasos estratégicos, Bab al Mandeb atraviesa una región marcada por conflictos persistentes. En sus márgenes, se encuentran países como Yibuti, Eritrea, Somalia y, especialmente, Yemen, donde operan grupos armados y redes de piratería. En este contexto, el movimiento hutí ha adquirido un protagonismo creciente, utilizando drones y misiles para atacar buques comerciales y generar un clima de inseguridad constante.

Desde finales de 2023, estas acciones han tenido un impacto tangible: decenas de buques han sido atacados o amenazados, y numerosas navieras internacionales se han visto obligadas a suspender o desviar sus rutas. La alternativa más segura consiste en rodear África por el cabo de Buena Esperanza, una opción que incrementa de forma significativa los tiempos y costos del transporte marítimo.

Para dimensionar el impacto, una ruta entre Asia oriental y el norte de Europa que normalmente se completa en poco más de veinticinco días a través del mar Rojo y el canal de Suez puede extenderse hasta más de 34 días si se evita Bab al Mandeb. Este aumento no solo encarece el transporte, sino que introduce disrupciones en las cadenas de suministro a escala global.

La combinación de estos dos cuellos de botella sitúa a Arabia Saudí ante un desafío estratégico de primer orden. La protección de sus infraestructuras energéticas no puede limitarse al ámbito terrestre o costero, sino que exige una capacidad efectiva para disuadir, vigilar y, llegado el caso, intervenir en espacios marítimos críticos.

En este sentido, la seguridad de Ormuz y Bab al Mandeb no es solo una cuestión nacional, sino un interés compartido por la comunidad internacional. Sin embargo, para Riad, estos estrechos representan algo más: son el vínculo indispensable entre su sistema energético y el mundo. Garantizar su estabilidad implica sostener su papel como proveedor fiable de energía y como actor central en el equilibrio geoeconómico global.

Para Arabia Saudí, esta situación presenta una paradoja estratégica. Por un lado, la internacionalización del problema refuerza

su narrativa de víctima de amenazas asimétricas y facilita la cooperación con socios externos. Por otro, reduce su control exclusivo sobre la gestión de la seguridad en un espacio que afecta de manera directa a sus intereses vitales. Esta tensión obliga al Reino a equilibrar su autonomía estratégica con la necesidad de coordinar esfuerzos dentro de marcos multilaterales.

4 Defensa de infraestructuras vitales y transformación militar saudí hacia 2030

4.1 Disuasión, diplomacia y alianzas estratégicas

Como uno de los principales productores de petróleo del mundo, Arabia Saudí enfrenta un desafío permanente: proteger a este entramado de infraestructuras críticas cuya vulnerabilidad ha obligado al Reino a replantear profundamente su enfoque defensivo.

Cesce (2023: 8) subraya que, a pesar de contar con uno de los mayores presupuestos en defensa a nivel mundial, los daños producidos a las refinerías, sumado a las acciones insurgentes hutíes que de manera intermitente pero efectiva siguen actuando contra el comercio marítimo, evidencian la vulnerabilidad saudí en este aspecto.

Esta realidad ha impulsado a Riad a adoptar una estrategia de disuasión integral, orientada no solo a responder a las amenazas actuales, sino a prevenir agresiones futuras en un entorno cada vez más complejo.

La estrategia saudí de disuasión se articula en torno a tres ejes complementarios: la diplomacia activa, la protección externa mediante alianzas y el desarrollo de capacidades militares propias más eficaces.

En el plano diplomático, el acercamiento con Irán, aunque frágil y condicionado, ha sido concebido como una herramienta para ganar tiempo estratégico. Reducir temporalmente la intensidad de las hostilidades permite al Reino avanzar en la modernización de sus Fuerzas Armadas y en la protección de sus infraestructuras sin verse arrastrado a una escalada directa.

Desde la perspectiva de los actores involucrados, Jahandad y Mustafa (2023: 101) corrobora que «Irán sigue sin percibir a Arabia Saudí como una amenaza militar directa; no obstante, Riad sí ve a Teherán como un peligro debido a su respaldo al

movimiento Ansar Allah» y como Huzzain (2024: 24) realza «aunque el acercamiento diplomático ha generado expectativas positivas, elementos de línea dura en ambas naciones podrían intentar socavar cualquier avance en la normalización de relaciones».

No obstante, tanto analistas como responsables militares saudíes coinciden en que el impacto real de esta vía es incierto, especialmente debido a la autonomía operativa de actores no estatales como los hutíes.

El segundo pilar de la disuasión saudí descansa en la protección externa, basada en la cooperación con aliados clave. Estados Unidos continúa siendo su principal socio en materia de seguridad, aunque Riad ha diversificado progresivamente sus relaciones, incorporando a China y a otros actores relevantes. Wezeman *et al.* (2024: 3) esgrimen que «esta estrategia lo ha posicionado entre los cinco principales importadores de armamento a nivel mundial, con un 15 % de sus adquisiciones solo provenientes de Estados Unidos».

El tercer eje, y quizá el más ambicioso, es el desarrollo de capacidades militares nacionales. En línea con la Visión 2030, Arabia Saudí ha iniciado un proceso de transformación orientado a crear una industria de defensa propia, reduciendo su dependencia externa y fortaleciendo su autonomía estratégica.

Este esfuerzo es especialmente visible en el ámbito naval. La Armada saudí ha experimentado una modernización significativa, basada no solo en la adquisición de nuevos buques, sino también en la transferencia tecnológica, la formación de personal y el aumento del nivel de adiestramiento conjunto con aliados regionales e internacionales. Los ejercicios combinados en el mar Rojo y el golfo Arábigo reflejan una clara intención de mejorar la interoperabilidad y la capacidad de respuesta frente a amenazas multidominio.

Un hecho particularmente revelador de esta nueva dinámica fue la solicitud saudí para realizar ejercicios navales conjuntos con Irán. A través de medios de comunicación privados (The New Arab, 2024), el comandante general de la Armada iraní, almirante Sharham, reveló que la monarquía saudí había solicitado realizar ejercicios militares conjuntos con el Estado persa en el mar Rojo.

A la luz de este singular pedido y desde una perspectiva de información e inteligencia, es sabido que los ejercicios militares otor-



Figura 2. El presidente estadounidense Donald Trump y el príncipe saudí Mohammed bin Salman en Riad, Arabia Saudí (Los Angeles time, 2025)

gan datos doctrinarios, de estado de material, de adiestramiento, entre otros, lo cual en una hipotética línea con el pensamiento de Sun Tzu[81], le proporcionaría grandes beneficios al Reino, más aun tratándose de su principal amenaza en la región.

4.2 Limitaciones del poder marítimo saudí: una lectura desde el pensamiento naval clásico

La evolución del componente naval saudí puede analizarse de forma especialmente esclarecedora a la luz de la teoría del poder marítimo de Alfred Thayer Mahan. Para este autor, la prosperidad y la seguridad de una nación dependen en gran medida de su capacidad para controlar las rutas marítimas, proteger el comercio y proyectar poder a través de una flota suficiente, bien distribuida y sostenida por una infraestructura logística adecuada.

Desde esta perspectiva, Arabia Saudí enfrenta importantes limitaciones estructurales. Su flota, dividida entre el golfo Arábigo y el mar Rojo, dispone de un número relativamente reducido de unidades de combate, lo que dificulta ejercer un control efectivo sobre un litoral extenso y altamente transitado.

[81] Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cien batallas.

El país posee un litoral de aproximadamente 2640 kilómetros (Torregrosa Ramos, 2023a: 3), además de una extensa porción territorial con derechos soberanos, resultando que la cantidad de bases navales establecidas en su territorio resulta insuficiente para un despliegue estratégico-militar efectivo.

La fragmentación de fuerzas se ve agravada por la geografía: la imposibilidad de trasladar rápidamente medios navales entre ambos frentes obliga a planificar la defensa como dos teatros prácticamente independientes, diluyendo la masa crítica de poder naval que Mahan consideraba esencial.

En concreto, la distancia entre el golfo Arábigo y el mar Rojo obliga a los buques saudíes a rodear la península a través del mar Arábigo y del golfo de Adén, debiendo recorrer aproximadamente 2500 millas náuticas, lo que supone un tránsito de más de siete días a velocidad de crucero[82], tiempo que debe ser considerado como factor de planeamiento en caso de que una flota demande el apoyo de la otra.

Asimismo, el control de puntos estratégicos clave otro elemento central del pensamiento mahaniano continúa siendo un desafío para el Reino. Los estrechos de Ormuz y Bab al Mandeb, vitales para el comercio energético saudí, permanecen expuestos a la influencia iraní y a la acción de milicias aliadas, lo que limita la libertad de maniobra de Riad y reduce su capacidad de garantizar la seguridad de las líneas de comunicación marítima.

Como mitigación de ello la transformación militar saudí ha adoptado un rumbo de avance sostenido. Consolidarse como una potencia naval regional, indefectiblemente requiere ampliar su infraestructura naval, diversificar sus adquisiciones estratégicas y avanzar hacia niveles superiores de autonomía, incluyendo la producción local de buques de guerra y el desarrollo de capacidades submarinas.

En última instancia, el objetivo saudí no se limita a la defensa pasiva de sus costas. La aspiración es construir un poder marítimo capaz de disuadir, proteger y proyectar influencia sobre las rutas que sostienen su economía y su papel geopolítico. En un entorno regional marcado por la incertidumbre, esta capacidad será determinante para garantizar la seguridad de sus infraestructuras vitales.

[82] Para este caso se tomará como velocidad crucero catorce nudos o lo que es igual a catorce millas por hora.

Desde 2016, Arabia Saudí ha emprendido un proceso sostenido de expansión y modernización de sus Fuerzas Armadas. Es por ello y que, como parte de este proceso, la nación saudí reforzó su flota con la adquisición de patrulleros y corbetas. Torregrosa Ramos (2023a: 545) sostiene «esta adquisición está destinada principalmente a la protección de refinerías e infraestructuras portuarias como a la escolta de petroleros en rutas de exportación».

En el ámbito marítimo, la estrategia saudí se orienta a limitar la libertad de acción de su principal competidor regional mediante una política de negación del espacio marítimo dentro de las áreas bajo soberanía nacional. Sin embargo, este objetivo se ve condicionado por el crecimiento constante del poder naval iraní, que en los últimos años ha incrementado su presupuesto, ampliado su flota y diversificado sus capacidades con tecnología propia y de origen chino.

Irán dispone hoy de una amplia cantidad de unidades costeras y lanchas de ataque rápido, diseñadas para ejecutar acciones asimétricas de alta velocidad, a lo que se suma una capacidad relevante en guerra de minas y una flota submarina en expansión. Este conjunto de medios representa un desafío directo para la seguridad del Golfo y obliga a Riad a compensar desventajas estructurales con tecnología, cooperación internacional y modernización doctrinaria.

4.3 El fortalecimiento naval saudí

En este contexto, Arabia Saudí ha apostado por reforzar sus flotas mediante la adquisición de buques multipropósito y patrulleros modernos. Un hito relevante fue la compra de cinco barcos de combate construidos por la empresa española Navantia[83] para su Flota Occidental, proyecto que incluyó transferencia tecnológica y producción parcial en territorio saudí. A estos se suman nuevas corbetas desarrolladas en cooperación con la industria de defensa nacional, integrando sistemas de combate propios.

De manera complementaria, la flota occidental ha incorporado nuevas patrulleras rápidas fabricadas por la empresa francesa Couach, mientras que la flota oriental se someterá a un proceso de modernización con la incorporación de cuatro buques tipo

[83] Navantia es una empresa pública española dedicada a la construcción naval militar. Ha participado en programas internacionales de fabricación de buques para países del Golfo, incluido Arabia Saudí.

MMSC[84], que serán adquiridos mediante el programa de ventas militares extranjeras de Estados Unidos. Según (Defense Arabia, 2023), este proyecto, conocido como proyecto Tuwaiq, cuenta con la empresa Lockheed Martin como contratista principal.

Aunque esta dinámica de adquisición de medios mejora favorablemente el panorama marítimo, desde una perspectiva realista, y como fue desarrollado con anterioridad, el Estado saudí aún presenta una importante vulnerabilidad: la carencia absoluta de submarinos. Esta limitación no solo restringe una potencial acción ofensiva, sino que también afecta el cumplimiento de diversas misiones defensivas, como la vigilancia y reconocimiento de embarcaciones militares, colocación de minas, entre otras.

Más aún y con relación a ello, la monarquía saudí no posee planes



Figura 3. Llegada de la primera corbeta a Arabia Saudí construida por Navantia (Infodefensa, 2022)

de modificar esta situación. La única intención de compra públicamente conocida se remonta al año 2013, fecha en que el Reino mostró un sólido interés en la adquisición de veinticinco de estos buques de clase 209 fabricados en Alemania bajo un acuerdo valorado en torno a los doce mil millones de euros, que como el diario germano *Bild* (2013) destacó, este contrato finalmente no prosperó.

84 *Multi-Mission Surface Combatant*.

4.4 Defensa aérea y protección del espacio estratégico

En el dominio aéreo, Arabia Saudí ha realizado inversiones significativas para proteger su territorio y sus infraestructuras críticas frente a ataques con misiles y aeronaves. La adquisición del sistema antimisiles *THAAD*[85] marcó un salto cualitativo en su capacidad defensiva. (Feickert, 2024: 1) indica que «esta clase de misil es capaz de atacar objetivos a una distancia de entre ciento cincuenta y doscientos kilómetros defendiendo áreas más amplias que el sistema Patriot[86]. Además, el Reino se convirtió en el primer país fuera de Estados Unidos en producir localmente componentes de este sistema, fortaleciendo su independencia logística.

Este esfuerzo se complementó con la compra de nuevos sistemas Patriot y con la incorporación de sistemas de defensa aérea de origen surcoreano, diseñados para interceptar misiles balísticos y aeronaves enemigas. La integración de estos sistemas, junto con acuerdos de transferencia tecnológica, refleja una clara intención de construir una arquitectura defensiva multicapa.

En cuanto a la aviación de combate, la Real Fuerza Aérea Saudí consolidó su flota con cazas Eurofighter y F-15SA de última generación, acompañados de paquetes completos de entrenamiento, soporte logístico y modernización de bases. A ello se sumó la incorporación de aeronaves de ala rotatoria, firmando luego en el año 2021 un contrato con los Estados Unidos para mejorar tecnológicamente las aeronaves Apache, simuladores y servicios logísticos, por un valor de 437 millones de dólares (Defense Arabia, 2021), fortaleciendo con estos medios sus capacidades de reconocimiento, ataque y transporte.

Un componente cada vez más relevante es el uso de sistemas no tripulados. Arabia Saudí opera drones armados de origen chino y proyecta incorporar modelos más avanzados, capaces de realizar misiones prolongadas y portar armamento aire-superficie. Además, mantiene intenciones de dotarse de los UCAV Wing Loong-10B que pueden

> «alcanzar una velocidad máxima de 620 kilómetros por hora y volar a 15 mil metros durante unas 20 horas, transportando 900 kg de munición aire-superficie, incluidos misiles

[85] El THAAD (Terminal High Altitude Area Defense) es un sistema estadounidense de defensa antimisiles diseñado para interceptar misiles balísticos a gran altitud.

[86] Este sistema posee un alcance conocido de setenta kilómetros.

planeadores propulsados por cohetes y misiles ligeros antibuque YJ-9E» (Satam, 2024).

4.5 Capacidades terrestres y ciberdefensa

En el plano terrestre, el Reino reforzó sus fuerzas con la adquisición de tanques modernos y vehículos blindados, mejorando tanto su capacidad defensiva como la interacción militar con países aliados. Malyasov (2016) plantea que «además de contribuir con la defensa nacional, la adquisición de este material a los Estados Unidos incrementa la interoperabilidad entre ambos ejércitos».

Aunque estas capacidades no están directamente orientadas al ámbito marítimo, contribuyen a la defensa integral del territorio y de las infraestructuras críticas.

Finalmente, la ciberseguridad se ha convertido en un pilar central de la estrategia defensiva saudí. Consciente de la creciente amenaza en el ciberespacio, el Reino desarrolló un marco nacional de ciberseguridad orientado a proteger sistemas gubernamentales, industriales y energéticos. De esta manera en el ámbito de la tecnología operativa, la nación saudí ha desarrollado controles específicos para garantizar la seguridad de sistemas industriales estratégicos. Estos controles incluyen medidas de gobernanza en ciberseguridad, mecanismos de defensa activa contra amenazas, entre otros, siendo la aplicación de estas medidas crucial para evitar la explotación de vulnerabilidades en los activos neurálgicos del país por actores malintencionados (TechSciresearch, 2024).

En conjunto, la expansión y modernización militar saudí reflejan un enfoque integral y multidominio de la seguridad nacional. Lejos de responder a una lógica puramente ofensiva, la mayor parte de estas capacidades están orientadas a la protección de infraestructuras vitales y a la disuasión de amenazas que podrían comprometer la estabilidad económica y política del Reino.

Este proceso, aún en desarrollo, posiciona a Arabia Saudí en una trayectoria clara hacia el fortalecimiento de su autonomía estratégica y su aspiración de liderazgo regional. No obstante, como se ha señalado a lo largo de este artículo, persisten desafíos estructurales que deberán ser abordados si el Reino pretende garantizar de manera plena la seguridad de sus intereses más críticos en un entorno regional altamente volátil.

4.6 Las Fuerzas Armadas saudíes como instrumento de la Visión 2030

La Visión 2030 constituye uno de los proyectos de transformación más ambiciosos impulsados por Arabia Saudí en su historia reciente. Concebida originalmente como un plan para diversificar la economía y reducir la dependencia del petróleo, esta estrategia incorpora de manera explícita un componente militar y de seguridad que resulta esencial para su viabilidad. En un entorno regional marcado por la inestabilidad y la competencia estratégica, la protección de infraestructuras críticas y rutas marítimas se ha convertido en una condición indispensable para el éxito del proyecto saudí.

Durante décadas, la industria militar del Reino dependió casi por completo de proveedores externos, especialmente de Estados Unidos. Sin embargo, como parte de su proceso de transformación, y de acuerdo con el informe científico (Gulf Research Centre, 2023: 7), como parte de su plan de transformación, el país ha establecido la meta de producir el 50 % de su equipamiento militar a nivel local para el año 2030, un cambio de paradigma que busca reducir vulnerabilidades estratégicas y ganar autonomía en la toma de decisiones.

Para alcanzar esta meta, Arabia Saudí ha puesto en marcha un conjunto de medidas que incluyen alianzas con empresas internacionales, inversiones sostenidas en investigación y desarrollo, y un fuerte impulso a la formación de capital humano especializado. La creación de organismos como la *GAMI* ha facilitado la concesión de licencias, la localización de empresas y la regulación del sector, generando un crecimiento notable de la industria de defensa nacional.

Un actor central de este proceso es el *Saudi Arabian Military Industries*, empresa estatal que opera como eje articulador del desarrollo industrial militar. A través de acuerdos con socios extranjeros, el SAMI ha avanzado en la transferencia tecnológica y en la fabricación local de sistemas avanzados, concentrando sus esfuerzos en cuatro áreas clave: sistemas aéreos, terrestres, armamento y misiles, y defensa cibernética.

Este impulso se ve reforzado por una intensa política de cooperación internacional. Carma (2024: 2), subraya que eventos como el World Defense Show, promovido por el propio gobierno saudí, se han consolidado como plataformas para atraer inver-

sión extranjera, exhibir capacidades nacionales y fortalecer vínculos con actores globales del sector defensa. El objetivo no es solo adquirir tecnología, sino internalizar conocimiento y sentar las bases de una industria sostenible en el largo plazo.

No obstante, el camino hacia la autosuficiencia militar no está exento de desafíos. La limitada experiencia técnica en algunos sectores estratégicos y la escasez de personal altamente capacitado representan obstáculos relevantes. Para mitigarlos, el Reino ha reforzado programas de formación de ingenieros, técnicos y especialistas en defensa, promoviendo la cooperación entre universidades, centros de investigación y la industria militar (Gulf Research Centre, 2023: 51). En paralelo, se ha incrementado la inversión en ciberseguridad, un ámbito crítico para proteger tanto sistemas militares como infraestructuras energéticas frente a amenazas no convencionales.

En términos operativos, la Visión 2030 también impulsa una transformación tangible de las capacidades militares. La modernización de las fuerzas navales, el fortalecimiento de la defensa aérea y el desarrollo de capacidades de inteligencia, vigilancia y reconocimiento reflejan una orientación clara hacia la protección del litoral marítimo y de los activos estratégicos asociados al comercio energético.

Este proceso no busca únicamente garantizar la seguridad nacional, sino también posicionar a Arabia Saudí como un actor militar regional en ascenso, menos dependiente de potencias externas que, históricamente, han condicionado su margen de maniobra estratégica.

En resumen, el análisis de la expansión y modernización del aparato militar saudí desde 2016 permite afirmar que el Reino ha alcanzado un nivel de capacidades que, si bien no lo hace invulnerable, sí le otorga una postura disuasiva creíble frente a amenazas. La incorporación de sistemas antimisiles avanzados, el refuerzo de la flota naval y la mejora de las capacidades ISR evidencian una transformación profunda, orientada a asegurar la continuidad operativa de las infraestructuras críticas del litoral marítimo.

De cara a 2030, las Fuerzas Armadas saudíes no solo cumplen una función defensiva, sino que se consolidan como un instrumento central del proyecto político, económico y estratégico del Reino, en un contexto regional donde la seguridad es, más que nunca, un prerrequisito del desarrollo.

La consolidación de las Fuerzas Armadas saudíes como instrumento central de la Visión 2030 refleja una concepción ampliada de la seguridad nacional, en la que la defensa deja de ser un fin en sí mismo para convertirse en un habilitador del desarrollo económico y la estabilidad política. La protección de infraestructuras críticas y del litoral marítimo no solo garantiza la continuidad operativa del sector energético, sino que también refuerza la confianza de inversores y socios internacionales en la capacidad del Reino para gestionar riesgos complejos.

En este sentido, la transformación militar saudí puede interpretarse como una inversión estratégica orientada a reducir vulnerabilidades estructurales y a aumentar la resiliencia del Estado frente a escenarios de presión prolongada. Aunque persisten limitaciones evidentes, especialmente en el ámbito naval, el progreso alcanzado desde 2016 indica una trayectoria coherente hacia una mayor autonomía estratégica.

Este proceso, sin embargo, no elimina la necesidad de adaptación constante. La evolución tecnológica, la proliferación de medios asimétricos y la persistencia de conflictos regionales obligarán a Arabia Saudí a revisar de manera periódica su postura defensiva, manteniendo un equilibrio delicado entre disuasión, cooperación y prudencia estratégica.

5 Conclusión

La protección de las infraestructuras críticas del litoral marítimo saudí se ha consolidado como uno de los ejes centrales de la seguridad nacional del Reino en un entorno regional caracterizado por la competencia estratégica, la proliferación de amenazas asimétricas y la persistencia de conflictos por delegación. La elevada dependencia del sistema energético saudí respecto de instalaciones costeras, pasos marítimos críticos y cadenas logísticas altamente interconectadas convierte cualquier alteración de estos activos en un factor de riesgo no solo nacional, sino de alcance regional y global.

El análisis desarrollado a lo largo de este trabajo permite afirmar que Arabia Saudí se enfrenta a un desafío estructural: garantizar la continuidad operativa de infraestructuras críticas vitales frente a adversarios que operan deliberadamente por debajo del umbral del conflicto convencional. Irán, mediante una estrategia de proyección indirecta de poder, y el movimiento hutí, como actor no

estatal con capacidades crecientemente sofisticadas, han demostrado la eficacia de las acciones asimétricas, híbridas y de zona gris para erosionar la percepción de seguridad del Reino y condicionar su margen de maniobra estratégica.

Los ataques contra instalaciones energéticas, puertos y rutas marítimas han puesto de manifiesto que la superioridad militar convencional no es, por sí sola, garantía suficiente para la protección de infraestructuras críticas. En este sentido, la vulnerabilidad demostrada de activos de alto valor simbólico y económico ha actuado como catalizador de una profunda revisión del enfoque defensivo saudí, impulsando una transformación orientada hacia una arquitectura de seguridad más integrada, resiliente y multidominio.

La respuesta saudí ha sido coherente con esta lectura estratégica. Desde 2016, y especialmente en el marco de la Visión 2030, el Reino ha llevado a cabo un proceso sostenido de modernización de sus Fuerzas Armadas, con especial énfasis en el fortalecimiento del componente naval, la defensa aérea y antimisiles, las capacidades de inteligencia, vigilancia y reconocimiento, y la protección del ciberespacio. Estas capacidades no persiguen únicamente una finalidad defensiva inmediata, sino que forman parte de una estrategia de disuasión convencional orientada a elevar los costes y reducir los incentivos para la agresión indirecta.

No obstante, el análisis desde la perspectiva del pensamiento naval clásico, en particular de Alfred Thayer Mahan, revela la persistencia de limitaciones estructurales en el poder marítimo saudí. La fragmentación de sus fuerzas navales entre el golfo Arábigo y el mar Rojo, la extensión de su litoral, la ausencia de capacidades submarinas y la exposición permanente de pasos estratégicos como Ormuz y Bab al Mandeb restringen su capacidad para ejercer un control efectivo y sostenido del dominio marítimo. Estas limitaciones obligan al Reino a complementar su esfuerzo militar con alianzas estratégicas, cooperación internacional y mecanismos diplomáticos orientados a la contención y a la gestión del riesgo.

En este contexto, la seguridad del litoral marítimo saudí y de sus infraestructuras críticas trasciende el ámbito estrictamente nacional. La estabilidad de los flujos energéticos y del comercio marítimo convierte a Arabia Saudí en un actor central del equilibrio geoeconómico global, lo que explica la creciente internacionalización de la seguridad de estos espacios. Sin embargo, esta

misma internacionalización introduce tensiones entre la autonomía estratégica del Reino y la necesidad de coordinar esfuerzos con actores externos, configurando una paradoja que condicionará sus decisiones futuras.

Finalmente, puede concluirse que Arabia Saudí ha logrado construir una postura disuasiva más creíble y adaptada al entorno contemporáneo, aunque no exenta de vulnerabilidades. La protección efectiva de sus infraestructuras críticas en el litoral marítimo dependerá de su capacidad para sostener en el tiempo la modernización militar, profundizar la integración entre dominios, fortalecer la resiliencia de sus sistemas críticos y mantener un delicado equilibrio entre disuasión, cooperación y prudencia estratégica. En un escenario regional volátil y dinámico, esta capacidad de adaptación será determinante no solo para la seguridad del Reino, sino para la estabilidad del sistema energético internacional en su conjunto.

Bibliografía

Aguas residuales.info (2023). La mayor desalinizadora del mundo, construida por ACCIONA en Arabia Saudí, ya está a pleno rendimiento [en línea]. Aguas residuales [Consulta: 16 julio 2026]. Disponible en: https://www.aguasresiduales.info/revista/noticias/la-mayor-desalinizadora-del-mundo-construida-por-a-Kp3GW

Airforce Tecnologhy, (2020). Royal Saudi Air Force receives final F-15SA fighter aircraft [en línea]. Airforce Technology. [Consulta: 27 enero 2025]. Disponible en: https://www.airforce-technology.com/news/royal-saudi-air-force-f-15sa-fighter-aircraft/

Alutaibi, K. S. (2009). Critical infrastructure protection in Saudi Arabia: a case study on petrochemical industry protection against terrorist attacks at Jubail industry city [trabajo de fin de máster] [en línea]. King Fahd University of Petroleum and Minerlas. [Consulta 11 agosto 2024]. Disponible en: https://eprints.kfupm.edu.sa/id/eprint/136100/1/Khaled_Alutaibi_976452.pdf

Álvarez, I. (2024). Arabia Saudí: la apertura como estrategia de supervivencia. *Panorama Estratégico 2024*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, pp. 199-219.

Ap News. (2024). OPEC + production cuts deepen with extensions from Saudi Arabia, Russia and other oil giants [en línea]. Ap News. [Consulta: 5 febrero 2025]. Disponible en https://apnews.com/article/opec-production-cuts-saudi-arabia-russia-90502ac95a2eed4e8c6d03f9bf9346b9

Ardemagni, E. (2023). Stormy waters for Saudi Arabia: regional conflict and red sea security [en línea]. Carnegie endowment for international peace. [Consulta: 8 septiembre 2024]. Disponible en https://carnegieendowment.org/sada/2023/11/stormy-waters-for-saudi-arabia-regional-conflict-and-red-sea-security?lang=en

Ashomer, A. (2024). El F-15SA Eagle debuta en el Royal International Air Tattoo 2024 [en línea]. Noticias de Israel. [Consulta: 10 septiembre 2024]. Disponible en: https://israelnoticias.com/militar/el-f-15sa-Eagle-debuta-en-el-royal-international-air-tattoo-2024/

Baabood, A. (2024). How gulf states are reinterpreting national security beyond their land borders [en línea]. Carnegie endowment for international peace. [Consulta: 10 septiembre 2024]. Disponible en: https://carnegieendowment.org/research/2024/08/how-gulf-states-are-reinterpreting-national-security-beyond-their-land-borders-abdullah-baabood?lang=en

Baqués, J. (2019). El papel de marina de guerra en la geoestrategia saudí. *Revista General de Marina*. N.º 276, pp. 519-531.

Basenton. (2023). Una guía de los 11 puertos más importantes de Arabia Saudita [en línea]. Basenton. [Consulta: 4 enero 2025]. Disponible en: https://www.basenton.com/a-guide-to-saudi-arabias-11-most-important-ports/

Bernin, P. (2021). El fiasco saudí en Yemen. La victoria irreversible de los rebeldes hutíes. *Le Monde diplomatique*. N.º 303, pp. 6-7.

Bordón, J. (2021). El conflicto de Yemen y Arabia Saudí: sin influencia para resolver pero con motivos para no hacerlo [en línea]. Análisis del Real Instituto Elcano (ARI). Real Instituto Elcano. N.º 70. [Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/servlet/revista?codigo=7438

Brodie, B. (1958). The anatomy of deterrence [en línea]. The Rand Corporation. [Consulta: 19 diciembre 2024]. Disponible en https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM2218.pdf

Cal, C. *et al. (2016). La cuestión estratégica – análisis y conducción.* Buenos Aires, Escuela de Guerra Naval de la República Argentina.

Carma. (2024). World Defense Show 2024. Defence Sector Trends Towards Localised Production, AI Integration, and Unmanned Systems [en línea]. Carma. [Consulta: 12 diciembre 2024]. Disponible en: https://7328329.fs1.hubspotusercontent-na1.net/hubfs/7328329/World%20Defense%20Show%202024%20-%20CARMA.pdf

Castaño, S. M. (2020). Proyección territorial y lugares sagrados: el rol legitimador de la religión en Arabia Saudí [en línea]. Revistas Académicas de la Universidad de Chile. 52(196), pp. 91-102. [Consulta: 2026]. Disponible en: https://revistas.uchile.cl/

Cerioli, L. (2023). Saudi Arabian strategy reassessment since 2003: The emergence of a regional leadership via Neoclassical Realist lenses. *Sage Journals*. 26(3), pp. 287-303.

Cesce. (2023). *Informe riesgo país Arabia Saudí*. Madrid, Cesce, dirección de riesgo país y deuda.

Chaker, R. (2024). Arab Gulf States naval procurement strategies: A three-level approach. *Marine Policy*. N.º 166.

Chen, V. (2017). Saudi Arabia and Iran: Sectarianism, a Quest for Regional Hegemony, and International Alignments [en línea]. Syracuse University. [Consulta: 6 diciembre 2024]. Disponible en https://surface.syr.edu /cgi/viewcontent.cgi?article=2013&context=honors_capstone

Chinchilla Adell, M. (2018). La efectividad de la teoría de la disuasión en la proliferación de armas nucleares en Oriente Medio. *Documento Marco 02/2018*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, pp. 873-924.

Chivvis, C. (2023). Saudi Arabia in the emerging world order [en línea]. Carnegie endowment for international peace. [Consulta: 13 septiembre 2024]. Disponible en https://carnegieendowment.org/research/2023/11/saudi-arabia-in-the-emerging-world-order?lang=en

Chivvis, C. et al. (2024). Is a defense treaty with Saudi Arabia worth the commitments? [en línea]. Carnegie endowment for international peace. [Consulta: 13 septiembre 2024]. Disponible en: https://carnegieendowment.org/emissary/2024/08/saudi-arabia-us-defense-treaty-worth-commitment

Connell, M. (2014) *Deterring Iran's Use of Offensive Cyber: A Case Study: Fort Belvoir*. Defense Technical Information Center, pp. 1-18.

Naciones Unidas. (1982). Convención de las Naciones Unidas sobre el Derecho del Mar [en línea]. Naciones Unidas [Consulta: 25 febrero 2025]. Disponible en: https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf

Covarrubias, M. G. S. (2021). La compra de armamento de Arabia Saudí a Estados Unidos como instrumento de control geopolitico de Medio oriente (2010-2019) [trabajo de fin de grado] [en línea]. Universidad Nacional Autónoma de México. [Consulta: 13 septiembre 2024]. Disponible en: https://ru.dgb.unam.mx/server/api/core/bitstreams/af2cff53-5e60-416e-9c62-5853cefb2449/content

De Carlos S. (2021). La pugna por la hegemonía regional: la rivalidad estratégica entre Arabia Saudí e Irán en la última década. *Revista del Instituto Español de Estudios Estratégicos*. N.º 17, pp. 13-38.

De Felice, F., Baffo, I. y Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and Future. *Sustainability review*. 14(4), pp. 1-20.

Defense Arabia. (2021). Boeing Secures Saudi's $437M Apache Helicopter Deal [en línea]. Defense Arabia. [Consulta: 19 noviembre 2024]. Disponible en: https://english.defensearabia.com/boeing-secures-saudis-437m-apache-helicopter-deal/

—. (2023). Royal Saudi Navy Marks Milestone in "Project Tuwaiq" with Keel-Laying Ceremony for "HMS King Abdullah" [en línea]. Defense Arabia. [Consulta: 19 septeimbre 2024]. Disponible en: https://English.defensearabia.com/royal-Saudi-navy-marks-milestone-in-project-tuwaiq-with-keel-laying-ceremony-for-hms-king-abdullah/

Díaz, E. L. J. (2021). Arabia Saudi: un coloso con los pies de barro. *Revista UNISCI*. N.º 57, p. 101.

Echagüe, A. (2015). Emboldened yet vulnerable. The changing foreign policies of Qatar and Saudi Arabia. FRIDE, a european think tank for global action, pp. 13-16.

Eisenstadt, M. (2021). Iran's gray zone strategy – cornerstone of its asymmetric way of war. *Institute for National Strategic Security.* National Defense University. 9(2), pp. 76-97.

El economista, (2025). El cable submarino que exprime un enorme yacimiento de petróleo casi único en su especie en el Reino del crudo [en línea]. El economista. [Consulta: 19 marzo 2025]. Disponible en: https://www.eleconomista.es/mercados-cotizaciones/noticias/13197879/01/25/el-cable-submarino-que-exprime-un-enorme-yacimiento-de-petroleo-casi-unico-en-su-especie-en-el-reino-del-crudo.html

Elentably, A. (2015). Strategic and Operational Plan Implementation of Seaports (Utilization Jeddah Port). *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*. 9(4), pp. 489-497.

Fédorova, K. (2013). La contribución histórica de A.T. Mahan. El análisis comparativo de los conceptos geopolíticos: estratégico-militar y natural-orgánico. *Revista de Filosofía, Derecho y Oolítica*. N.º 17, pp. 3-27.

Feickert, A. (2024). The Terminal High Altitude Area Defense (THAAD) System. Washington D.C., Congressional Research Service.

Fernández Rodríguez, J. C., Payá Santos, C. y Ramírez, J. M. (2015). Análisis de riesgos y amenazas a infraestructuras críticas. Servicio de Publicaciones de la Universidad Nebrija, pp. 19-35.

Frías Sánchez, C. J. (2016). La disuasión convencional. *Revista del Instituto Español de Estudios Estratégicos*. N.º 8, pp. 103-125.

Fuente Cobo, I. (2017). Claves para entender el conflicto de Yemen. En: Izquierdo Alberca, M.ª J. (coord.). Panorama geopolítico de los conflictos 2027. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, pp. 161-180.

Galindo, A. (2011). Las relaciones entre China y Arabia Saudí. La diplomacia del Petróleo. *Red de Revistas Científicas de América Latina, el Caribe, España y Portugal*. 46(1), pp. 35-63.

Gea Congosto. (2020). La insurgencia hutí en la guerra civil de Yemen. *Revista del Instituto Español de Estudios Estratégicos*. N.º 16, pp. 117-156.

Global Fire Power. (2025). 2025 Saudi Arabia Military Strength [en línea]. Global Fire Power. [Consulta: 20 enero 2025]. Disponible en: https://www.globalfirepower.com/country-military-strength-detail.php?country_id=saudi-arabia

González Laxe, F. (2024). Vulnerabilidad de los choke points oceánicos e implicaciones económicas del conflicto en el mar

Rojo. *Boletín Económico de ICE (Serie histórica).* N.º 3170, pp. 53-73.

Gray, A. (2022). Jazan, our new smart self-powering refinery [en línea]. Aramco. [Consulta: 15 noviembre 2024]. Disponible en: https:/ / www. aramco. com/en / news-media/ elements-magazine/2022/jazan-complex

Gulf Research Center. (2023). The Military and defense industries sector in the Kingdom of Saudi Arabia: opportunities and challenges [en línea]. Investigación, Centro de Estudios Islámicos, Universidad de Cambridge. [Consulta: 18 noviembre 2024]. Disponible en: https://www.grc.net/documents/64d-4d9c9c170dMilitaryStudy3.pdf

Hellyer, D. H. A. (2023). Turning the page: Saudi Arabia's new diplomatic approach [en línea]. RUSI. [Consulta: 15 octubre 2024]. Disponible en: https://rusi.org/explore-our-research/publications/commentary/turning-page-saudi-arabias-new-diplomatic-approach

Hernández Martínez, D. (2022). La política de defensa de Arabai Saudí en el nuevo contexto regional de Oriente Medio. *Revista de Pensamiento Estratégico y Seguridad CISDE*. 7(1), pp. 25-39.

Herrera, M. (2023). Las ambiciones nucleares de Arabia Saudí: ¿congeladas de nuevo? [en línea]. Política exterior. [Consulta: 12 octubre 2024]. Disponible en: https://www.politicaexterior.com/las-ambiciones-nucleares-de-arabia-saudita-congeladas-de-nuevo/

Iddon, P. (2024). Arabia Saudita diversifica su defensa antiaérea e impulsa la industria local [en ínea]. Galaxia Militar. [Consulta: 15 diciembre 2024]. Disponible en: https://galaxia mili tar. es /arabia-saudita-diversifica-su-defensa-antiaerea-e-impulsa-la-industria-local/

Infodefensa. (2024). Llega a Arabia Saudí la primera corbeta construida por Navantia [en línea]. Infodefensa. [Consulta: 2 enero 2025]. Disponible en: https://www. Infodefensa .com / texto – diario / mostrar / 3891585 / llega – arabia – saudí -primera – corbeta – construida – navantia

Jahandad, J. y Mustafa, A. (2023). Saudi-Iran rivalry: a sectarian divide or security dilemma. *Journal of Contemporary Studies*. 11(2), pp. 86-101.

Khalil, F. (2022). Iranian nuclear weapons "Impact of Iranian nuclear weapons in the Middle East" [en línea]. Internation-

al Journal for Humanities and Social Sciences (IJHS). 1(1), pp. 1-4. [Consulta: 2026]. Disponible en: https://uobasrah.academia.edu/IJHS

Li, N. (2023). Saudi Arabian-Led Intervention in Yemen Conflicts. *Global Journal of Arts, Humanities and Social Sciences*. 11(1), pp. 46-64.

Lukman, M. (2024). The Civil War in Yemen and Saudi Regional Hegemonic Ambition: Perang Saudara Yaman dan Cita-cita Hegemoni Serantau Saudi. *International Journal of Interdisciplinary and Strategic Studies.* 5(8), pp. 509-522.

Lynch, M. (2016). *The new arab wars.* Philadelfia, Public Affairs.

Malyasov, D. (2016). U.S. approves sale of more than 133 Abrams battle tanks to Saudi Arabia [en línea]. Defence blog. [Consulta: 8 marzo 2025]. Disponible en: https://defence-blog.com/u-s-approves-sale-of-more-than-133-abrams-battle-tanks-to-saudi-arabia/

Marine Traffic. (2025). Estrecho de Ormuz [en línea]. [Consulta: 23 marzo 2025]. Disponible en: https ://www .marinetraffic .com /en/ais/home /centerx:56.6/ centery:23.6 /zoom:5

Martin, A. G. (2021). La marina del cuerpo de guardias revolucionarios islámicos y la guerra naval asimétrica. *Boletín IEEE*. 13(21), pp. 436-447.

Mearsheimer, J. (2001). *The tragedy of great power politics*. Nueva York y Londres, W anclas Norton & Company.

Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. (2024). *Arabia Saudí - Reino de Arabia Saudí*. Madrid, Dirección General de Comunicación, Diplomacia Pública y Redes.

Ministerio de Defensa. (1994). *Cuadernos de Estrategia. Análisis factorial de las causas que originan conflictos bélicos*. Madrid, Ministerio de Defensa, Instituto Español de Estudios Estratégios. N.º 69.

Ministerio de Economía, Comercio y Empresa. (2024). Informe económico y comercial de Arabia Saudí. Riad, Oficina económica y comercial de España en Riad.

Mnekhir, A. J. (2023). The strategy of rapprochement between Iran and Saudi Arabia is an important step towards peace and stability in the region. *Russian Law Journal*. 11(11), pp. 104-111.

Moniri, H., Fallahzadeh, M. y Eftekhari, L. (2020). Study of the Ways to Diffuse the Islamic Revolution Values through Hajj

Based on the Theory of Diffusion. *Journal of contemporary Research on Islamic revolution*. 2(3), pp. 103-119.

Moreno, A. P. (2017). La reconfiguración de Arabia Saudí. Del «modelo de los tres pactos» a la «visión 2030». *Repositorio comillas*. N.º 5, pp. 464-477.

Nasser, S. (2024). The winds of normalization: reshaping Saudi Arabia's image [en línea]. Carnegie endowment for international peace. [Consulta: 13 septiembre 2024]. Disponible en: https:// carnegieendowment. org/sada /2024/03/ the-winds-of- normalization-reshaping-saudi-arabias-image?lang=en

Navantia. (2024). Navantia construirá tres nuevas corbetas Avante 2200 para Arabia Saudí [en línea]. Navantia. [Consulta: 23 enero 2025]. Disponible en: https://www. Navantia . es / es / actualidad/ notas-prensa/navantia – construira - tres-nuevas -corbetas-avante-2200-para-arabia-saudi/

Nawaz, A. (2022). Normalization of Relations Between Saudi Arabia & Israel: Assessment of Critical Aspects. *International journal pf advanced academic studies.* 4(3), pp. 170-179.

NCA. (2018). Essential Cybersecurity Controls. National Cybersecurity Authority, pp. 1-35.

Noraini Z., Ridzuan M., Ariffin M. (2023). Iran and Oman conflict in the Strait of Hormuz: the potential for cooperation. *International Journal of Education and Humanities*. 3(1), pp. 24-42.

Obaid, N. (2014). *A saudi arabian defense doctrine: mapping the expanded force structure the kingdomneeds to lead the arab world, stabilize the region, and meet its global responsibilities*. Cambridge, Harvard University.

Orus, A. (2024). *Volumen de productos petrolíferos exportados desde España 2005-2023*. Madrid, Statista.

Raydan N. (2024). Los ataques hutíes y el transporte marítimo [en línea]. Afkar-Ideas. [Consulta: 2 noviembre 2024]. Disponible en: https://www.iemed.org/publication/los-ataques-huties-y-el-transporte-maritimo/

Saab, B (2023). Saudi Arabia's deterrence options against Iran. *Middle East Institute*. N.º 3, pp. 1-12.

Salimi, H. y Dareini, A. (2023). Scrutinizing Iran's Strategy of Latent Nuclear Deterrence. *SCIREA Journal of Sociology*. 7(4), pp. 257-276.

Satam, P. (2024). La Fuerza Aérea Saudita selecciona dron de reconocimiento chino Wing Loong-10B [en línea]. Galax-

ia Militar. [Consulta: 16 diciembre 2024]. Disponible en: https:// galaxiamilitar.es/la-fuerza-aerea-saudita-selecciona-el-dron-de-reconocimiento -chino-wing-loong-10b/

SASREF. (2026). Saudi Aramco Shell Refinery Company (SASREF) [en línea]. SASREF. [Consulta: 16 julio 2026]. Disponible en: https://sasref.com.sa/

Satorp. (2024). The Saudi Aramco Total Refining and Petrochemical Company [en línea]. Satorp. [Consulta: 12 febrero 2025]. Disponible en https://www.satorp.com/

Techsciresearch. (2024). *Saudi arabia operational technology market*. Nueva York, Techsciresearch

Tetsuro Sumida, J. (2006). Geography, technology, and british naval strategyin the dreadnought era. *Naval War College Review*. 59(3), pp. 89-102.

The guardian. (2022). Fire breaks out at Jeddah oil depot before Saudi Arabia grand prix [en línea]. The guardian. [Consutlta: 24 noviembre 2024]. Disponible en: https://www. The guardian .com /world / 2022 / mar / 25 / fire - breaks- out- at- jeddah-oil-depot-ahead-of-saudi-arabia -grand-prix

The New Arab. (2024). Iran, Saudi Arabia reportedly plan joint military exercises in Red Sea [en línea]. The New Arab. [Consulta: 5 enero 2025]. Disponible en: https://www.newarab.com/news/iran-saudi-reportedly-plan-joint-red-sea-military-exercises

Theran Times. (2024). Iran's Navy unveils plans for new submarines, expanded global presence [en línea]. Theran Times. [Consulta: 9 febrero 2025]. Disponible en: https://www.tehrantimes.com/news/506660/Iran-s-Navy-unveils-plans-for-new-submarines-expanded-global

Times Aerospace. (2024). WDS: UK moves in on new Saudi Typhoon order [en línea]. Times Aerospace. [Consulta: 19 marzo 2025]. Disponible en: https://www.timesaerospace. aero/news/events/wds-uk-moves-in-on-new-saudi-typhoon-order

Torregrosa Ramos, N. (2023a). Arabia Saudí, una acción exterior polifacética. *Boletín IEEE*. N.º 32, pp. 402-409.

—. (2023b). La Visión 2030 en Arabia Saudí. *Boletín IEEE*. N.º 22, pp. 1-18.

Villaverde, J. A. N. (2019). Abqaiq: ataque al corazón del sistema saudí [en línea]. Real Instituto Elcano. [Consulta: 20 septiembre 2024]. Disponible en: https://www.realinstitutoelcano.

org/comentarios/abqaiq-ataque-al-corazon-del-sistema-saudi/

Wezeman, P. D. (2018). Saudi Arabia, armaments and conflict in the Middle East [en linea]. SIPRI. [Consulta: 11 septiembre 2024]. Disponible en: https ://www.sipri .org/ commentary/ topical-backgrounder /2018/saudi-arabia-armaments-and-conflict-middle-east

Wezeman. P. et al. (2024). Trends in international arms transfer, 2023 [en línea]. SIPRI. [Consulta: 14 noviembre 2024]. Disponible en: https:// www.sipri.org /publications /2024/ sipri-fact-sheets/ trends-international-arms-transfers-2023

Wright, J. (2024). U.S. Marines Complete Historic Exercise Native Fury 24 In Saudi Arabia and United Arab Emirates [en línea]. Marines. [Consulta: 10 diciembre 2024]. Disponible en https://www.2ndmlg.marines.mil/News/Article/Article/3793130/us-marines-complete-historic-exercise-native-fury-24-in-saudi-arabia-and-united/

Capítulo décimo

Hacia un nuevo modelo de colaboración entre Fuerzas Armadas y fuerzas y cuerpos de seguridad en la seguridad pública en España

Juan Miguel Planchuelo Castiñeira

Resumen

El presente trabajo analiza el impacto que supondría una mayor participación de las Fuerzas Armadas en la seguridad pública en España, examinando su encaje constitucional, su desarrollo normativo y sus implicaciones operativas y democráticas. Partiendo de la evolución del concepto de seguridad pública hacia un enfoque más amplio de seguridad nacional, el estudio aborda la progresiva integración de capacidades civiles y militares ante amenazas complejas, como el terrorismo, las emergencias sanitarias, las catástrofes naturales o las amenazas híbridas.

El marco constitucional español establece una diferenciación funcional clara entre defensa nacional y seguridad interior, reservando esta última a las Fuerzas y Cuerpos de Seguridad. No obstante, la legislación posterior, especialmente la Ley Orgánica 5/2005, la Ley 36/2015 de Seguridad Nacional y la Ley Orgánica 4/1981, permite la intervención de las Fuerzas Armadas en situaciones excepcionales, siempre bajo los principios de subsidiariedad, excepcionalidad y mando civil.

Este estudio examina también experiencias recientes en España, como la Operación Balmis durante la pandemia de COVID-19,

la actuación ante incendios forestales o grandes emergencias, destacando el papel de la Unidad Militar de Emergencias como modelo especializado de apoyo. Asimismo, se realiza un análisis comparado con Francia, Italia y Reino Unido, identificando enseñanzas aplicables al caso español.

Finalmente, se analizan los riesgos que pueden implicar una mayor participación militar en la seguridad pública, como la posible pérdida del carácter excepcional de su intervención, la confusión de competencias entre instituciones y su impacto en la sociedad.

Para ello, se proponen principios rectores y condiciones básicas para articular un modelo de colaboración estructurada, apoyado en un marco normativo claro que refuerce la capacidad de respuesta del Estado. Asimismo, se señala que dicha participación podría integrarse de forma coherente en el modelo constitucional español, siempre que mantenga un carácter complementario y temporal, además de estar plenamente sometida al control civil y jurídico y no afecte al equilibrio institucional, a los derechos fundamentales ni a los valores democráticos.

Palabras clave

Seguridad nacional, Seguridad pública, Fuerzas Armadas, Control civil, Excepcionalidad.

Towards a New Model of Collaboration Between the Armed Forces and the Law Enforcement Agencies in Public Security in Spain

Abstract

This paper analyses the impact of increased participation of the Armed Forces in public security in Spain would have, examining its constitutional framework, its regulatory development, and its operational and democratic implications. Starting from the evolution of the concept of public security toward a broader notion of national security, the study addresses the progressive integration of civilian and military capabilities in response to complex

threats such as terrorism, health emergencies, natural disasters, and hybrid threats.

The Spanish constitutional framework establishes a clear functional distinction between national defence and internal security, reserving the latter to the State Security Forces and Corps. However, subsequent legislation, particularly Organic Law 5/2005, Law 36/2015 on National Security, and Organic Law 4/1981, allows for the intervention of the Armed Forces in exceptional situations, always under the principles of subsidiarity, exceptionality, and civilian command.

This study also examines recent experiences in Spain, such as Operation Balmis during the COVID-19 pandemic, responses to wildfires and major emergencies, highlighting the role of the Military Emergency Unit as a specialized support model. In addition, a comparative analysis is conducted with France, Italy, and the United Kingdom, identifying lessons applicable to the Spanish case.

Finally, the paper analyses the risks associated with greater military involvement in public security, such as the potential loss of the exceptional nature of their intervention, the blurring of institutional responsibilities, and its impact on society.

To this end, guiding principles and basic conditions to articulate a model of structured collaboration, supported by a clear regulatory framework that strengthens the State's response capacity. It is also noted that such participation could be coherently integrated into the Spanish constitutional model, provided that it maintains a complementary and temporary character, is fully subject to civilian and legal control, and does not affect the institutional balance, fundamental rights, or democratic values.

Key words

National security, Public security, Armed Forces, Civilian control, Exceptionality.

1 Introducción

La seguridad pública ha sido históricamente una función esencial del Estado y un elemento clave de su legitimidad. Desde el inicio del pensamiento político moderno, garantizar la seguridad se ha vinculado a la preservación del orden y a la protección de la sociedad frente a la violencia.

Thomas Hobbes sostuvo que, sin un poder capaz de imponer la paz, la sociedad quedaría expuesta al conflicto permanente. En esta visión, la seguridad se configura como el fundamento mismo de la organización política y de la autoridad del Estado (Hobbes, 1651).

El pensamiento liberal introdujo posteriormente una concepción distinta de la seguridad pública. Se defendió que la finalidad principal del Estado era la protección de los derechos naturales, especialmente la vida, la libertad y la propiedad. La seguridad dejó así de entenderse solo como control y pasó a concebirse como una garantía al servicio de los ciudadanos (Locke, 1690).

Desde entonces, la evolución de las políticas de seguridad en los Estados democráticos ha estado marcada por una tensión constante entre protección y libertad. Esta tensión continúa siendo un elemento central en el debate contemporáneo sobre la seguridad pública (Locke, 1690).

En las sociedades actuales, el concepto de seguridad pública se ha ampliado de forma significativa. Ya no se limita al mantenimiento del orden o a la respuesta frente al delito, sino que incorpora la gestión de riesgos complejos y amenazas de alcance global (Beck, 1992).

Ulrich Beck describió estos riesgos como difusos, globales y difícilmente previsibles, superando los marcos tradicionales de actuación estatal. Esta evolución ha contribuido a diluir las fronteras clásicas entre seguridad interior y otros ámbitos de la acción pública.

En España, este proceso se ha reflejado en una progresiva integración de la seguridad pública dentro de un enfoque más amplio de seguridad nacional. La Constitución española establece una diferenciación funcional clara entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad, asignando funciones distintas a cada una.

No obstante, el desarrollo normativo posterior ha incorporado una visión más integrada de la respuesta del Estado frente a determinadas amenazas. Este enfoque reconoce que, en situaciones concretas, resulta necesaria la coordinación de distintos instrumentos y capacidades (Ley Orgánica 5/2005).

Esta concepción se consolida en las Estrategias de Seguridad Nacional, que entienden la seguridad como una política de Estado de carácter transversal. En este marco, se subraya la necesidad de una acción coordinada de los distintos actores públicos.

La seguridad nacional implica la integración coherente de recursos civiles y militares bajo dirección política y dentro de un marco jurídico común. Esta aproximación responde a la complejidad del entorno estratégico actual y a la naturaleza híbrida de muchas amenazas.

Sin embargo, la ampliación del concepto de seguridad no está exenta de riesgos. Cuando la seguridad se utiliza de forma continua como justificación de la acción del Estado, las medidas excepcionales tienden a prolongarse y a erosionar las garantías del Estado de derecho.

Por ello, cualquier análisis sobre la participación de las Fuerzas Armadas en la seguridad pública debe abordarse desde una perspectiva crítica. Resulta imprescindible atender tanto a su encaje jurídico como a su legitimidad democrática y social.

A partir de este marco, el presente trabajo analiza el impacto de una mayor participación de las Fuerzas Armadas en la seguridad pública en España, atendiendo a su encaje jurídico, a su justificación operativa y a sus implicaciones democráticas, con el objetivo de valorar si este fenómeno puede integrarse de forma coherente en el modelo constitucional vigente.

2 La seguridad pública en el contexto de la seguridad nacional

2.1 La evolución del concepto de seguridad pública

Tradicionalmente, la seguridad ha constituido una preocupación central en la organización de las sociedades. En los primeros sistemas políticos, esta función recaía principalmente en comunidades locales y en estructuras estatales incipientes, cuyo objetivo fundamental era garantizar la convivencia y el orden social.

Con el proceso de consolidación del Estado, la seguridad pública pasó a entenderse progresivamente como una función esencial de la autoridad estatal, orientada a garantizar el orden social y la protección de las personas frente a amenazas internas, dando lugar al desarrollo de diversas concepciones sobre el papel del poder en su provisión.

Durante el siglo XVII, Thomas Hobbes (1651) argumentó que solo un Estado con control absoluto podía evitar el caos y la violencia, justificando así la concentración del poder en un soberano.

En el pensamiento contractualista, la seguridad pública se concibió como un elemento legitimador del Estado. En este marco, John Locke sostuvo que la principal finalidad del poder político es la protección de los derechos naturales, vida, libertad y propiedad, de modo que la seguridad deja de ser solo un instrumento de control y pasa a entenderse como una garantía al servicio de los ciudadanos (Locke, 1690).

Posteriormente, Montesquieu aportó una concepción más equilibrada de la seguridad al advertir sobre los riesgos inherentes a la concentración del poder. Desde su perspectiva, la preservación del orden y la seguridad debía ser compatible con la garantía de las libertades individuales, lo que exigía la separación de poderes como mecanismo para evitar que la búsqueda de seguridad derivase en formas de arbitrariedad o tiranía (Montesquieu, 1748).

Con la consolidación del Estado moderno, la seguridad pública se institucionalizó de forma progresiva, pasando a vincularse a estructuras permanentes de control y coerción.

En los siglos XIX y XX, los procesos de urbanización e industrialización impulsaron la creación de cuerpos policiales y sistemas penales orientados sobre todo al control del delito y al mantenimiento del orden interno, lo que reforzó una concepción de la seguridad predominantemente represiva y centrada en la disciplina social (Foucault, 1977).

Asimismo, Ulrich Beck (1992) aportó la teoría de la sociedad del riesgo, evidenciando cómo la gestión del riesgo ha ampliado las funciones del Estado en materia de seguridad.

Más recientemente, Agamben (2005) argumentó que los Estados han utilizado la seguridad como pretexto para suspender derechos y mantener un estado de emergencia permanente.

Esta evolución ha llevado a concebir la seguridad pública como parte de un enfoque más amplio, en el que convergen instrumentos civiles y militares y en el que la actuación del Estado requiere coordinación interinstitucional.

La seguridad deja así de centrarse en la reacción frente al delito para incorporar la prevención, la gestión del riesgo y la anticipación de amenazas como elementos centrales de la acción pública (Iglesias, 2011).

En conclusión, la evolución del pensamiento sobre seguridad refleja la tensión entre protección y control. Desde Hobbes hasta Agamben, se han desarrollado visiones diversas sobre cómo los Estados deben garantizar la estabilidad sin vulnerar las libertades individuales. En un mundo globalizado, estos debates siguen vigentes, influyendo en las políticas de seguridad actuales.

2.2 La seguridad nacional como política del Estado

Una vez ampliado el concepto de seguridad pública, los Estados han tendido a incorporarlo al núcleo de su acción política, configurando la seguridad nacional como una política pública de carácter transversal.

En este enfoque, la seguridad deja de ser una función sectorial limitada a ámbitos concretos, como la defensa o el orden público, y pasa a integrarse en el conjunto de las políticas del Estado, orientadas a garantizar la estabilidad institucional y la protección de la sociedad frente a amenazas complejas (Iglesias, 2011).

Desde esta perspectiva, la seguridad nacional se articula como una política que requiere dirección política, planificación estratégica y coordinación entre instituciones. La respuesta a los riesgos contemporáneos exige la implicación de múltiples actores estatales y la integración de capacidades civiles y militares bajo un marco común que permita una actuación coherente del Estado en su conjunto (Iglesias, 2011).

En el ámbito europeo, la seguridad nacional se ha integrado de forma estable en la acción ordinaria del Estado como una política transversal, basada en el refuerzo de capacidades y en una mayor coordinación administrativa. Este enfoque ha permitido superar respuestas limitadas a la gestión puntual de crisis. Al mismo tiempo, esta centralidad de la seguridad exige establecer límites claros para evitar un uso excesivo del control o la norma-

lización de medidas excepcionales que puedan afectar innecesariamente a la sociedad.

Por ello, resulta imprescindible que la seguridad nacional se ejerza dentro de marcos jurídicos bien definidos y con pleno respeto a los derechos y libertades fundamentales (Agamben, 2005).

En definitiva, la seguridad pública se ha convertido en un eje central de las políticas gubernamentales, en especial tras los atentados del 11 de septiembre de 2001. Además, la digitalización ha introducido nuevas problemáticas, entre ellas el uso de inteligencia artificial para la vigilancia y la recopilación masiva de datos personales, generando debates sobre los límites de la seguridad y la privacidad en las sociedades democráticas.

2.3 Relación entre seguridad interior y defensa nacional

A lo largo del tiempo, los Estados han establecido una distinción funcional entre seguridad interior y defensa nacional. La primera se ha vinculado al mantenimiento del orden público y a la protección de los ciudadanos frente a amenazas internas, mientras que la segunda se ha orientado a la protección del Estado frente a agresiones externas.

El entorno de seguridad actual ha difuminado la división clásica entre lo interno y lo externo. La aparición de amenazas de alcance transnacional ha obligado a los Estados a articular respuestas más coordinadas y flexibles, al afectar de forma simultánea a la seguridad interior y a la defensa nacional (Iglesias, 2011).

En el ámbito europeo, esta relación se articula cada vez más mediante fórmulas de cooperación entre la seguridad interior y la defensa. Los Estados han reforzado la coordinación y la integración de capacidades para afrontar riesgos que superan las funciones ordinarias de las fuerzas y cuerpos de seguridad, sin que ello implique una fusión de ambos ámbitos, sino una articulación complementaria basada en criterios de necesidad y proporcionalidad (Bigo, 2016).

La defensa nacional aporta capacidades, medios y estructuras orientadas a escenarios de alta complejidad, mientras que la seguridad interior mantiene su papel central en la protección cotidiana de los ciudadanos. La cooperación entre ambos ámbitos se justifica, por tanto, cuando las amenazas exceden el marco

ordinario de actuación y requieren una respuesta reforzada del Estado (Iglesias, 2011).

No obstante, algunas posturas críticas advierten de los riesgos que pueden surgir cuando las lógicas de seguridad propias de situaciones excepcionales se trasladan al ámbito interno. En este sentido, Foucault señala que este desplazamiento puede favorecer un aumento de los mecanismos de control social y una mayor intervención del Estado sobre la población (Foucault, 1977).

En una línea complementaria, Agamben advierte del riesgo de que la excepcionalidad asociada a la defensa se convierta en algo habitual cuando sus instrumentos se aplican a la seguridad interior, lo que puede debilitar las garantías jurídicas y los límites al ejercicio del poder estatal (Agamben, 2005).

En consecuencia, la relación entre seguridad interior y defensa nacional se configura hoy como un equilibrio dinámico que exige marcos jurídicos claros, liderazgo político y mecanismos de control democrático.

Lejos de una confusión de funciones, se trata de una coordinación ordenada que permita al Estado responder eficazmente a amenazas complejas, preservando al mismo tiempo la diferenciación funcional y el respeto a los derechos fundamentales que caracterizan a los Estados democráticos (Iglesias, 2011).

3 Marco jurídico de la participación de las Fuerzas Armadas en seguridad pública en España

3.1 Fundamento constitucional de la actuación de las Fuerzas Armadas

El marco constitucional español define con claridad las funciones y límites de las Fuerzas Armadas, situándolas al servicio del orden constitucional. El artículo 8.1 de la Constitución les atribuye la defensa de la soberanía e independencia de España, la integridad territorial y el ordenamiento constitucional, lo que constituye el punto de partida para analizar su posible actuación en el ámbito de la seguridad pública.

Ahora bien, la Constitución no les asigna funciones ordinarias de mantenimiento del orden público. Esta responsabilidad corresponde, con carácter general, a las fuerzas y cuerpos de segu-

ridad, a las que el artículo 104 encomienda la protección de los derechos y libertades y la garantía de la seguridad ciudadana.

Esta diferenciación funcional refleja la voluntad del legislador de separar los ámbitos de la defensa nacional y de la seguridad interior en situaciones de normalidad constitucional.

En este punto, la Constitución no excluye de forma absoluta la actuación de las Fuerzas Armadas en el ámbito interior. El artículo 8.1 CE les atribuye la misión de salvaguardar el ordenamiento constitucional, sin distinguir entre amenazas internas o externas. Esta formulación permite interpretar que su intervención puede producirse en apoyo de las autoridades civiles cuando se ven comprometidos los fundamentos del Estado constitucional, siempre dentro del marco que establezca la legalidad vigente.

De igual modo, la Constitución contempla mecanismos excepcionales que permiten la participación de las Fuerzas Armadas en el ámbito de la seguridad interior. Los artículos 55 y 116 regulan los estados de alarma, excepción y sitio, estableciendo distintos grados de alteración del orden constitucional y habilitando, según su gravedad, una mayor intervención de los instrumentos del Estado, incluidas las Fuerzas Armadas.

En todos los casos, esta actuación queda sometida al control civil y a la legalidad vigente, lo que confirma el carácter excepcional y reglado de la participación militar en la seguridad pública.

En este marco, adquiere especial importancia el principio de subordinación de las Fuerzas Armadas al poder civil. El artículo 97 de la Constitución atribuye al Gobierno la dirección de la política interior y exterior y de la defensa del Estado, lo que implica que cualquier actuación de las Fuerzas Armadas en el ámbito de la seguridad pública debe desarrollarse bajo su autoridad y dentro del marco legal establecido. De este modo, la intervención militar queda integrada en una decisión política sujeta a control democrático y no responde a iniciativas autónomas o discrecionales.

En síntesis, el fundamento constitucional de la actuación de las Fuerzas Armadas en el ámbito de la seguridad pública descansa en una habilitación limitada y en una delimitación de funciones. La Constitución permite su intervención únicamente en situaciones excepcionales o como apoyo a las autoridades civiles, excluyendo su empleo como instrumento ordinario de seguridad ciudadana. Este planteamiento mantiene bajo control la actuación de las Fuerzas Armadas, refuerza la autoridad civil y preserva los lími-

tes entre defensa nacional y seguridad interior, con pleno respeto a los derechos fundamentales.

3.2 Marco normativo aplicable en seguridad pública

El marco normativo español establece un sistema escalonado y coherente para regular la participación de las Fuerzas Armadas en el ámbito de la seguridad pública, partiendo de la diferenciación funcional entre defensa nacional y seguridad interior.

Tras la habilitación constitucional analizada en el apartado anterior, corresponde a la legislación orgánica y ordinaria concretar los supuestos, límites y procedimientos que permiten la intervención militar en apoyo de las autoridades civiles.

En primer lugar, la Ley Orgánica 5/2005, de la Defensa Nacional, constituye la norma básica que regula la organización, misiones y empleo de las Fuerzas Armadas. Esta ley reafirma que su misión principal es garantizar la defensa de España y contribuir a la seguridad nacional, estableciendo que su actuación se realizará siempre bajo la dirección del Gobierno y conforme a los principios constitucionales.

Aunque no atribuye a las Fuerzas Armadas funciones ordinarias de seguridad pública, sí contempla su participación en apoyo a otras autoridades cuando así lo exijan las circunstancias y lo disponga el Gobierno.

Por su parte, la Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad, sitúa la seguridad pública como una función propia de los cuerpos policiales, tanto estatales como autonómicos y locales, dentro de sus respectivas competencias. De este modo, el mantenimiento del orden público y de la seguridad ciudadana queda, con carácter general, en manos de cuerpos de naturaleza civil, permaneciendo la actuación de las Fuerzas Armadas fuera del ejercicio ordinario de estas funciones.

Un elemento central del marco normativo es la Ley 36/2015, de Seguridad Nacional, que adopta una visión más amplia de la seguridad y establece mecanismos de coordinación entre los distintos instrumentos del Estado. Esta norma no atribuye funciones policiales a las Fuerzas Armadas ni militariza la seguridad pública, pero sí prevé la movilización de recursos y capacidades, incluidas las militares, cuando la gravedad de la situación lo exige. De este modo, se encuadra su posible participación en

apoyo de la seguridad interior dentro de un sistema de dirección política y coordinación claramente definido.

Asimismo, la normativa reguladora de los estados de alarma, excepción y sitio, desarrollada por la Ley Orgánica 4/1981, constituye un instrumento jurídico esencial para la participación de las Fuerzas Armadas en el ámbito interior. En función del estado declarado y de la intensidad de la crisis, esta ley permite ampliar el papel de las Fuerzas Armadas, siempre bajo control civil, con respeto a la legalidad y con sujeción a los límites temporales y materiales establecidos por la Constitución.

Finalmente, debe tenerse en cuenta que toda actuación de las Fuerzas Armadas en seguridad pública se encuentra sometida al conjunto del ordenamiento jurídico, incluidos los principios de legalidad, proporcionalidad y control jurisdiccional.

La intervención militar en apoyo de la seguridad interior no se produce en un vacío normativo, sino dentro de un marco jurídico detallado que busca compatibilizar la eficacia de la respuesta del Estado con la protección de los derechos fundamentales y el respeto al modelo democrático.

3.3 Principios de subsidiariedad, excepcionalidad y mando civil

La participación de las Fuerzas Armadas en la seguridad pública se encuentra condicionada por una serie de principios jurídicos que se derivan directamente del marco constitucional y legal. La Constitución asigna a las Fuerzas Armadas la defensa de la soberanía, la integridad territorial y el ordenamiento constitucional, mientras que atribuye a las fuerzas y cuerpos de seguridad la protección de los derechos y la seguridad ciudadana.

Esta separación de funciones constituye la base sobre la que se apoyan los principios que regulan una eventual intervención militar, posteriormente desarrollados por la legislación en materia de defensa y seguridad.

El principio de subsidiariedad se desprende de esta distribución constitucional de funciones y supone que la intervención de las Fuerzas Armadas en seguridad pública solo resulta legítima cuando las capacidades disponibles de las fuerzas y cuerpos de seguridad resultan insuficientes para hacer frente a una situación concreta.

Este enfoque se refuerza en la Ley Orgánica 5/2005, de la Defensa Nacional, que concibe el empleo de las Fuerzas Armadas como un instrumento al servicio del Estado bajo dirección gubernamental, y en la Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad, que reserva el ejercicio habitual de la seguridad ciudadana a cuerpos de naturaleza civil.

De forma complementaria, el principio de excepcionalidad establece que la actuación de las Fuerzas Armadas en el ámbito interior no tiene carácter ordinario. Su participación solo se justifica ante situaciones de especial gravedad y con carácter temporal y limitado.

Este criterio se recoge en el régimen de los estados de alarma, excepción y sitio, regulado en los artículos 55 y 116 de la Constitución y desarrollado por la Ley Orgánica 4/1981, que prevé distintos niveles de respuesta en función de la gravedad de la situación.

El principio de mando civil garantiza que cualquier actuación de las Fuerzas Armadas en apoyo de la seguridad pública se realice bajo la autoridad civil. Según el artículo 97 de la Constitución, corresponde al Gobierno la dirección de la política interior, exterior y de la defensa, lo que excluye cualquier intervención militar autónoma. En la misma línea, la Ley Orgánica 5/2005 sitúa a las Fuerzas Armadas bajo la dependencia directa del Gobierno y supedita su actuación a las decisiones adoptadas por las autoridades civiles competentes.

En conclusión, la aplicación conjunta de los principios de subsidiariedad, excepcionalidad y mando civil permite articular un modelo de intervención militar compatible con el orden constitucional. Su función queda así sometida al control democrático y al respeto de los derechos fundamentales, así como a los mecanismos de control democrático previstos en el ordenamiento jurídico, en particular los derivados del control parlamentario y jurisdiccional de la actuación del Gobierno conforme a la Constitución y a la Ley 36/2015, de Seguridad Nacional.

3.4 Límites jurídicos y garantías democráticas

La participación de las Fuerzas Armadas en el ámbito de la seguridad pública se encuentra sujeta a límites jurídicos precisos, derivados del Estado social y democrático de derecho proclamado en el artículo 1.1 de la Constitución española.

Estos límites tienen como finalidad garantizar que el empleo de los instrumentos militares en el ámbito interior no altere el equilibrio institucional ni suponga una restricción indebida de los derechos fundamentales.

Uno de los principales límites viene determinado por el principio de legalidad, conforme al que toda actuación de los poderes públicos debe estar expresamente prevista en la ley.

En este sentido, cualquier intervención de las Fuerzas Armadas en apoyo de la seguridad pública debe contar con una habilitación normativa clara y ajustarse estrictamente a las condiciones y procedimientos establecidos en la Constitución y en la legislación orgánica aplicable, en particular la Ley Orgánica 5/2005, de la Defensa Nacional, y la Ley 36/2015, de Seguridad Nacional.

La protección de los derechos fundamentales constituye otro límite esencial a la actuación militar en el ámbito interior. Incluso en situaciones excepcionales, la Constitución establece que los derechos solo pueden ser restringidos en los términos expresamente previstos en los artículos 55 y 116 CE y conforme a los principios de necesidad y proporcionalidad.

La intervención de las Fuerzas Armadas no puede justificar, por sí sola, la suspensión o limitación generalizada de derechos fuera de los supuestos constitucionalmente previstos.

Asimismo, la actuación de las Fuerzas Armadas en seguridad pública se encuentra sometida a control parlamentario. El Gobierno, como autoridad responsable de la dirección política y de la defensa del Estado (art. 97 CE), debe rendir cuentas ante las Cortes Generales sobre las decisiones adoptadas, especialmente cuando estas implican el empleo de medios militares en el ámbito interior o la declaración de estados excepcionales conforme a la Ley Orgánica 4/1981.

Junto con el control parlamentario, opera el control jurisdiccional de la actuación del poder ejecutivo. Los tribunales, y en particular el Tribunal Constitucional, garantizan que las medidas adoptadas se ajusten a la Constitución y que no se produzcan vulneraciones de derechos fundamentales. Este control judicial refuerza el carácter garantista del sistema y actúa como contrapeso frente a posibles excesos en el uso de los instrumentos de seguridad.

Finalmente, estos límites y garantías configuran un marco jurídico destinado a evitar la normalización de la intervención militar en tareas de seguridad pública. La combinación de legalidad, control

democrático y protección de los derechos fundamentales asegura que la participación de las Fuerzas Armadas se mantenga dentro de los márgenes propios de un Estado democrático de derecho, preservando la primacía del poder civil y la excepcionalidad del empleo militar en el ámbito interior.

4 Capacidades de las Fuerzas Armadas aplicables a la seguridad pública en España

4.1 Capacidades de despliegue, apoyo logístico y apoyo operativo

Las Fuerzas Armadas españolas están preparadas para actuar en escenarios de alta exigencia, tanto en el exterior como en el interior del territorio nacional, siempre en los términos previstos por la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

Esta preparación las convierte en un recurso estratégico del Estado que, empleado de forma adecuada y bajo dirección civil, puede resultar decisivo ante situaciones de grave impacto para la seguridad colectiva (Ministerio de Defensa, 2018).

Una de sus principales fortalezas es la capacidad de despliegue y sostenimiento logístico. Las Fuerzas Armadas disponen de medios propios para proyectar personal y recursos con rapidez, establecer hospitales de campaña, asegurar el abastecimiento de víveres y medicamentos y crear centros de mando y coordinación en zonas afectadas.

Estas capacidades permiten actuar incluso cuando las infraestructuras civiles se encuentran dañadas o colapsadas, como ha quedado acreditado en situaciones de emergencia y catástrofes recientes (Salvador, Almaraz y Penilla, 2021).

Junto con el componente logístico, destaca la formación continuada en gestión de crisis y operaciones complejas. El personal militar está entrenado para actuar en entornos de alta presión, con procedimientos normalizados, disciplina operativa y una clara cadena de mando.

Esta estructura facilita su integración rápida en dispositivos interinstitucionales y su actuación coordinada con autoridades civiles, incluso en contextos caracterizados por la incertidumbre y

por escenarios de desorden derivados del carácter excepcional de los hechos (López, 2023).

Igualmente, las Fuerzas Armadas cuentan con capacidades tecnológicas avanzadas que refuerzan su valor como apoyo a la seguridad pública. Entre ellas, se incluyen sistemas de mando y control, comunicaciones seguras, medios de vigilancia y reconocimiento, empleo de drones y unidades especializadas en riesgos NBQ (nuclear, biológico y químico). Estas capacidades permiten complementar eficazmente la actuación de los cuerpos civiles en situaciones de especial sensibilidad o riesgo elevado (Martínez, 2015).

En conjunto, estas capacidades de despliegue, logística, tecnología y apoyo operativo configuran a las Fuerzas Armadas como un instrumento idóneo para prestar apoyo a la seguridad pública en situaciones excepcionales. Su empleo bajo dirección civil permite reforzar la respuesta del Estado sin sustituir las funciones propias de las fuerzas y cuerpos de seguridad, contribuyendo así a una gestión más eficaz de crisis de gran complejidad (Ministerio de Defensa, 2018).

4.2 La Unidad Militar de Emergencias como referencia operativa

La Unidad Militar de Emergencias constituye el principal referente operativo de la participación de las Fuerzas Armadas españolas en el ámbito de la seguridad pública. Creada en 2005, la Unidad Militar de Emergencias se concibió como una fuerza conjunta, permanente y especializada, destinada a intervenir en situaciones de grave riesgo, catástrofe o calamidad pública, tanto en territorio nacional como en el exterior, en apoyo de las autoridades civiles y de los sistemas de protección civil, conforme a lo dispuesto en el Real Decreto 416/2006.

La creación de la Unidad Militar de Emergencias respondió a la necesidad de reforzar la respuesta del Estado ante emergencias de gran magnitud como incendios forestales, inundaciones o riesgos tecnológicos.

Las Fuerzas Armadas contaban con capacidades específicas, como la rapidez de despliegue, la concentración de medios, la autonomía logística y la disciplina operativa, que permitían asumir una función especializada en este ámbito sin alterar su misión principal de defensa nacional (Pérez *et al*., 2022).

Este despliegue operativo se apoya en un marco jurídico propio que se ha ido consolidando de forma progresiva. El Real Decreto 1097/2011 aprobó su protocolo de intervención, delimitando las situaciones en las que puede ser activada y el tipo de actuaciones que puede desarrollar.

Posteriormente, la Ley 17/2015, del Sistema Nacional de Protección Civil, reforzó este modelo al reconocer a la Unidad Militar de Emergencias como servicio público de intervención y asistencia en emergencias, de acuerdo con lo previsto en dicha ley y en disposiciones posteriores como la Orden DEF/160/2019.

La estructura territorial de la Unidad Militar de Emergencias, con cinco batallones de Intervención en Emergencias distribuidos por el territorio nacional, permite su despliegue en plazos muy reducidos, generalmente inferiores a cuatro horas.

Esta organización, unida a su cadena de mando específica y a sus capacidades de mando y control, facilita una respuesta rápida y coordinada ante emergencias complejas que superan las capacidades habituales de las administraciones civiles (Orden DEF/160/2019).

La Unidad Militar de Emergencias ha desarrollado su actuación en escenarios operativos diversos, tanto en el ámbito nacional como en el internacional, configurando un modelo de intervención orientado al apoyo a las autoridades civiles en situaciones de emergencia (Pérez *et al*., 2022).

La actuación de la Unidad Militar de Emergencias durante crisis recientes de gran impacto, como la Operación Balmis[87] durante la pandemia de COVID-19, la borrasca Filomena o la erupción volcánica de La Palma, ha puesto de manifiesto su capacidad para integrarse eficazmente en dispositivos interinstitucionales complejos.

Estas intervenciones han reforzado su legitimidad social y han contribuido a mejorar la percepción pública de las Fuerzas Armadas como instrumento al servicio de la ciudadanía en situaciones excepcionales (Martínez *et al*., 2024).

[87] La Operación Balmis, lanzada en marzo de 2020, fue un despliegue militar para combatir la propagación del COVID-19 en España. Su nombre rinde homenaje al médico militar Francisco Javier de Balmis, quien llevó la vacuna de la viruela a América y Filipinas.

Los estudios comparados destacan que el modelo español de la Unidad Militar de Emergencias se basa en una unidad militar especializada y claramente definida. Este enfoque evita la atribución indiscriminada de funciones de emergencia a unidades sin preparación específica y permite mantener una intervención militar acotada y bajo control civil en situaciones de emergencia (Martínez *et al*., 2024).

En conjunto, la Unidad Militar de Emergencias representa un ejemplo consolidado de cómo las Fuerzas Armadas pueden contribuir a la seguridad pública sin asumir funciones policiales ni alterar el principio de excepcionalidad. Su existencia permite canalizar la participación militar en emergencias de forma ordenada, jurídicamente delimitada y socialmente legitimada, constituyendo un referente operativo clave dentro del modelo español de colaboración entre defensa y seguridad pública (Pérez y Valiño, 2022).

5 La participación reciente de las Fuerzas Armadas en la seguridad pública en España

5.1 Actuaciones recientes de las fuerzas armadas en el ámbito interior

La seguridad pública en España se apoya en un marco normativo que regula la colaboración entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad en situaciones excepcionales, siempre bajo control civil. La Constitución delimita las competencias en materia de seguridad y defensa y, a través del artículo 8, permite la intervención de las Fuerzas Armadas en circunstancias extraordinarias cuando se vean comprometidos el orden constitucional o la integridad territorial.

En este contexto normativo, la colaboración entre las Fuerzas Armadas y los cuerpos de seguridad ha demostrado ser crucial en escenarios críticos recientes. La Ley Orgánica 4/1981, que regula los estados de alarma, excepción y sitio, establece las condiciones jurídicas para que las Fuerzas Armadas apoyen a las fuerzas y cuerpos de seguridad en contextos de grave riesgo.

Esta normativa resultó esencial durante la pandemia de COVID-19 para habilitar la Operación Balmis, en la que las Fuerzas Armadas llevaron a cabo labores de desinfección de instalaciones, apoyo

logístico sanitario y transporte de suministros médicos en todo el territorio nacional.

Otro ejemplo significativo de actuación reciente fue el apagón eléctrico masivo del 28 de abril de 2025[88], que afectó simultáneamente a buena parte del territorio nacional, así como a regiones del sur de Francia y Portugal.

La magnitud del suceso llevó a varias Comunidades Autónomas a solicitar el apoyo del Gobierno central, activándose el nivel 3 de emergencia y declarándose la situación de interés nacional mediante la Orden INT/399/2025, conforme al artículo 30 de la Ley 17/2015 del Sistema Nacional de Protección Civil.

El Ministerio del Interior asumió la dirección de la respuesta y coordinó los recursos civiles y militares, entre ellos la Unidad Militar de Emergencias y otras capacidades del Ejército, que participaron en tareas de seguridad, abastecimiento, rescate y asistencia a la población.

Asimismo, las Fuerzas Armadas intervinieron de forma destacada durante la campaña de incendios forestales del verano de 2025[89], caracterizada por la simultaneidad y la intensidad de los fuegos en amplias zonas del territorio nacional. La Unidad Militar de Emergencias y otros efectivos militares fueron activados para apoyar a los servicios civiles en tareas de extinción, protección de poblaciones, apoyo logístico y vigilancia, reforzando la respuesta del Estado ante una emergencia de gran alcance.

Estas actuaciones conjuntas pusieron de relieve la importancia de contar con mecanismos ágiles de cooperación interinstitucional, así como la utilidad de redefinir de forma estructurada el papel de las Fuerzas Armadas en la respuesta a crisis complejas que comprometen el funcionamiento esencial del Estado.

Más allá de las emergencias puntuales, la Ley 36/2015, de Seguridad Nacional, encuadra la colaboración de las Fuerzas Armadas con las fuerzas y cuerpos de seguridad en ámbitos como la protección de infraestructuras críticas y la seguridad

[88] El apagón en el suroeste de Europa de 2025 fue una interrupción masiva en el suministro eléctrico que ocurrió el 28 de abril de 2025 a las 12:33 horas, que afectó a España, Portugal, y al suroeste de Francia.

[89] Los incendios forestales de 2025 fueron una serie de grandes fuegos que afectaron a la península desde julio de ese año, quemando cerca de cuatrocientas mil hectáreas, la peor campaña en más de treinta años, con especial incidencia en Orense, León y Zamora.

de eventos de alto riesgo, mediante mecanismos de cooperación interinstitucional. En este mismo ámbito, la Ley 8/2011 y el Real Decreto 704/2011 regulan la protección de infraestructuras esenciales, previendo la participación de las Fuerzas Armadas junto con organismos civiles en los sectores estratégicos identificados, algunos de ellos bajo responsabilidad directa del Ministerio de Defensa.

España se enfrenta, además, a una serie de amenazas que afectan de forma directa a su seguridad nacional, entre las que destacan el terrorismo, la inmigración irregular, el narcotráfico y las ciberamenazas.

El terrorismo continúa siendo una de las principales amenazas a la seguridad pública y, tras los atentados del 11 de marzo de 2004, se reforzó el marco legal para facilitar una mejor incorporación de las Fuerzas Armadas en tareas de apoyo, especialmente en la protección de infraestructuras críticas y el respaldo a las Fuerzas y Cuerpos de Seguridad (ver figura 1).

En niveles elevados de alerta antiterrorista, las Fuerzas Armadas pueden ser activadas para reforzar la seguridad de infraestructuras sensibles y contribuir a la vigilancia de puntos estratégicos. El Plan de Prevención y Protección Antiterrorista, actualizado mediante la Instrucción 2/2022 de la Secretaría de Estado de Seguridad, contempla esta posibilidad en su nivel 5 de riesgo muy alto, si bien hasta la fecha no ha sido necesaria su aplicación efectiva.

Otro desafío relevante en el ámbito de la seguridad interior es la gestión de la inmigración irregular, especialmente debido a la posición geográfica estratégica de España. La presión migratoria en determinadas zonas ha reforzado la coordinación entre instituciones y ha abierto el debate sobre el apoyo de las Fuerzas Armadas en tareas de vigilancia marítima y control de espacios estratégicos, siempre como complemento a la actuación de las autoridades civiles (Infobae, 2024).

Un ejemplo reciente de esta necesidad de coordinación se produjo en Ceuta a finales de julio de 2026, cuando la entrada irregular de miles de personas procedentes de Marruecos desbordó las capacidades ordinarias de respuesta en la ciudad autónoma. La magnitud del episodio, que provocó la saturación de los dispositivos de acogida y obligó a concentrar los recursos de las fuerzas y cuerpos de seguridad y de los servicios de emergencia en la atención y control de la situación, llevó al Gobierno a movilizar

unidades del Ejército de Tierra desplegadas en Ceuta para prestar apoyo a los efectivos de las fuerzas y cuerpos de seguridad. El presidente de la Ciudad Autónoma solicitó, además, la decla-



Figura 1. Dispositivo conjunto de FCS y FAS en la protección de infraestructuras críticas

ración de emergencia nacional y la asunción de un mando único por parte del Gobierno (Morán, 2026).

Este episodio constituye un ejemplo especialmente significativo de la convergencia entre seguridad interior y defensa en escenarios de especial gravedad. La intervención de las Fuerzas Armadas no supuso la asunción ordinaria de competencias policiales, sino la utilización temporal de capacidades militares para reforzar la respuesta del Estado ante una situación de carácter extraordinario. El caso de Ceuta pone así de manifiesto la utilidad de disponer de mecanismos previamente definidos de coordinación entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad, particularmente en territorios fronterizos de especial relevancia estratégica.

El narcotráfico constituye igualmente un problema relevante para la seguridad nacional que requiere una respuesta coordinada entre las fuerzas y cuerpos de seguridad y las Fuerzas Armadas. Si bien la seguridad ciudadana corresponde a los cuerpos policiales, las Fuerzas Armadas han asumido funciones de apoyo en la vigilancia de infraestructuras críticas y en operaciones conjuntas

contra el crimen organizado, tal y como señalan diversos estudios comparados sobre seguridad y defensa (EU-LAC Foundation, 2023).

La creciente capacidad operativa de las organizaciones dedicadas al narcotráfico, especialmente en el litoral del sur de España, ha incrementado el nivel de riesgo para los agentes encargados de combatir este fenómeno. Los graves sucesos registrados recientemente durante una persecución de una narcolancha frente a las costas de Huelva, en los que fallecieron dos agentes de la Guardia Civil y otros dos resultaron heridos, reflejan la peligrosidad de estas organizaciones y la complejidad de las operaciones desarrolladas en el ámbito marítimo. Este contexto pone de manifiesto la necesidad de seguir reforzando la coordinación institucional y los medios disponibles para hacer frente a este tipo de amenazas (El País, 2026).

En coherencia con este enfoque, la *Estrategia española de Seguridad Nacional* establece la necesidad de una respuesta integral frente a amenazas de diversa naturaleza. La interconexión entre terrorismo, inmigración irregular, crimen organizado y ciberamenazas justifica una mayor implicación de las Fuerzas Armadas en tareas de apoyo a la seguridad interior, siempre bajo el principio de cooperación y el respeto a las competencias de cada institución.

La Ley Orgánica 5/2005, de la Defensa Nacional, refuerza este planteamiento al asignar a las Fuerzas Armadas la misión de garantizar la soberanía, la independencia y la integridad territorial de España, previendo su participación en operaciones de vigilancia y protección de los espacios marítimos y aéreos como parte de la acción del Estado para prevenir amenazas.

En este marco, la Guardia Civil, de naturaleza militar, cumple una función relevante en la vigilancia costera y el control del tráfico marítimo, bajo la coordinación del Ministerio del Interior y, en determinados supuestos, con apoyo del Ministerio de Defensa, reforzando la cooperación entre instituciones.

En el ámbito del ciberespacio, la creación del Mando Conjunto del Ciberespacio[90] en 2020 permitió integrar las capacidades cibernéticas de las Fuerzas Armadas con las de las fuerzas y cuerpos

[90] El Mando Conjunto de Ciberespacio (MCCE), conocido hasta 2020 como Mando Conjunto de Ciberdefensa, es la unidad de las FAS encargada de coordinar la protección de redes y sistemas militares frente a ciberataques, así como de apoyar la defensa de infraestructuras críticas en colaboración con otras entidades nacionales.

de seguridad. Su colaboración con el Centro Criptológico Nacional y con Europol refuerza la protección de infraestructuras críticas frente a ciberamenazas, un ámbito cada vez más relevante para la seguridad nacional.

En conjunto, el modelo español de seguridad pública se apoya en una colaboración equilibrada entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad.

Su aplicación reciente ha mostrado resultados positivos en situaciones críticas, como la pandemia de COVID-19, el apagón eléctrico de 2025 o la lucha contra el terrorismo, aunque la delimitación de competencias sigue planteando retos que requieren una adaptación continua del marco jurídico y operativo para responder a amenazas emergentes sin afectar a los principios democráticos ni a los derechos fundamentales.

5.2 Lecciones aprendidas en el contexto español

La experiencia reciente en la participación de las Fuerzas Armadas en el ámbito interior pone de manifiesto, en primer lugar, la utilidad de contar con un marco jurídico previo y claro que permita una activación ordenada y legítima del instrumento militar.

La existencia de normas como la Ley del Sistema Nacional de Protección Civil y la Ley de Seguridad Nacional ha evitado improvisaciones y ha facilitado respuestas rápidas ante crisis complejas, reforzando la capacidad del Estado para actuar de forma coordinada sin necesidad de recurrir a mecanismos excepcionales (Ley 36/2015).

Los acontecimientos registrados en Ceuta durante el verano de 2026 pusieron de manifiesto algunas de las dificultades que pueden surgir cuando las Fuerzas Armadas son desplegadas en apoyo de las fuerzas y cuerpos de seguridad en escenarios de elevada tensión. Tras diversas agresiones sufridas por patrullas militares, se autorizó que determinados efectivos dispusieran de armamento con munición real y se activaron reglas de enfrentamiento para regular su utilización en situaciones de autodefensa. Estas medidas no modificaron, sin embargo, el carácter de apoyo de la misión ni atribuyeron con carácter general a los militares las funciones propias de los cuerpos policiales (De Santos, 2026).

La situación generó un debate sobre la delimitación de las funciones asignadas, las reglas de actuación y la cobertura jurídica de los militares desplegados. Diversas asociaciones profesionales

reclamaron una mayor precisión del marco aplicable, especialmente ante la eventual necesidad de emplear el armamento en situaciones de riesgo, así como instrucciones claras y una adecuada coordinación con las autoridades competentes (De Santos, 2026). El caso de Ceuta evidencia así la importancia de que la participación de las Fuerzas Armadas en apoyo de la seguridad interior se encuentre acompañada de una definición previa y precisa de la misión, las facultades de actuación y los mecanismos de coordinación, proporcionando seguridad jurídica tanto a los efectivos intervinientes como al conjunto de las instituciones implicadas.

Una segunda lección relevante es la importancia de la dirección civil y de la delimitación funcional de competencias. Las actuaciones recientes han demostrado que la integración de las Fuerzas Armadas en dispositivos de seguridad interior resulta más eficaz cuando se mantiene una clara separación entre funciones militares y policiales, evitando solapamientos y garantizando que la intervención militar conserve su carácter subsidiario y excepcional (LO 5/2005).

Asimismo, la experiencia ha evidenciado que la coordinación interinstitucional es un factor clave para el éxito de las operaciones. La interacción entre administraciones autonómicas, organismos estatales, fuerzas y cuerpos de seguridad y Fuerzas Armadas ha permitido optimizar recursos y mejorar la gestión de crisis de gran magnitud.

No obstante, también se han identificado dificultades en los flujos de información y en la interoperabilidad, lo que sugiere la necesidad de seguir perfeccionando los mecanismos de coordinación y planificación conjunta (Ley 17/2015).

Otra lección aprendida se refiere a la normalización del empleo de las Fuerzas Armadas en apoyo a la seguridad interior, sobre todo en contextos de emergencia. Si bien esta tendencia ha sido socialmente aceptada en situaciones de grave riesgo, diversos enfoques críticos advierten del riesgo de que la reiteración de estas intervenciones diluya su carácter excepcional y genere una percepción de militarización de la seguridad pública, lo que obliga a extremar la transparencia y la comunicación institucional (Foucault, 1977).

En este sentido, la experiencia española subraya la necesidad de reforzar las garantías democráticas y jurídicas que acompañan a la intervención militar en el ámbito interior.

El respeto a los derechos fundamentales y el sometimiento de la actuación de las Fuerzas Armadas a marcos normativos precisos constituyen elementos esenciales para preservar la legitimidad del modelo y evitar derivas excepcionales no justificadas (Agamben, 2005).

Finalmente, las actuaciones recientes ponen de relieve que la participación de las Fuerzas Armadas en la seguridad pública debe entenderse como un complemento del sistema ordinario, y no como un sustituto de las fuerzas y cuerpos de seguridad. El modelo español ha demostrado ser eficaz cuando se basa en la cooperación, la subsidiariedad y la planificación previa, lo que sugiere la conveniencia de seguir avanzando hacia un esquema de colaboración estructurada que permita afrontar amenazas futuras sin comprometer los principios democráticos del Estado (Iglesias, 2011).

6 Modelos comparados en el entorno europeo

6.1 Francia: empleo de las Fuerzas Armadas en la seguridad interior

Francia cuenta con un modelo normativo que integra eficazmente a las Fuerzas Armadas en la seguridad pública. Con este modelo se combina la centralización en la toma de decisiones con una clara delimitación de competencias, permitiendo que las Fuerzas Armadas actúen como un recurso estratégico bajo supervisión civil (Secrétariat général de la défense et de la sécurité nationale, 2016).

Normativas fundamentales como el Code de la Défense[91], el Code de la Sécurité Intérieure[92] y el programa VIGIPIRATE establecen las bases legales para su participación en la seguridad nacional.

El Código de Defensa regula la actuación de las Fuerzas Armadas y las habilita a intervenir en situaciones de emergencia nacional

[91] El Código de Defensa regula la estructura, funciones y misiones de las Fuerzas Armadas francesas, incluyendo su interacción con actores civiles y militares en la protección del Estado y la población.

[92] El Código de Seguridad Interna reúne las disposiciones legales sobre seguridad pública y protección ciudadana en Francia, consolidando leyes para facilitar la coordinación y eficiencia entre los actores de la seguridad nacional.

o amenazas graves, como el terrorismo, las catástrofes naturales o los ataques no convencionales.

Este marco jurídico garantiza que su participación en tareas de seguridad pública sea siempre temporal y bajo estricta supervisión civil, permitiendo, además, el despliegue de unidades especializadas frente a amenazas de tipo nuclear, biológico o químico, reforzando así la capacidad de respuesta del Estado ante escenarios de alta complejidad.

Por su parte, el Código de Seguridad Interna define las competencias de las fuerzas policiales y regula la colaboración con las Fuerzas Armadas en circunstancias excepcionales. En estos casos, las Fuerzas Armadas complementan a la Gendarmería Nacional y a la Policía Nacional en la protección de infraestructuras críticas y la vigilancia de áreas urbanas.

Uno de los pilares de la colaboración entre las Fuerzas Armadas y la seguridad pública en Francia es el programa VIGIPIRATE. Implementado en 1978 y actualizado continuamente, este sistema establece diferentes niveles de alerta que determinan las medidas de protección para la población y las infraestructuras críticas.

Entre sus mayores logros destaca la coordinación entre militares y fuerzas policiales, permitiendo el despliegue de tropas en áreas urbanas estratégicas, como estaciones de tren y centros comerciales, para reforzar la vigilancia y disuadir amenazas. Asimismo, VIGIPIRATE protege infraestructuras sensibles como embajadas y edificios gubernamentales, garantizando la seguridad en momentos de crisis.

El éxito de VIGIPIRATE radica en su flexibilidad operativa, lo que permite adaptar las respuestas de seguridad según la magnitud de la amenaza. Su capacidad para integrar de manera efectiva recursos civiles y militares ha fortalecido el modelo de seguridad francés, demostrando la importancia de una estrategia coordinada ante riesgos emergentes.

En este marco, se inscribe la operación Sentinelle, puesta en marcha tras los atentados de 2015, que reforzó la presencia militar en el espacio público y la protección de infraestructuras críticas mediante el despliegue de efectivos en apoyo de las fuerzas policiales, con un claro componente disuasorio frente al terrorismo (Pelletier y Drozda-Senkowska, 2016).

En situaciones de desastres naturales o emergencias nacionales, las Fuerzas Armadas actúan bajo el mando de las autoridades civiles para garantizar la seguridad pública. Durante la pandemia de COVID-19, las Fuerzas Armadas francesas desempeñaron un papel fundamental en apoyo a las autoridades civiles. El 25 de marzo de 2020, el presidente de la República Francesa, Emmanuel Macron, anunció la Operación Resiliencia, destinada a brindar asistencia logística y médica en la lucha contra el virus.

Esta operación incluyó el despliegue de recursos militares para el transportar suministros médicos, construir hospitales de campaña y ofrecer apoyo logístico en zonas críticas. Por ejemplo, se instaló un hospital de campaña en la ciudad francesa de Mulhouse para aliviar la presión sobre los servicios sanitarios locales (Ministère des Armées, 2022).

Las Fuerzas Armadas también han intervenido ante emergencias climáticas, como inundaciones y tormentas, proporcionando apoyo logístico y operativo a las fuerzas civiles (France 24, 2024).

La protección del ciberespacio es otra área estratégica donde las Fuerzas Armadas francesas están involucradas. La creación de la Comandancia de Defensa Cibernética (COMCYBER)[93] ha permitido coordinar acciones defensivas y ofensivas en el ámbito digital. COMCYBER trabaja en colaboración con agencias civiles y empresas privadas para proteger infraestructuras críticas frente a ciberataques y garantizar la resiliencia tecnológica del país.

A pesar de su efectividad, el modelo francés enfrenta desafíos. Uno de ellos es evitar la dependencia excesiva de las Fuerzas Armadas en tareas civiles, lo que podría desdibujar su misión principal de defensa. Además, la percepción pública de una «militarización» de la seguridad puede generar tensiones sociales. Para mitigar estos riesgos, Francia ha invertido en formación conjunta y comunicación transparente entre las instituciones civiles y militares (De Massol, 2019).

6.2 Italia: modelo híbrido y cooperación estructurada

[93] La Comandancia de Defensa Cibernética (COMCYBER) es la unidad del Ministerio de Defensa francés encargada de coordinar las operaciones cibernéticas defensivas y ofensivas, proteger infraestructuras críticas y garantizar la seguridad nacional frente a ciberamenazas.

El marco normativo italiano otorga un papel esencial a las Fuerzas Armadas en la seguridad pública, especialmente para responder a amenazas como el terrorismo, la inmigración irregular, el narcotráfico y las ciberamenazas. Este enfoque se fundamenta en un conjunto de disposiciones legales que definen su papel como complemento de las fuerzas policiales, siempre bajo supervisión civil. Normas como la Ley n.º 125/2008, el Código de Defensa y la Ley Antiterrorista n.º 43/2015 son pilares fundamentales que regulan esta colaboración.

La Constitución italiana, en su artículo 117, establece que la seguridad pública es competencia exclusiva del Estado. Dicho principio proporciona una base centralizada para las políticas de orden público, permitiendo la intervención de las Fuerzas Armadas en circunstancias excepcionales bajo la autoridad del Ministerio del Interior.

En este marco, la Ley n.º 121/1981 organiza las fuerzas policiales en Italia y otorga un rol de coordinación destacado a los Carabinieri, un cuerpo de naturaleza militar que opera tanto en el ámbito de la defensa como en el de la seguridad pública.

En Italia, la Ley n.º 125/2008 dio cobertura a la operación Strade Sicure, que permite el despliegue de personal militar en apoyo de las fuerzas policiales en tareas de vigilancia y protección de objetivos sensibles. Los efectivos militares actúan bajo la autoridad del Ministerio del Interior y en coordinación con la Policía del Estado y los Carabinieri.

En este marco, las Fuerzas Armadas refuerzan la vigilancia en grandes ciudades, infraestructuras de transporte, zonas fronterizas, aeropuertos y eventos multitudinarios, concentrando su actuación en espacios considerados de riesgo. Su presencia contribuye a reforzar la seguridad del entorno sin asumir funciones policiales ordinarias.

La continuidad de Strade Sicure pone de relieve la viabilidad de un modelo de colaboración en el que el apoyo militar se integra en la seguridad interior de forma limitada y ordenada, sin alterar la naturaleza civil de la seguridad pública.

Por otra parte, las Fuerzas Armadas italianas desempeñan un papel crucial en la lucha contra el terrorismo. La Ley Antiterrorista n.º 43/2015 permite su colaboración en tareas de prevención y persecución de actos terroristas.

Tras los atentados de París en 2015, las Fuerzas Armadas italianas participaron activamente en la vigilancia de infraestructuras críticas y eventos masivos, aplicando un modelo preventivo coordinado con la Policía del Estado y los Carabinieri.

Esta colaboración incluye patrullas conjuntas y la protección de objetivos sensibles, reforzando la capacidad del Estado para disuadir y responder ante eventuales ataques.

En esta línea, Italia, como punto de entrada estratégico en el Mediterráneo, enfrenta desafíos significativos relacionados con la inmigración irregular. Las Fuerzas Armadas colaboran estrechamente con la Guardia Costera y la Guardia di Finanza en operaciones de vigilancia marítima, rescate e interdicción de embarcaciones. Operaciones como «Mare Nostrum»[94] (2013-2014) ejemplifican esta colaboración, combinando objetivos humanitarios con los de seguridad.

Actualmente, las Fuerzas Armadas también participan en misiones europeas como EUNAVFOR MED o Sophia[95], orientadas a combatir el tráfico de personas y otras actividades ilícitas en el Mediterráneo.

En paralelo, el narcotráfico constituye otra prioridad para la seguridad italiana, especialmente en regiones del sur como Calabria y Sicilia. En el marco de la operación Strade Sicure, las Fuerzas Armadas prestan apoyo a la Guardia di Finanza en tareas de vigilancia y control de rutas utilizadas por redes criminales. De forma complementaria, los Carabinieri lideran las investigaciones contra el tráfico de drogas y las organizaciones mafiosas, reforzando la lucha contra el crimen organizado mediante una actuación coordinada entre instituciones.

Por otro lado, la Estrategia Nacional de Seguridad Cibernética de 2017 asigna a las Fuerzas Armadas un papel clave en la protección de infraestructuras críticas frente a ciberataques. Este marco normativo refuerza la cooperación entre actores civiles y militares, fomentando la integración tecnológica y el intercambio de inteligencia.

---

[94] La Operación Mare Nostrum fue el conjunto de acciones navales y aéreas desarrollada en 2013 por el Gobierno de Italia, para abordar el incremento de la inmigración irregular, y los consiguientes naufragios trágicos de embarcaciones de migrantes frente a la isla de Lampedusa.

[95] La EUNAVFOR MED o Sophia es una operación militar con la que la Unión Europea (UE) pretende desmantelar las redes de tráfico de inmigrantes a través del Mediterráneo.

Las Fuerzas Armadas también están preparadas para actuar en otras amenazas emergentes, como eventuales ataques de tipo químico o biológico, garantizando la resiliencia del sistema de seguridad pública.

No obstante, este modelo enfrenta desafíos, ya que el uso prolongado de las Fuerzas Armadas en tareas de orden público genera debate sobre su impacto en la percepción ciudadana y la posible desnaturalización de su misión defensiva (Vergnano, 2023).

6.3 Reino Unido: apoyo militar a las autoridades civiles

El Reino Unido dispone de un marco normativo que regula la cooperación entre las Fuerzas Armadas y las instituciones civiles en materia de seguridad pública. Aunque su sistema de seguridad mantiene una separación estricta entre las funciones militares y policiales, las Fuerzas Armadas pueden intervenir en situaciones de emergencia nacional, amenazas terroristas o para proteger infraestructuras críticas, siempre bajo supervisión civil.

Esta colaboración se basa en normativas como el protocolo de Military Aid to Civil Authorities (MACA)[96] y en estrategias nacionales como la UK National Security Strategy[97].

El marco legislativo británico regula la participación de las Fuerzas Armadas en tareas de seguridad pública mediante la MACA y otras leyes[98] que habilitan su actuación en circunstancias excepcionales, como atentados terroristas, emergencias civiles o desastres naturales. La UK National Security Strategy, actualizada en 2021, destaca la importancia de la colaboración interinstitucional para abordar amenazas de diversa índole, como el terrorismo, los ciberataques y el crimen organizado. En todos estos supuestos, el despliegue de las Fuerzas Armadas se realiza siempre bajo supervisión de las autoridades civiles y con carácter

[96] Ayuda militar a las autoridades civiles (MACA) es el término colectivo utilizado por el Ministerio de Defensa del Gobierno del Reino Unido para referirse al despliegue operativo de las Fuerzas Armadas del Reino Unido en apoyo de las autoridades civiles.
[97] La Estrategia de Seguridad Nacional del Reino Unido es un documento establece los riesgos que enfrenta el país y cómo el gobierno del momento abordará dichos riesgos.
98 Civil Contingencies Act 2004: Regula la respuesta a emergencias y permite la intervención de las Fuerzas Armadas en crisis. Terrorism Act 2000: habilita la cooperación de las Fuerzas Armadas en operaciones antiterroristas. Investigatory Powers Act 2016: autoriza la colaboración de las Fuerzas Armadas en inteligencia y vigilancia.

temporal, asegurando que su rol principal como fuerza militar no se vea comprometido.

El terrorismo ha sido una prioridad en la política de seguridad pública británica, especialmente tras los atentados de Londres en 2005 y ataques más recientes en Mánchester y Westminster. Estos sucesos llevaron al Gobierno a reforzar sus estrategias antiterroristas y a mantener un nivel alto de alerta (La Vanguardia, 2019).

En tales casos, las Fuerzas Armadas han participado activamente en el refuerzo de la seguridad mediante la Operación Temperer[99], implementada cuando el nivel de alerta terrorista alcanza su grado crítico.

En este marco, las Fuerzas Armadas colaboran con la Policía Metropolitana de Londres y otros organismos de seguridad en la protección de infraestructuras críticas, la vigilancia de espacios públicos y el apoyo logístico en situaciones de crisis, reforzando la capacidad del Estado para responder a escenarios de riesgo elevado sin asumir funciones policiales ordinarias.

Además, las Fuerzas Armadas reciben formación específica para intervenir ante incidentes químicos, biológicos o nucleares, reforzando la capacidad del Estado para responder a situaciones críticas en instalaciones sensibles. Un ejemplo significativo fue el atentado con agente químico en Salisbury en 2018, tras el que las Fuerzas Armadas participaron en tareas de descontaminación y protección de la población local.

6.4 Enseñanzas aplicables al caso español

El análisis comparado de los modelos francés, italiano y británico permite extraer una primera enseñanza fundamental: la participación de las Fuerzas Armadas en la seguridad interior puede ser compatible con un Estado democrático siempre que esté claramente delimitada por un marco jurídico preciso, subordinada al poder civil y concebida como un recurso complementario.

En este sentido, el modelo español comparte rasgos con los tres casos analizados, pero presenta todavía un margen de mejora

99 La Operación Temperer es un plan del Gobierno británico para desplegar liberar a los agentes de policía en lugares clave tras un importante ataque terrorista o un importante desorden público.

en términos de sistematización y claridad competencial (Iglesias, 2011).

Una segunda enseñanza se refiere a la necesidad de planificación previa y estructuras estables de coordinación. Tanto Francia, a través de VIGIPIRATE, como Italia, mediante Strade Sicure, muestran la utilidad de contar con mecanismos permanentes que permitan integrar a las Fuerzas Armadas en la respuesta a crisis sin recurrir a soluciones improvisadas.

Para el caso español, esta experiencia refuerza la conveniencia de consolidar marcos de actuación predefinidos que faciliten la cooperación interinstitucional en situaciones de emergencia, reduciendo la incertidumbre operativa y política (Pelletier y Drozda-Senkowska, 2016).

Al mismo tiempo, los modelos analizados ponen de relieve la importancia de preservar el carácter excepcional de la intervención militar en el ámbito interior.

El enfoque restrictivo del Reino Unido, basado en el principio de último recurso, constituye una referencia útil para evitar una normalización excesiva del empleo de las Fuerzas Armadas en tareas de seguridad pública.

Esta cautela resulta especialmente relevante para España, donde la aceptación social de la intervención militar en emergencias es elevada, pero podría verse erosionada si se percibe una extensión injustificada de su presencia en funciones ordinarias (Martínez *et al*., 2024).

Otra enseñanza relevante es el valor de unidades especializadas y claramente definidas, como la Unidad Militar de Emergencias en el caso español. La experiencia francesa e italiana confirma que la especialización contribuye a legitimar la intervención militar, al asociarla a misiones concretas y socialmente aceptadas, como la protección civil o la respuesta ante catástrofes.

Este enfoque reduce el riesgo de confusión de roles y facilita la integración de las Fuerzas Armadas en la gestión de crisis sin afectar a las competencias de las fuerzas policiales (De Massol, 2019).

Finalmente, el análisis comparado subraya la importancia de la comunicación institucional y la transparencia. Los debates existentes en Francia e Italia sobre la militarización de la seguridad interior muestran que la legitimidad de estos modelos no

depende solo de su eficacia operativa, sino también de la claridad con la que se expliquen sus límites, objetivos y duración.

Para España, esta enseñanza resulta clave a la hora de reforzar la confianza ciudadana y garantizar que la participación de las Fuerzas Armadas en la seguridad pública se perciba como una herramienta excepcional al servicio del Estado de derecho y no como una sustitución de las funciones civiles (Agamben, 2005).

7 Riesgos asociados de una mayor participación de las Fuerzas Armadas en la seguridad pública en España

7.1 Percepción ciudadana de la presencia militar en la seguridad pública

La participación de las Fuerzas Armadas en tareas de seguridad pública influye directamente en la forma en que la ciudadanía percibe el funcionamiento del sistema democrático. Esta percepción no depende únicamente de la legalidad de la intervención, sino también de cómo se interpretan sus efectos sobre el equilibrio entre seguridad interior y defensa nacional.

Uno de los elementos que condiciona la percepción social es la claridad en la delimitación de funciones. Cuando la frontera entre seguridad interior y defensa aparece difusa, pueden surgir dudas sobre el papel que corresponde a cada institución y sobre el respeto al principio de control civil.

La literatura clásica sobre relaciones civil-militares ya advertía de la importancia de preservar este equilibrio para evitar tensiones institucionales en los sistemas democráticos (Huntington, 1996).

La reiteración del empleo del instrumento militar en la gestión de crisis internas constituye otro factor relevante desde el punto de vista perceptivo. Cuando las Fuerzas Armadas se utilizan de forma frecuente como respuesta a problemas de seguridad complejos, parte de la ciudadanía puede interpretar que las capacidades civiles resultan insuficientes o que no se están reforzando adecuadamente. Esta percepción puede generar una sensación de dependencia poco deseable a medio plazo (De Massol, 2020).

La presencia militar en el espacio público también tiene un impacto simbólico. Aunque las Fuerzas Armadas mantienen en España elevados niveles de confianza social, su despliegue en entornos

urbanos o en funciones próximas al orden público puede generar recelos si se prolonga en el tiempo o no se explica con claridad.

Las experiencias en países del entorno europeo muestran que la aceptación social depende en gran medida del carácter temporal, limitado y bien justificado de estas intervenciones (Vergnano, 2023).

Desde una perspectiva institucional, la coordinación entre actores civiles, policiales y militares influye igualmente en la percepción ciudadana. La coexistencia de múltiples autoridades en un mismo escenario exige sistemas de dirección claros y procedimientos bien definidos.

Cuando estos mecanismos no están lo suficiente desarrollados, pueden proyectarse imágenes de desorganización o falta de control político, especialmente en situaciones de alta presión (Iglesias, 2011).

Estas dificultades se ven acentuadas por las diferencias organizativas entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad. Cada institución opera con estructuras, procedimientos y culturas profesionales propias, lo que puede dificultar la comunicación sobre el terreno. En ausencia de experiencias previas compartidas, estas barreras pueden afectar tanto a la eficacia operativa como a la percepción pública de la intervención (Salvador, Almaraz y Penilla, 2021).

La falta de formación y de ejercicios conjuntos previos constituye otro elemento que condiciona la percepción social. La cooperación no puede construirse únicamente en situaciones de emergencia, ya que la improvisación incrementa el riesgo de errores visibles y mensajes contradictorios. La planificación previa y el conocimiento mutuo resultan esenciales para proyectar una imagen de coordinación y control institucional (López, 2023).

A estos elementos se suma la dimensión comunicativa, que desempeña un papel central en la legitimidad democrática de estas actuaciones. La percepción ciudadana no depende solo de lo que se hace, sino de cómo se explica. Cuando la excepcionalidad de la intervención militar no se comunica de forma adecuada, pueden surgir interpretaciones erróneas sobre el alcance real de su actuación y sobre sus límites jurídicos (Bernal, 2011).

La experiencia reciente en España muestra que, en contextos como la pandemia de COVID-19, la erupción volcánica de La Palma, las inundaciones o el apagón eléctrico de 2025, la actua-

ción regulada y temporal de las Fuerzas Armadas ha contribuido a reforzar su percepción como un recurso al servicio de la sociedad. Sin embargo, esta aceptación social no es automática ni permanente, y requiere un esfuerzo continuado de información y rendición de cuentas por parte de las autoridades públicas.

En este sentido, el nivel de conocimiento cívico sobre el marco jurídico que regula la intervención de las Fuerzas Armadas resulta determinante. El desconocimiento de los principios de subsidiariedad, excepcionalidad y control civil puede debilitar la confianza institucional. Explicar estos elementos no constituye un aspecto técnico secundario, sino una exigencia democrática (Bernal, 2011).

En conjunto, la percepción ciudadana de la presencia militar en la seguridad pública depende de una combinación de factores jurídicos, operativos y comunicativos. La experiencia española pone de manifiesto que estas intervenciones solo son socialmente viables cuando se gestionan con prudencia, claridad y respeto a los límites institucionales, preservando así la confianza ciudadana y el equilibrio del sistema democrático (Bernal, 2011).

7.2 Cambio cultural en la sociedad española en materia de defensa

El análisis del cambio cultural en la sociedad española en materia de defensa resulta relevante para comprender algunos de los riesgos asociados a una mayor participación militar en la seguridad pública. La forma en que la ciudadanía percibe a las Fuerzas Armadas, su función y sus límites condiciona directamente la legitimidad social de su empleo en el ámbito interior.

La cultura de defensa no se limita al conocimiento institucional o normativo. Integra experiencias compartidas, mecanismos de socialización y marcos simbólicos que influyen en la legitimidad social del instrumento militar y en la percepción de su posible empleo en tareas vinculadas a la seguridad pública (Navajas, 2016).

Uno de los factores que ha influido de forma significativa en esta evolución ha sido la suspensión del servicio militar obligatorio. La desaparición de este mecanismo de socialización directa redujo el contacto cotidiano de amplios sectores de la población con las Fuerzas Armadas, contribuyendo a una progresiva desvinculación cultural entre la institución militar y la sociedad civil.

Diversos estudios señalan que este proceso tuvo un impacto relevante en la transmisión informal de valores asociados a la defensa y en la percepción social de su utilidad (Alfaro, 2025).

Este distanciamiento no se tradujo necesariamente en una actitud de rechazo, sino en una creciente indiferencia hacia las cuestiones relacionadas con la defensa nacional. La defensa pasó a percibirse como una política pública altamente especializada, delegada en profesionales y apenas conectada con las preocupaciones cotidianas de la ciudadanía.

Este marco cultural condicionó durante años el debate público sobre el papel de las Fuerzas Armadas, limitando su visibilidad social fuera de contextos estrictamente militares (Ballesteros, 2010).

En la última década, se ha producido un cambio gradual en la forma en que la sociedad española percibe la defensa y el papel de las Fuerzas Armadas. La aparición de amenazas complejas, como las crisis sanitarias, las catástrofes naturales o las emergencias de gran impacto, ha contribuido a que una parte creciente de la ciudadanía relacione la defensa no solo con escenarios bélicos, sino también con la protección directa de la población.

Esta evolución ha favorecido una visión más práctica y cercana del papel de las Fuerzas Armadas, entendidas como un recurso del Estado al servicio de la seguridad colectiva en situaciones excepcionales, dentro del marco del Estado democrático (Alfaro, 2025).

Las intervenciones de las Fuerzas Armadas en apoyo de las autoridades civiles han actuado como un factor relevante de normalización cultural. La Operación Balmis (COVID-19), la crisis del volcán de La Palma[100], la respuesta a la DANA[101] en Valencia (2024) o el apagón en el suroeste de Europa de 2025 han reforzado el papel de las Fuerzas Armadas en la seguridad y la protección civil.

[100] La erupción volcánica de La Palma de 2021 se inició el 19 de septiembre en la zona de Montaña Rajada, cercano a la localidad de El Paraíso del municipio de El Paso, en la isla de La Palma.

[101] El término DANA, en realidad, hace referencia a una sigla que se usan en meteorología con frecuencia. Por lo que el significado de DANA es en realidad el siguiente: Depresión Aislada en Niveles Altos. Es lo que antiguamente se conocía como gota fría.

En estas actuaciones, las Fuerzas Armadas actuaron como un instrumento de apoyo a las fuerzas y cuerpos de seguridad y a las autoridades civiles, demostrando que su función no se limita al ámbito de la defensa, sino que también son un recurso fundamental en la gestión de crisis y emergencias, fortaleciendo su vínculo con la sociedad.

A pesar de los avances señalados, la cultura de defensa sigue siendo un ámbito pendiente en España. Persisten sectores sociales que continúan percibiendo a las Fuerzas Armadas como entidades militarizadas y alejadas de la realidad civil, lo que limita una comprensión plena de su papel en la seguridad pública.

Esta realidad exige reforzar de forma continuada la educación en materia de defensa, la comunicación institucional y la cooperación entre actores civiles y militares, con el fin de clarificar funciones, límites y responsabilidades (Martínez & Durán, 2024).

En síntesis, la participación de las Fuerzas Armadas en la seguridad pública solo resulta socialmente aceptable cuando se percibe como una intervención excepcional, jurídicamente delimitada y sometida a control civil.

Solo cuando estas condiciones se mantienen, puede integrarse el apoyo militar a la gestión de crisis complejas como un recurso del Estado, sin alterar el reparto de funciones con las fuerzas y cuerpos de seguridad (Martínez & Bueno, 2024).

La experiencia comparada, a través de modelos como VIGIPIRATE en Francia, muestra que es posible articular una participación militar limitada y claramente delimitada en el ámbito de la seguridad nacional, sin desdibujar la misión principal de las Fuerzas Armadas.

8 Hacia un modelo de colaboración entre Fuerzas Armadas y fuerzas y cuerpos de seguridad en España

8.1 Principios rectores del modelo

La configuración de un modelo de colaboración entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad debe partir de la definición de principios rectores claros, orientados a garantizar su eficacia operativa y su adecuación al Estado de derecho.

La experiencia acumulada en España y en el entorno europeo muestra que la falta de principios bien definidos incrementa el riesgo de improvisación, solapamientos competenciales y tensiones institucionales en situaciones de crisis (Iglesias, 2011).

Este modelo debe, en primer lugar, asumir la transformación del concepto de seguridad nacional y reconocer que la seguridad del Estado se enfrenta hoy a riesgos que afectan tanto al ámbito interior como al exterior.

Esta realidad exige mejorar la coordinación entre las distintas instituciones responsables de la seguridad, sin que ello suponga alterar el reparto de competencias ni el papel propio de cada una de ellas (Bigo, 2016).

Cualquier esquema de colaboración debe partir, en primer lugar, del respeto al principio de dirección civil. La intervención de las Fuerzas Armadas en el ámbito interior solo puede producirse bajo la autoridad de las instituciones civiles competentes, garantizando el control político de la actuación militar y la responsabilidad democrática de las decisiones adoptadas.

La experiencia demuestra que la eficacia de la respuesta no depende de una mayor presencia militar, sino de la claridad en la toma de decisiones y en la asignación de responsabilidades (Bueno y Remiro, 2024).

Junto con ello, el principio de subsidiariedad resulta esencial para delimitar el papel de las Fuerzas Armadas como recurso de apoyo del Estado. Su actuación debe producirse únicamente cuando las capacidades civiles se ven desbordadas, evitando que el instrumento militar se convierta en una solución habitual para problemas que corresponden a otros ámbitos. Este criterio permite preservar la función propia de las fuerzas y cuerpos de seguridad y refuerza la coherencia del sistema de seguridad pública.

Otros principios esenciales son el de excepcionalidad y temporalidad. La participación de las Fuerzas Armadas ha de responder a circunstancias concretas y claramente definidas, con una duración limitada y objetivos precisos. Convertir estas intervenciones en prácticas prolongadas puede generar confusión institucional y dificultar su aceptación social (Martínez *et al*., 2024).

Por último, la protección de los derechos fundamentales y la transparencia en la actuación pública deben constituir un principio transversal. El control parlamentario, la supervisión jurídica y una comunicación institucional resultan indispensables para

garantizar la legitimidad democrática de cualquier intervención en el ámbito interior (Bigo, 2016).

8.2 Condicionantes para la implantación del modelo

La puesta en práctica de un modelo de colaboración entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad exige atender a una serie de condiciones estructurales que resultan determinantes para su viabilidad.

Entre ellas, destaca, en primer lugar, la necesidad de preservar el carácter excepcional de la intervención militar en el ámbito interior.

La utilización recurrente de un instrumento concebido para situaciones extraordinarias puede alterar el equilibrio del sistema de seguridad pública y desdibujar la frontera entre seguridad interior y defensa nacional (Beck, 1992).

Otro condicionante esencial es la preservación de la identidad funcional de las Fuerzas Armadas**.** El empleo continuado de unidades militares en cometidos propios del ámbito policial puede generar confusión competencial y afectar a la misión principal de las Fuerzas Armadas, definida por el artículo 8 de la Constitución española y la Ley Orgánica 5/2005 como la defensa nacional.

Cuando las Fuerzas Armadas asumen de forma prolongada tareas de seguridad interior, se produce una tensión entre la preparación militar y las funciones policiales, con efectos negativos tanto en la eficacia operativa como en la percepción social de su papel institucional (Hémez, 2017).

Desde una perspectiva operativa, la implantación del modelo requiere evitar que el apoyo militar se convierta en una respuesta habitual ante situaciones que corresponden a los ámbitos civiles.

La reiteración de este tipo de intervenciones puede debilitar el desarrollo de capacidades propias de las Fuerzas y Cuerpos de Seguridad y de los sistemas de protección civil, afectando a la coherencia del conjunto del sistema de seguridad pública (Salvador, Almaraz y Penilla, 2021).

A ello se suma la aceptación social y la legitimidad democrática como condicionantes indispensables. Aunque en España la actuación de las Fuerzas Armadas en situaciones de emergencia ha sido valorada de forma positiva, su extensión a funciones de

seguridad ordinaria exige una gestión especialmente prudente. La confianza ciudadana depende en gran medida de la claridad con la que se expliquen los objetivos, límites y duración de estas actuaciones, así como de la percepción de que se mantienen bajo control civil efectivo (Navajas, 2016).

Asimismo, la cooperación entre Fuerzas Armadas y fuerzas y cuerpos de seguridad requiere condiciones adecuadas de coordinación operativa. La existencia de protocolos claros, formación conjunta periódica y una delimitación precisa de funciones y responsabilidades constituye un requisito previo para evitar desajustes en la cadena de mando y problemas de ejecución en situaciones reales de crisis. La experiencia demuestra que la cooperación civil-militar no puede improvisarse, sino que debe construirse con antelación (Salvador, Almaraz y Penilla, 2021).

Por último, la implantación del modelo exige mecanismos estables de evaluación y control**.** La ausencia de sistemas de revisión a medio y largo plazo puede dificultar la detección de disfunciones y la corrección de prácticas ineficaces.

El control parlamentario, la evaluación operativa y la rendición de cuentas periódica se configuran, como elementos esenciales para garantizar que la colaboración refuerce la seguridad pública sin comprometer los valores democráticos ni el principio de excepcionalidad que la justifica (Lunn, 2023).

8.2.1 Necesidad de un nuevo marco normativo

La evolución del entorno de seguridad en España muestra que las amenazas actuales no siguen patrones previsibles ni se presentan de forma aislada. En este contexto, la respuesta del Estado no puede apoyarse en actuaciones improvisadas, sino en una planificación previa que permita coordinar de manera eficaz los recursos disponibles, incluidos los militares cuando la situación lo requiera. La experiencia en la gestión de crisis indica que la falta de planificación reduce la eficacia de la respuesta pública y aumenta las dificultades de coordinación (Iglesias, 2011).

Desde el punto de vista jurídico, el ordenamiento español incorpora la planificación como un elemento esencial de la seguridad nacional. La Ley 36/2015 de Seguridad Nacional y la Ley 17/2015 del Sistema Nacional de Protección Civil establecen la necesidad de anticipación, coordinación y planes previos para afrontar emergencias de gran magnitud. Estas normas confirman que la

planificación no es una opción, sino una exigencia del propio sistema de seguridad.

La experiencia reciente en España confirma los riesgos de actuar sin un marco previamente definido. Situaciones como la pandemia de COVID-19, la erupción volcánica en La Palma, las DANAS o el apagón eléctrico de 2025 pusieron de manifiesto la importancia de contar con procedimientos claros para la activación y coordinación de recursos extraordinarios, entre ellos las Fuerzas Armadas.

Cuando estos mecanismos existen, la respuesta resulta eficaz y cuenta con respaldo social. Cuando faltan, aparecen problemas de coordinación, tensiones entre instituciones y dificultades operativas que afectan a la actuación del conjunto del Estado.

Por el contrario, los mecanismos planificados facilitan una movilización más coherente, eficaz y legítima de los recursos militares en apoyo a la seguridad interior (Bueno y Remiro, 2024).

En el ámbito de la cooperación entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad, la ausencia de una planificación previa incrementa el riesgo de respuestas improvisadas, condicionadas por el contexto político o por la urgencia del momento. La falta de criterios claros puede dar lugar a solapamientos de funciones, dudas en la cadena de mando y un uso poco adecuado de capacidades militares concebidas para situaciones excepcionales, con efectos negativos sobre la eficacia de la respuesta pública (Herbón, 2021).

Asimismo, un marco previamente definido resulta clave para preservar la legitimidad democrática de la colaboración. La existencia de reglas claras y procedimientos conocidos refuerza la transparencia, facilita el control político y parlamentario y ayuda a que la sociedad comprenda mejor el papel de las Fuerzas Armadas en el ámbito interior. La confianza ciudadana se ve reforzada cuando las intervenciones excepcionales responden a planes definidos y evaluables, y no a decisiones adoptadas de forma apresurada en situaciones de urgencia (Bernal, 2011).

En otros países europeos, la cooperación entre autoridades civiles y Fuerzas Armadas se apoya de manera habitual en marcos previamente establecidos. En casos como Francia o el Reino Unido, la participación militar en apoyo a la seguridad interior se articula mediante criterios claros de activación y mecanismos de revisión periódica.

Los análisis disponibles coinciden en que los principales problemas no derivan del uso planificado de las Fuerzas Armadas, sino de la falta de criterios estables y de evaluaciones continuadas sobre su impacto (Lunn, 2023).

En consecuencia, avanzar hacia una colaboración ordenada exige dejar atrás la lógica de la improvisación y apoyarse en un marco planificado, previsible y evaluable.

La posible participación de las Fuerzas Armadas en la seguridad pública debe estar prevista y regulada con carácter previo, mediante planes específicos para situaciones excepcionales, protocolos claros de coordinación y mecanismos de evaluación posterior. Todo ello permite evitar respuestas improvisadas y preservar el carácter subsidiario y extraordinario de su intervención.

Solo de este modo es posible que la actuación excepcional de las Fuerzas Armadas refuerce la capacidad de respuesta del Estado sin generar disfunciones operativas ni tensiones institucionales, manteniéndose compatible con los principios del Estado de derecho.

9 Conclusiones

El análisis desarrollado a lo largo de este artículo muestra que la seguridad pública en España ya no puede entenderse como un ámbito cerrado ni exclusivamente policial. La evolución del entorno de amenazas, marcado por su carácter complejo, transversal y en muchos casos imprevisible, ha ampliado el marco tradicional de la seguridad interior y ha reforzado la necesidad de respuestas integradas por parte del Estado.

En este contexto, la posible participación de las Fuerzas Armadas en apoyo a las fuerzas y cuerpos de seguridad en tareas de seguridad pública se inserta dentro de un marco jurídico claro y deliberadamente restrictivo.

La Constitución y la legislación de desarrollo no atribuyen a las Fuerzas Armadas funciones ordinarias de seguridad ciudadana, pero sí permiten su intervención en situaciones excepcionales, siempre bajo dirección civil, con carácter subsidiario y dentro de límites jurídicos precisos.

El análisis del marco normativo pone de manifiesto que la participación de las Fuerzas Armadas en apoyo de la seguridad pública se encuentra claramente prevista en determinados ámbitos,

como la seguridad nacional, la protección civil o la lucha contra el terrorismo, donde existen habilitaciones jurídicas expresas y procedimientos definidos.



Figura 2. Presencia naval preventiva en el Campo de Gibraltar como apoyo a la vigilancia marítima y a la lucha contra el narcotráfico y el crimen organizado

No obstante, en otros escenarios vinculados al crimen organizado, la gestión de flujos migratorios o determinadas amenazas híbridas, la cobertura normativa resulta más limitada o fragmentaria, lo que abre un espacio de reflexión sobre la adecuación del marco jurídico vigente a la evolución del entorno de seguridad.

Desde una perspectiva operativa, las Fuerzas Armadas aportan capacidades especialmente valiosas en escenarios de alta complejidad y presión institucional. Más allá de las emergencias sanitarias o los desastres naturales, su contribución se orienta a reforzar la acción del Estado cuando concurren amenazas que desbordan los mecanismos ordinarios de respuesta. En estos supuestos, su intervención se concibe como un apoyo puntual y especializado, sin sustituir en ningún caso a las fuerzas y cuerpos de seguridad.

La experiencia reciente en España muestra que, cuando esta colaboración se produce dentro de marcos planificados y conocidos, la actuación resulta eficaz y cuenta con un amplio respaldo social. Por el contrario, la ausencia de criterios claros de activación, coordinación y desactivación genera incertidumbre operativa y dificulta la gestión de crisis complejas, reforzando la importancia de la planificación frente a la improvisación.

El análisis comparado con otros países europeos confirma que la clave no reside en ampliar o restringir de forma abstracta el empleo de las Fuerzas Armadas en el ámbito interior, sino en definir con claridad las condiciones, los límites y los objetivos de su participación.

La planificación previa, el control político y la evaluación posterior aparecen como elementos comunes en los modelos que han logrado integrar el apoyo militar sin erosionar el funcionamiento ordinario de la seguridad pública interior.

Finalmente, la reflexión sobre la cultura de defensa pone de manifiesto que la aceptación social de estas fórmulas de colaboración depende, en gran medida, de la transparencia, la pedagogía institucional y la claridad en la delimitación de funciones.

La participación de las Fuerzas Armadas en la seguridad pública no debe entenderse como una ampliación de su presencia en la vida cotidiana, sino como un recurso excepcional del Estado para hacer frente a amenazas que superan los mecanismos ordinarios (ver figura 2).

En definitiva, la colaboración entre las Fuerzas Armadas y las fuerzas y cuerpos de seguridad se configura como una herramienta útil y legítima cuando se apoya en la planificación, el control civil y el respeto a los principios democráticos. Desde este enfoque, la intervención militar en el ámbito interior no desdibuja el modelo de seguridad pública, sino que contribuye a reforzar la capacidad del Estado para proteger a la sociedad frente a riesgos cada vez más complejos.

Bibliografía

Agamben, G. (2005). Estado de excepción [en línea]. Buenos Aires, Adriana Hidalgo Editora. [Consulta: 2026]. Disponible en: https://geopolitica.iiec.unam.mx/sites/default/files/2017-08/Agamben Giorgio - Estado de excepción - Adriana Hidalgo.pdf

Alfaro López, J. A. (2025). Evolución de la relación entre la sociedad española y sus Fuerzas Armadas. En L. A. Hernández García (Ed.), El factor personal: Elemento clave en la evolución y desarrollo de las Fuerzas Armadas (pp. 29–50). Ministerio de Defensa. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/Factor_personal_elemento_clave_evolucion_y_desarrollo_de_las_fuerzas_armadas.pdf

Ballesteros, M. (2010). El papel de las fuerzas armadas en la lucha contra el terrorismo internacional [en línea]. Real Instituto Elcano. [Consulta: 2026]. Disponible en: https://www.realinstitutoelcano.org/analisis/el-papel-de-las-fuerzas-armadas-en-la-lucha-contra-el-terrorismo-internacional/

Beck, U. (1992). La sociedad del riesgo: Hacia una nueva modernidad [en línea]. Barcelona, Paidós. [Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/servlet/libro?codigo=113853

Bernal, P. (2011). La cultura de seguridad y defensa en España. Sus orígenes y evolución [en línea] Cuadernos de estrategia. N.º 155, pp. 22-63. [Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3834214

Bigo, D., Guild, E., & Walker, R. B. J. (2016). The changing landscape of European liberty and security. En D. Bigo, S. Carrera, E. Guild, & R. B. J. Walker (Eds.), Europe's 21st century challenge: Delivering liberty (pp. 1–28). Routledge. Disponible en: https://dokumen.pub/europes-21st-century-challenge-delivering-liberty-9781409499886-140949988x.html

Bueno, A. y Remiro, L. (2024). Relaciones civiles-militares y legitimidad democrática en España [en línea]. En: Martínez, R. y Durán, M. (dir.). Repensando el papel de las Fuerzas Armadas españolas ante los nuevos desafíos a la seguridad. Foros y Debates. [Consulta: 2026]. Disponible en: https://www.cepc.gob.es/sites/default/files/2025-02/a-1218-48-repensando-el-papel-de-las-ffaa-accesible.pdf

De Massol De Rebetz, R. y Van Der Woude, M. (2019). Marianne's Liberty in Jeopardy? A French Analysis on Recent Counter-terrorism Legal Developments [en línea]. Critical Studies on Terrorism. 13(1), pp. 1-23. [Consulta: 2026]. Disponible en: Full article: Marianne's liberty in jeopardy? A French analysis on recent counterterrorism legal developments

El País (2026). Dos guardias civiles muertos y otros dos heridos al chocar dos embarcaciones en la persecución a una

narcolancha. El País, 8 de mayo. Disponible en: https://elpais.com/espana/2026-05-08/muere-un-guardia-civil-al-chocar-dos-embarcaciones-persiguiendo-una-narcolancha-en-huelva.html

España. (1978). Constitución Española [en línea]. Boletín Oficial del Estado. 29 de diciembre, núm. 311. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con

—. (1981). Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio [en línea]. Boletín Oficial del Estado. 6 de junio, núm. 134. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1981-12774

—. (1986). Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad [en línea]. Boletín Oficial del Estado. 14 de marzo, núm. 63. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859

—. (2005). Ley Orgánica 5/2005, de 17 de noviembre de 2005, de la Defensa Nacional [en línea]. Boletín Oficial del Estado. 18 de noviembre, núm. 276. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2005-18933

—. (2011). Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas [en línea]. Boletín Oficial del Estado. 21 de mayo, núm. 121, pp. 50808-50826. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2011-8849

—. (2015a). Ley Orgánica 4/2015, de 30 de marzo de 2015, de protección de la seguridad ciudadana [en línea]. Boletín Oficial del Estado. 31 de marzo, núm. 77. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/lo/2015/03/30/4/con

—. (2015b). Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil [en línea]. Boletín Oficial del Estado. 10 de julio, núm. 164. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-7730

—. (2015c). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional [en línea]. Boletín Oficial del Estado. 29 de septiembre, núm. 233. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389

—. (2025). Orden INT/399/2025, de 28 de abril, por la que se declara la emergencia de interés nacional en el territorio de diversas comunidades autónomas como consecuencia de la interrupción del suministro eléctrico acaecida el 28 de abril de

2025 [en línea]. Boletín Oficial del Estado. 29 de abril, núm. 103, pp. 57619-57620. [Consulta: 2026]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-8486

EU-LAC Foundation. (2023). Las Fuerzas Armadas y la Seguridad Ciudadana: un estudio comparado entre la UE y América del Sur [en línea]. EU-LAC Foundation. [Consulta: 2026]. Disponible en: https://eulacfoundation.org/system/files/digital_library/2023-07/_FFAA_COMPARADAS_UE_AMSUR.pdf

Foucault, M. (1977). Vigilar y castigar: Nacimiento de la prisión [en línea]. Madrid, Siglo xxi Editores. [Consulta: 2026]. Disponible en: https://www.ivanillich.org.mx/Foucault-Castigar.pdf

France 24. (2024). Francia: lluvias torrenciales han dejado al menos cuatro muertos y cuatro desaparecidos [en línea]. France 24. [Consulta: 2026]. Disponible en: https://www.france24.com/es/europa/20240310-lluvias-torrenciales-dejan-un-muerto-y-siete-desaparecidos-al-sureste-de-francia

Hémez, R. (2017). The French Army at a Crossroads [en línea]. The US Army War College Quarterly Parameters. 47(1), pp. 103-116. [Consulta: 2026]. Disponible en: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2840&context=parameters

Herbón Costas, J. (2021). La gestión de las crisis en el marco de la Ley de Seguridad Nacional [en línea]. Revista Española de Derecho Constitucional. N.º 121, pp. 139-168. [Consulta: 2026]. Disponible en: https://recyt.fecyt.es/index.php/REDCons/article/view/89215

Hobbes, T. (1651). Leviatán o la materia, forma y poder de una república eclesiástica y civil [en línea]. Londres, Andrew Crooke. [Consulta: 2026]. Disponible en: https://www.marxists.org/espanol/hobbes/1651/leviatan/lev.htm

Huntington, S. (1996). *El choque de civilizaciones y la reconfiguración del orden mundial*. Madrid: Paidós

Infobae. (2024). ¿Es necesaria la participación de las Fuerzas Armadas en el control de la inmigración? [en línea]. Infobae. [Consulta: 2026]. Disponible en: https://www.infobae.com/espana/2024/07/05/es-necesaria-la-participacion-de-las-fuerzas-armadas-en-el-control-de-la-inmigracion/?utm_source=chatgpt.com

La Vanguardia. (2019). Ataques terroristas en Reino Unido desde 2005 [en línea]. La Vanguardia. [Consulta: 2026].

Disponible en: https://www.lavanguardia.com/internacional/20191129/471952350917/ataques-terroristas-en-reino-unido-desde-2005.html

Locke, J. (1690). Dos tratados sobre el gobierno civil [en línea]. Londres, Awnsham Churchill. [Consulta: 2026]. Disponible en: https://archive.org/details/locke-segundo-tratado-civil

López, G. (2023). The Spanish Army in Security Force Assistance: Lessons Learned in Iraq [en línea]. Revista Científica General José María Córdova. 21(41), pp. 5-24. [Consulta: 2026]. Disponible en: https://digibug.ugr.es/handle/10481/83632

Lunn, S. (2023). Ensuring Democratic Control of Armed Forces – The Enduring Challenges [en línea]. Connections: The Quarterly Journal. 22(1), pp. 29-51. [Consulta: 2026]. Disponible en: https://connections-qj.org/article/ensuring-democratic-control-armed-forces-enduring-challenges

Martínez, J. M.ª (2015). Análisis de las capacidades terrestres de los países de nuestro entorno [en línea]. Cuadernos de Estrategia. Ministerio de Defensa, Instituto Español de Estudios Estratégicos (IEEE). N.º 179, pp. 59-143. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5621489.pdf

Martínez, R., & Bueno, A. (2024). Causas de la militarizacion de las emergencias civiles. Revista Científica General José María Córdova, 22(48), 903-924. Disponible en: https://revistacientificaesmic.com/index.php/esmic/article/view/1389/1356

Martínez, R. y Pion-Berlín, D. (2017). Soldiers, politicians and civilians [en línea]. Cambridge University Press. [Consulta: 2026]. Disponible en: https://api.pageplace.de/preview/DT0400.9781108365215_A30911451/preview-9781108365215_A30911451.pdf

Ministère des Armées. (2022). Opération Résilience [en línea]. [Consulta: 2026]. Disponible en: https://www.defense.gouv.fr/terre/actualites/operation-resilience-militaires-du-regiment-medical-engages

Ministerio de Defensa. (2018). *PDC-01(A). Doctrina para el Empleo de las Fuerzas Armadas*. Ministerio de Defensa, Secretaría General Técnica.

Montesquieu. (1748). El espíritu de las leyes [en línea]. Ginebra, Barrillot & Son. [Consulta: 2026]. Disponible en: https://proletarios.org/books/Montesquieu-Espiritu_De_Las_Leyes.pdf

Navajas, C. (2016). Las Fuerzas Armadas y la sociedad en la España democrática [en línea]. Ayer. N.º 104, pp. 231-246.

[Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5771296

Neag, M. et al. (2019). Contribution to the participation of military structures in the fight against terrorism [en línea]. Scientific Journal of the Military University of Land Forces. 51(4), pp. 605-615. [Consulta: 2026]. Disponible en: https://doi.org/10.5604/01.3001.0013.6409

Pelletier, P. y Drozda-Senkowska, E. (2016). The Charlie Hebdo terror attack in Paris: Follow-up of French citizens' terrorist threat perception and its aftermath [en línea]. International Review of Social Psychology. 29(1), pp. 85-98. [Consulta: 2026]. Disponible en: https://doi.org/10.5334/irsp.51

Pérez, C. y Valiño, A. (2016). Repercusiones de la lucha contra el terrorismo sobre la defensa nacional y sus costes [en línea]. ICE Economía del Terrorismo. N.º 893, pp. 101-113. [Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6074238

Salvador, J., Almaraz, S. y Penilla, P. (2021). Las Fuerzas Armadas españolas en la lucha antiterrorista [en línea]. Revista del Instituto Español de Estudios Estratégicos. N.º 18, pp. 111-144. [Consulta: 2026]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8459848

Sansó-Rubert Pascual, D. (2017). Inteligencia militar y criminalidad organizada. Retos a debatir en América Latina [en línea]. URVIO, Revista Latinoamericana de Estudios de Seguridad. N.º 21, pp. 22-38. [Consulta: 2026]. Disponible en: https://revistas.flacsoandes.edu.ec/urvio/article/view/2952/2013

Secrétariat général de la défense et de la sécurité nationale. (2016). Plan VIGIPIRATE: Vigilance, prévention et protection face à la menace terroriste. Francia. Disponible en https://www.sgdsn.gouv.fr/files/files/Vigipirate/plan-vigipirate-gp-bd.pdf

Vergnano, C. (2023). Italian Uprising from Covid Skepticism to Societal Polarization [en línea]. En: Butter, M. y Knight, P. (eds.). Covid Conspiracy Theories in Global Perspective. Routledge. [Consulta: 2026]. Disponible en: https://doi.org/10.4324/9781003330769-23

Composición del grupo de trabajo

Presidente:	**Jose Antonio Fuentes de la Orden** *General de brigada del Ejército de Tierra. Jefe de Estudios de la Escuela Superior de las Fuerzas Armadas (ESFAS)*.
Coordinador:	**Raúl Sampedro Oliver** Teniente coronel psicólogo. Sección de Acción Tutorial de la Escuela Superior de las Fuerzas Armadas.
Vocales:	**Antonio Balas Dávila** Teniente coronel de la Guardia Civil.
	Noel Díaz Muñoz Comandante del Ejército del Aire y del Espacio.
	Francisco Freire Rodríguez *Comandante del Ejército de Tierra.*

Jaime Graus Thiesen

Comandante del Ejército de Tierra.

Miguel Requeno Soler

Comandante del Ejército de Tierra.

Diego Abel Redondo Olmedo

Comandante de la Guardia Civil.

Fernando Casado Yagüe

Comandante del Ejército de Tierra.

Jordi Francesc Rubio Carceller

Comandante del Ejército de Tierra.

Patricio Adrián Alisi

Capitán de fragata de la Armada argentina.

Juan Miguel Planchuelo Castiñeira

Inspector jefe de la Policía Nacional.

Relación de Monografías del CESEDEN

1. Clausewitz y su entorno intelectual. Kant, Guibert, Fichte, Moltke, Schlieffen, Lenin
2. Las Conversaciones de Desarme Convencional (CFE)
3. Disuasión convencional y conducción de conflictos: el caso de Israel y Siria en el Líbano
4. Cinco sociólogos de interés militar
5. Primeras Jornadas de Defensa Nacional
6. Prospectiva sobre cambios políticos en la antigua URSS. Escuela de Estados Mayores Conjuntos. XXIV Curso 91/92
7. Cuatro aspectos de la defensa nacional. (Una visión universitaria)
8. Segundas Jornadas de Defensa Nacional
9. IX y X Jornadas CESEDEN-IDN de Lisboa
10. XI y XII Jornadas CESEDEN-IDN de Lisboa
11. Anthology of the essays
12. XIII Jornadas CESEDEN-IDN de Portugal. La seguridad de la Europa Central y la Alianza AtlánticaTerceras Jornadas de Defensa Nacional
13. II Jornadas de Historia Militar. La presencia militar española en Cuba (1868-1895)
14. La crisis de los Balcanes
15. La Política Europea de Seguridad Común (PESC) y la Defensa
16. Second anthology of the essays
17. Las misiones de paz de la ONU

18. III Jornadas de Historia Militar. Melilla en la historia militar española
19. Cuartas Jornadas de Defensa Nacional
20. La Conferencia Intergubernamental y de la Seguridad Común Europea
21. IV Jornadas de Historia Militar. El Ejército y la Armada de Felipe II, ante el IV centenario de su muerte
22. Quintas Jornadas de Defensa Nacional
23. Altos estudios militares ante las nuevas misiones para las Fuerzas Armadas
24. Utilización de la estructura del transporte para facilitar el cumplimiento de las misiones de las Fuerzas Armadas
25. Valoración estratégica del estrecho de Gibraltar
26. La convergencia de intereses de seguridad y defensa entre las Comunidades Europeas y Atlánticas
27. Europa y el Mediterráneo en el umbral del siglo XXI
28. I Congreso Internacional de Historia Militar. El Ejército y la Armada en 1898: Cuba, Puerto Rico y Filipinas
29. Un estudio sobre el futuro de la no-proliferación
30. El islam: presente y futuro
31. Comunidad Iberoamericana en el ámbito de la Defensa
32. La Unión Europea Occidental tras Ámsterdam y Madrid
33. Iberoamérica, un reto para España y la Unión Europea en la próxima década
34. La seguridad en el Mediterráneo. Coloquios C-4/1999
35. Marco normativo en que se desarrollan las operaciones militares
36. Aproximación estratégica española a la última frontera: la Antártida
37. Modelo de seguridad y defensa en Europa en el próximo siglo
38. V Jornadas de Historia Militar. La aviación en la guerra española
39. Retos a la seguridad en el cambio de siglo. (Armas, migraciones y comunicaciones)
40. La convivencia en el Mediterráneo Occidental en el siglo XXI
41. La seguridad en el Mediterráneo. Coloquios C-4/2000
42. Rusia: conflictos y perspectivas

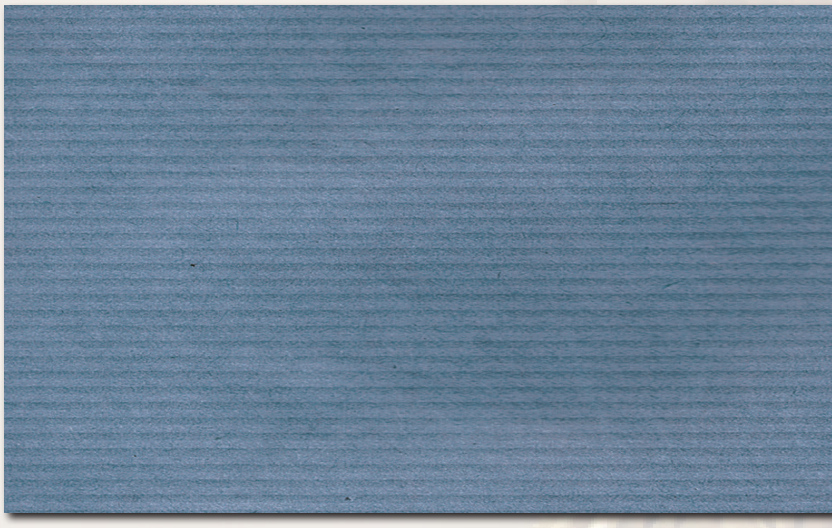
43. Medidas de confianza para la convivencia en el Mediterráneo Occidental
44. La cooperación Fuerzas de Seguridad-Fuerzas Armadas frente a los riesgos emergentes
45. La ética en las nuevas misiones de las Fuerzas Armadas
46. VI Jornadas de Historia Militar. Operaciones anfibias de Gallípoli a las Malvinas
47. La Unión Europea: logros y desafíos
48. La seguridad en el Mediterráneo. Coloquios C-4/2001
49. Un nuevo concepto de la defensa para el siglo XXI
50. Influencia rusa en su entorno geopolítico
51. Inmigración y seguridad en el Mediterráneo: el caso español
52. Cooperación con Iberoamérica en el ámbito militar
53. Retos a la consolidación de la Unión Europea
54. Revisión de la Defensa Nacional
55. Investigación, Desarrollo e innovación (I+D+i) en la Seguridad y la Defensa
56. VII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Génesis de la España contemporánea
57. La seguridad en el Mediterráneo. Coloquios C-4/2002
58. El Mediterráneo: Proceso de Barcelona y su entorno después del 11 de septiembre
59. La industria de defensa: el desfase tecnológico entre la Unión Europea y Estados Unidos de América
60. La seguridad europea y las incertidumbres del 11 de septiembre
61. Medio ambiente y Defensa
62. Pensamiento y pensadores militares iberoamericanos del siglo xx y su influencia en la Comunidad Iberoamericana
63. Estudio preliminar de la operación: Libertad para Irak
64. Adecuación de la defensa a los últimos retos
65. VIII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). La organización de la defensa de la Monarquía
66. Fundamentos de la estrategia para el siglo XXI
67. Las fronteras del mundo iberoamericano

68. Occidente y el Mediterráneo: una nueva visión para una nueva época
69. IX Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Las bases de la potencia hispana
70. Un concepto estratégico para la Unión Europea
71. El vínculo transatlántico
72. Aproximación a las cuestiones de seguridad en el continente americano
73. Defensa y Sociedad Civil
74. Las organizaciones internacionales y la lucha contra el terrorismo
75. El esfuerzo de defensa. Racionalización y optimización
76. El vínculo transatlántico en la guerra de Irak
77. Mujer, Fuerzas Armadas y conflictos bélicos. Una visión panorámica
78. Terrorismo internacional: enfoques y percepciones
79. X Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). El acontecer bélico y sus protagonistas
80. Opinión pública y Defensa Nacional en Iberoamérica
81. Consecuencias de la guerra de Irak en el Mediterráneo Occidental
82. La seguridad en el Mediterráneo. Coloquio C-4/2004-2005
83. Hacia una política de cooperación en Seguridad y Defensa con Iberoamérica
84. Futuro de la Política Europea de Seguridad y Defensa
85. Una década del Proceso de Barcelona: evolución y futuro
86. El conflicto árabe-israelí: nuevas expectativas
87. Avances en tecnologías de la información y de las comunicaciones para la Seguridad y la Defensa
88. La seguridad en el Mediterráneo. Coloquio C-4/2006
89. La externalización en las Fuerzas Armadas: equilibrio entre el apoyo logístico propio y el externalizado
90. La adhesión de Turquía a la Unión Europea
91. La seguridad en el Mediterráneo: complejidad y multidimensionalidad
92. La situación de seguridad en Irán: repercusión en el escenario regional y en el entorno mundial

93. Tecnología y Fuerzas Armadas
94. Integración de extranjeros en las Fuerzas Armadas españolas
95. El mundo iberoamericano ante los actuales retos estratégicos
96. XI Jornadas de Historia Militar. La enseñanza de la historia militar en las Fuerzas Armadas
97. La energía y su relación con la Seguridad y Defensa
98. Prospectiva de Seguridad y Defensa: viabilidad de una unidad de prospectiva en el CESEDEN
99. Repercusión del actual reto energético en la situación de seguridad mundial
100. La evolución de la Seguridad y Defensa en la Comunidad Iberoamericana
101. El Oriente Próximo tras la crisis de El Líbano
102. Los estudios de posgrado en las Fuerzas Armadas
103. Las fronteras exteriores de la Unión Europea
104. La industria y la tecnología en la Política Europea de Seguridad y Defensa
105. De la milicia concejil al reservista. Una historia de generosidad
106. La Agencia Europea de Defensa: pasado, presente y futuro
107. China en el sistema de seguridad global del siglo XXI
108. Naciones Unidas como principal elemento del multilateralismo del siglo XXI
109. Las relaciones de poder entre las grandes potencias y las organizaciones internacionales
110. Las nuevas guerras y la polemología
111. La violencia del siglo XXI. Nuevas dimensiones de la guerra
112. Influencia de la nueva Rusia en el actual sistema de seguridad
113. La nueva geopolítica de la energía
114. Evolución del concepto de interés nacional
115. Sesenta años de la OTAN ¿Hacia una nueva estrategia?
116. La importancia geoestratégica del África Subsahariana
117. El Mediterráneo: cruce de intereses estratégicos

118. Seguridad Nacional y estrategias energéticas de España y Portugal
119. Las armas NBQ-R como armas de terror
120. El futuro de las relaciones Latinoamérica-Estados Unidos
121. La influencia social del islam en la Unión Europea
122. África ¿nuevo escenario de confrontación?
123. Las nuevas guerras: globalización y sociedad
124. El impacto de la crisis económica en el área de la Seguridad y la Defensa
125. El ciberespacio. Nuevo escenario de confrontación
126. En una sociedad posheroica: la transformación del paradigma militar
127. Los ámbitos no terrestres en la guerra futura: espacio
128. Valores y conflictos. Las claves culturales en el conflicto del siglo XXI
129. Análisis prospectivo de las operaciones de multipolaridad
130. Nuevas guerras. Nuevas paces
131. Valores y conflictos. Aproximación a la crisis
132. Análisis y evaluación de la estabilidad del Magreb
133. África: riesgos y oportunidades en el horizonte de 2035
134. Enfoque integral de la seguridad en el espacio marítimo español
135. El liderazgo en las Fuerzas Armadas del siglo XXI
136. Necesidad de una conciencia nacional de ciberseguridad. La ciber–defensa: un reto prioritario
137. Racionalización de las estructuras de las Fuerzas Armadas. Hacia una organización conjunta
138. África futuro escenario de operaciones militares
139. Capacidades futuras de las Fuerzas Armadas
140. Recursos vitales y recursos energéticos. Implicaciones para la seguridad
141 - B. Vital resources and energy resources. Repercussions for security
141. Nanociencia, nanotecnología y defensa
142. La piratería emergente en el Golfo de Guinea. Estrategia de la UE para el Golfo de Guinea
143. África
144. Nuestra frontera más avanzada entre el Sahara Occidental y Senegal

145. La industria de defensa en España tras los consejos europeos de diciembre de 2013 y junio de 2015
146. La geopolítica líquida del siglo XXI
147. Inteligencia. Un enfoque integral
148. El nivel operacional
149. Efectos sobre la PCSD de la Unión Europea de la crisis migratoria
150. La coordinación de elementos militares policiales y judiciales en las misiones de reconstrucción de los Estados
151. Las migraciones internacionales, percepción y realidad. Un análisis desde la perspectiva de la seguridad
152. XIX CEMFAS. Selección de trabajos fin de curso
153. Selección de los ocho mejores trabajos de fin de curso del XX CEMFAS en el año escolar 2018-2019 impartido en el CESEDEN
154. Selección de los ocho mejores trabajos de fin de curso del XXI CEMFAS en el año escolar 2019-2020 impartido en el CESEDEN
155. Selección de los ocho mejores trabajos de fin de curso del XXII CEMFAS en el año escolar 2020-2021 impartido en el CESEDEN
156. Selección de los ocho mejores trabajos de fin de curso del XXIII CEMFAS y el mejor trabajo fin de curso del XV CSIFAS en el año escolar 2021-2022 impartido en el CESEDEN
157. Selección de los ocho mejores trabajos de fin de curso del XXIV CEMFAS y el mejor trabajo de fin de curso del XVI CSIFAS en el año escolar 2022-2023 impartido en el CESEDEN
158. Selección de los ocho mejores trabajos de fin de curso del XXV CEMFAS y el mejor trabajo de fin de curso del XVII CSIFAS en el año escolar 2023-2024 impartido en el CESEDEN



PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL