La transformación de la inteligencia a través de la innovación

Cdi 3

CUADERNOS DE INTELIGENCIA

MINISTERIO
DE DEFENSA

La transformación de la inteligencia a través de la innovación

CUADERNOS DE INTELIGENCIA

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

Entidad colaboradora:
Universidad Nebrija

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

© Autores y editor, 2025

NIPO 083-25-228-X (edición impresa)
ISSN 3101-3740 (edición impresa)

NIPO 083-25-229-5 (edición en línea)

Depósito legal M 18633-2025
Fecha de edición: diciembre de 2025
Maqueta e imprime: Imprenta Ministerio de Defensa

Las opiniones emitidas en esta publicación son de exclusiva responsabilidad de los autores 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.

publicaciones.defensa.gob.es
cpage.mpr.gob.es

Índice

Presentación 11
Carlos Alberto Ramírez Sánchez

Artículo primero

La transformación de la inteligencia en la seguridad y defensa de Europa: desafíos y oportunidades en la era digital 15
Carlos Hugo Fernández-Roca Suárez

1 Introducción 17
2 Impactos de la Cuarta Revolución Industrial en la inteligencia de defensa 17
3 La inteligencia artificial como factor transformador 18
4 Respuestas institucionales de Europa: del Plan ReArm Europe a la Estrategia Industrial de Defensa 20
5 Casos de aplicación tecnológica en inteligencia y defensa 23
6 La búsqueda de la soberanía tecnológica europea 26
7 Aspectos normativos en la transformación digital de la seguridad y defensa en Europa 27
8 Escenarios prospectivos hacia 2040: el futuro de la inteligencia digital europea 29
8.1 Escenario primero: autonomía e inteligencia europea integrada 29
8.2 Escenario segundo: dependencia persistente 30
8.3 Escenario tercero: cooperación condicionada 31
9 Conclusiones 32
Referencias bibliográficas 34

Artículo segundo

***Conductual explorer:* una solución autónoma frente al desafío del entorno cognitivo** 37
Pablo Caneda González, María Porrar Santisteban, Álvaro Álvarez Álvarez

1 Introducción 39
1.1 Motivación: resolver necesidades internas con creatividad y bajo coste 40
1.2 Contexto del proyecto y su relevancia 41
1.3 Objetivos y alcance del programa 42

2 Necesidad de un analista y creación de la base de datos 43
2.1 Análisis de la Zona: recopilación y estructuración de datos 44
2.1.1 Definición del ámbito de estudio 44
2.1.2 Selección y filtrado de fuentes de información 44
2.1.3 Identificación de actores clave 45
2.2 Herramientas empleadas en el análisis inicial 47
2.3 Construcción de una base de datos 48
3 Códigos desarrollados y su funcionamiento 49
3.1 Código 1: análisis de sentimiento del entorno informativo 49
3.1.1 Objetivo y lógica detrás del análisis 49
3.1.2 Técnicas utilizadas: procesamiento del lenguaje natural (PLN) y clasificación por taxonomías 50
3.1.3 Ejemplo práctico y resultados esperados 51
3.2 Código 2: clasificación de redes sociales y MMCC con *machine learning* 54
3.2.1 Definición de categorías y enfoque clasificatorio 54
3.2.2 Algoritmos y modelos implementados 56
3.2.3 Resultados esperados de un supuesto práctico 56
3.3 Código 3: clasificación de contenido en TikTok en varias fases 57
3.3.1. Filtrado por *hashtags* y taxonomías en la descripción del vídeo 58
3.3.2 Filtrado por análisis de comentarios 58
3.3.3 Filtrado por fotogramas mediante procesado de imágenes con *deep learning* 58
4 Conclusiones y aprendizajes 59
4.1 Impacto del programa en la organización 59
4.2 Principales aprendizajes y contribuciones 60
4.3 Próximos pasos y mejoras propuestas 61

Artículo tercero

Inteligencia posnormal: gestión de riesgos en la zona gris ... 63
Jesús Hernández Álvarez

1 Introducción 65
2 Ciencia posnormal 67
3 Del ciclo de la inteligencia a la gestión del riesgo 72
4 Inteligencia y cognición 76
4.1 Sesgos cognitivos 76
4.2 Pensamiento lineal vs. sistémico 78
4.3 Modelos mentales vs. modelos conceptuales 81
4.4 Conciencia situacional 82
5 Sistemas evolutivos 83
6 Un nuevo paradigma en la Inteligencia 86
7 El ámbito cognitivo como activo a proteger 87

8 Conclusiones: escenarios de innovación 88
Bibliografía 91

Artículo cuarto

Una experiencia real de uso de la IA en el análisis de fuentes abiertas: la factoría de análisis del Centro de Análisis y Prospectiva de la Guardia Civil 95

Enrique Ávila Gómez, Lorenzo Luna Zambrana

1 Introducción 97
2 El Centro de Análisis y Prospectiva de la Guardia Civil (CAP) 98
3 Escenario previo: idioma, detección, validación y tiempo 99
4 El problema del talento 110
5 Alucinaciones y otras cuestiones: una aproximación práctica 113
6 Conclusiones 119
Bibliografía 121

Artículo quinto

ECySAP y la conciencia situacional en operaciones de guerra multidominio 123

Antonio Legaz, Juan Tejero, José Francisco Suárez Mulero

1 Fundamentos de la Conciencia Situacional Cibernética (CySA) 125
1.1 Del Coup d'Oeil a la Conciencia Situacional Cibernética: transformación del paradigma militar 125
1.2 Evolución histórica de la conciencia situacional: de Sun Tzu al entorno digital 125
1.3 Marco teórico de la Conciencia Situacional Cibernética: el modelo de Endsley en el Ciberespacio 126
1.4 Contexto operativo contemporáneo: guerra multidominio y enfoque mosaico 127
2 ECySAP: plataforma integral para la Conciencia Situacional Cibernética 128
2.1 Arquitectura funcional de ECySAP: de la percepción a la proyección 129
2.2 Aplicaciones de ECySAP en la planificación operativa y cursos de acción 130
2.3 Gestión de riesgos y evaluación de incidentes a través de ECySAP 130
2.4 Integración de inteligencia artificial: potenciando las capacidades de ECySAP 131
2.5 ECySAP en el contexto de la Guerra Mosaico: habilitador de Conciencia Situacional Multidominio 132
2.6 ECySAP como habilitador de operaciones sincronizadas en entornos multidominio 133
3 Marco doctrinal y normativo 134
3.1 La doctrina en ciberdefensa 134
3.2 Marco normativo 135

4 Caso de uso 137
4.1 Contexto histórico: guerra mosaico y anexión de Crimea 137
4.2 Capas de Análisis de ECySAP en el contexto Crimea-Rusia 138
4.3 Protección frente a la desinformación 139
4.4 Protección de infraestructura crítica 140
4.5 Protección de activos físicos militares 141
4.6 Conclusiones caso de uso 142
5 Conclusiones 143
Bibliografía 143

Artículo sexto

La innovación tecnológica en el área de la inteligencia de ciberamenazas y por extensión de la ciberdefensa 149
Juan Adolfo Montero

1 Introducción: la inteligencia de ciberamenazas como base de la transición de la ciberseguridad a la ciberdefensa 151
1.1 ¿Por qué la ciberseguridad tradicional ya no es suficiente? (Rodríguez, 2023) 152
1.2 Diferencias clave entre ciberseguridad y ciberdefensa 153
1.3 Analogía militar: ciberseguridad como defensa básica 153
2 La «Operacionalización» del ciberespacio 153
3 La ciberdefensa: un enfoque integral y dirigido por la Inteligencia de Ciberamenazas 154
3.1 Ventajas y desventajas del atacante y del defensor 154
3.2 Ciberdefensa: de la reacción a la anticipación 155
3.2.1 La Amenaza 155
3.2.2 La Misión 155
3.2.3 El ciberespacio a defender 156
3.3 Aplicación de inteligencia táctica, operacional y estratégica 156
3.4 El modelo IPB aplicado al ciberespacio (Cyber-IPB) 157
3.4.1 Cyber-IPB: objetivos y beneficios 158
3.5 Planes de ciberdefensa (Corletti Estrada, 2017) 159
3.5.1 Plan de Detección Avanzada 160
3.5.2 Plan de Obstáculos 160
3.5.3 Plan de Mitigación de Efectos 161
3.5.4 Plan de Reacción 161
3.5.5 Plan de Recuperación 161
4 Desafíos Tecnológicos en Ciberdefensa 162
4.1 Necesidad de soluciones nacionales y estratégicas 162
4.2 Necesidad de desarrollos y adquisiciones ágiles 163
4.3 Lagunas Tecnológicas 163
4.3.1 Conciencia Situacional (CySA) 163
4.3.2 Modelado de la ciberamenaza 164

5 Iniciativas tecnológicas impulsadas por el MCCE 167
5.1 Plataforma PICO 167
5.1.1 ¿Qué ofrece PICO? 167
5.2 ECYSAP / ECYSAP EYE 172
5.2.1 ECYSAP v1.0 172
5.2.2 ECYSAP v2.0 (ECYSAP EYE) 175
5.3 SCOMCE: sistema de Combate en el Ciberespacio 175
6 Requisitos tecnológicos avanzados para el SCOMCE 176
6.1 Tecnología de datalake 177
6.1.1 Fuentes de información y datos a integrar 178
6.1.2 Estructura del *datalake* 179
6.1.3 Desafío en la implementación de un *datalake* 179
6.2 Ontología 180
6.3 Aplicación de Inteligencia Artificial (IA) 181
6.4 Aplicación de técnicas de simulación 183
6.4.1 Simulación como herramienta estratégica 184
7 Conclusiones 185
Bibliografía 186

Artículo séptimo

Matrices de impacto cruzado y método estructural: una revisión parcial o de herramientas para la construcción de escenarios futuros 189

Licesio J. Rodríguez-Aragón

1 Introducción 190
2 Modelización y Simulación en Prospectiva 192
2.1 Modelización 193
2.2 Simulación 195
3 Matrices de Impacto Cruzado (Cross-Impact Matrix Methods) 196
4 Análisis Estructural de las Matrices de Impacto 198
5 Gráfico de Influencia x Dependencia 200
6 Multiplicación de la Matriz de Impactos Cruzados Aplicada a la Clasificación (Matrice d'Impacts Croisés Multiplication Appliquée à une Classification-MICMAC) 203
7 Conclusión 206
Bibliografía 208

Artículo octavo

La tecnología al servicio de la disuasión 211

Emilia José Peña Ruiz

1 Introducción 212
1.1 La necesidad de un sistema de salvaguardias 214

1.2 Cómo participan los sistemas de información geográfica en el sistema de salvaguardias 217
2 Un ejemplo práctico: el caso de Corea del Norte 221
3 Conclusión 224
Bibliografía 225

Artículo noveno

Transformación del ciclo JISR en la era digital: innovación tecnológica para alcanzar la superioridad informativa 227
Begoña Rojo Carralero
1 Introducción 229
2 Conceptos básicos del proceso ISR 230
3 JISR en las operaciones multidominio y el campo de batalla transparente 232
4 Iniciativas OTAN y europeas relacionadas con el ciclo de inteligencia 233
5 Transformación del proceso JISR: del modelo clásico al digital y multidominio 235
6 Impacto de las tecnologías emergentes en el proceso JISR 237
6.1 IA y Computación en el borde (edge computing) 237
6.2 Expansión y diversificación de sensores 239
6.3 Uso de plataformas no tripuladas 239
6.4 Tecnologías cuánticas 240
6.5 Espacio / satélites 241
6.6 Sistemas hipersónicos 243
6.7 Tendencias transversales en tecnologías emergentes aplicables a ISR 243
7 Posibles mejoras en cada una de las fases del proceso JISR 244
7.1 *Tasking* – Planificación y asignación de recursos 244
7.2 *Collection* – Obtención de información 245
7.3 *Processing* – Tratamiento y clasificación de datos e información 246
7.4 *Exploitation* – Análisis de los datos y la información 246
7.5 *Dissemination* – Difusión y uso de la información 246
7.6 Lecciones aprendidas y condiciones de éxito 247
8 Interoperabilidad y filosofía del «dato único» 247
9 Innovación tecnológica como amenaza al proceso JISR 249
9,1 La importancia de la ciberseguridad en el Proceso JISR 249
9.2 Sesgos y vulnerabilidades de la inteligencia artificial en el proceso JISR 250
10 Conclusión 251
Bibliografía 253

Artículo décimo

Adaptación de nuevas tecnologías en la comunidad JISR. Particularidades del ámbito marítimo 255
Alfonso Herrero Pita

1 La revolución de la información y la comunidad de inteligencia 257
2 Vectores de cambio 257
3 Adaptación de estructuras tradicionales 258
4 JISR como paradigma de innovación 258
5 Desafíos en la adaptación tecnológica a la capacidad JISR 259
5.1 Entorno original 259
5.2 Herramientas tecnológicas para ISR, ¿ISR = I + SR? 261
5.3 El entorno marítimo 262
5.4 Estándares de Interoperabilidad. MAJIIC2. ¿Proyectos frustrados? 263
5.5 Estándares de interoperabilidad; impacto organización (normalidad) 264
5.6 Estándares de interoperabilidad; impacto en operaciones caso del MCC 266
6 Conclusiones 266
Bibliografía 267

Artículo undécimo

Inteligencia narrativa en la era de la IA: análisis de la desinformación antiucraniana de Rusia 269

Viktoriia Romaniuk, Yevhen Fedchenko y traducido al castellano por Tara Zielinski

1 Introducción 271
2 Inteligencia de Narrativas: perspectivas interdisciplinarias y definiciones 273
3 Narrativas contra Ucrania 276
4 La inteligencia artificial y la promoción de narrativas contra Ucrania en las campañas de desinformación del Kremlin 278
5 El *deepfake* como una forma de diseminar narrativas desinformativas 282
5.1 Caso 1: Comandante en Jefe de las Fuerzas Armadas de Ucrania, el general Valerii Zaluzhnyi (2021-2024) 283
5.2 Caso 2: Comandante en Jefe de las Fuerzas Armadas de Ucrania, Oleksandr Syrskyi 285
5.3 Caso 3: Michael O'Flaherty, Alto Comisionado de Derechos Humanos del Consejo de Europa 286
6 Conclusiones 287
Bibliografía 288

Artículo duodécimo

¿Qué significa el crecimiento de la OSINT para los analistas de inteligencia militar? 293

Marcel Plichta, Edwin Dudley-Taylor y traducido al castellano por Daniel Blanco

1 Introducción 295
2 ¿Qué es OSINT? 295

3 Prioridades de la inteligencia militar y civil 296
4 Ventajas de la OSINT para los analistas militares 298
5 La utilización de la OSINT para mejorar y verificar la obtención 300
6 Uso de OSINT en transparencia e intercambio de inteligencia 301
7 Retos para los analistas militares 302
8 Restricciones legales y privatización de la obtención 304
9 Conclusiones 306
Bibliografía 307

Comité Científico y Consejo Editorial 309

Normas de envío de artículos 313

Presentación

Carlos Alberto Ramírez Sánchez

La tercera edición del «Cuaderno de Inteligencia» mantiene la línea de continuidad y desarrollo que ha caracterizado a los números anteriores.

El primer número, allá por el 2023, intentaba esbozar el nacimiento de una publicación que buscaba cubrir un espacio casi vacío de publicaciones sobre inteligencia centrándose, sobre todo, en un área poco conocida y enormemente compleja, como es la inteligencia militar.

El segundo ejemplar trataba de abrir el amplio abanico de la inteligencia a todos los organismos civiles y militares que conforman el riquísimo ecosistema que se enfrenta cada día a las amenazas que acechan la Seguridad Nacional.

Este tercer número reafirma una premisa fundamental: la inteligencia no constituye un patrimonio exclusivo de ningún organismo. Por el contrario, su valor reside en su capacidad de adaptarse a las necesidades específicas de cada entidad u organización, proporcionando asesoramiento eficaz a los responsables de la toma de decisiones.

Bajo esta perspectiva, adquiere especial relevancia el concepto de «Comunidad Nacional de Inteligencia Ampliada», que postula una sinergia integral de todas las capacidades en inteligencia del Estado para abordar amenazas y desafíos de forma cohesionada y eficaz.

En esta edición se da de nuevo voz a todas las vertientes de la inteligencia (militar, civil, policial, académica, empresarial, etc.) con la convicción de que, con el tiempo, lo que une a estos actores superará sus diferencias.

El «Cuaderno de Inteligencia» número tres, lleva por título genérico «La transformación de la inteligencia a través de la innovación». Se decidió centrar este número en la innovación aplicada a la inteligencia para intentar exponer las enormes transformaciones que la inteligencia está sufriendo, a caballo del desarrollo de la tecnología.

Conceptos como «campo de batalla transparente» ya no suenan a ciencia ficción. Al mismo tiempo, las noticias que llegan de las zonas de conflicto nos dejan sorprendidos por la eficacia que adquieren las operaciones militares cuando una inteligencia potenciada por las nuevas tecnologías proporciona al decisor una ventaja diferencial sobre sus oponentes: golpear antes y de forma más precisa.

El creciente interés del sector empresarial por integrar la inteligencia en sus estrategias ha impulsado la creación de departamentos especializados, los

cuales operan en coordinación con los organismos oficiales. Paralelamente, el ámbito académico ha experimentado una consolidación notable de sus programas de posgrado en inteligencia, tanto en número como en calidad, proyectando un horizonte no muy lejano en el que se verá un grado universitario en Inteligencia.

Este empuje académico, unido a la fuerza de las empresas, hace que la inteligencia de la Defensa tenga la oportunidad de avanzar y evolucionar convirtiéndose en una capacidad diferencial que facilita la eficaz defensa contra las amenazas actuales, cada vez más dinámicas y sorprendentes.

Una inteligencia meramente reactiva frente al avance tecnológico resultaría insuficiente para cumplir su misión. En cambio, una inteligencia que se consolide como disciplina proactiva e innovadora podrá brindar, en todos los ámbitos, la libertad de acción necesaria para mitigar los riesgos del mañana.

En el «Cuaderno de Inteligencia» número tres se tratan los siguientes temas:

— El avance decidido de la Unión Europea hacia la consecución de una soberanía tecnológica que garantice plenamente su autonomía estratégica, para lo que se está avanzando en tecnologías aplicadas a la inteligencia.

— Una solución de las FAS al reto de mantenerse actualizado sobre el entorno cognitivo y sus amenazas.

— Se explorará la ciencia posnormal como marco conceptual para abordar problemas con hechos inciertos, valores en conflicto y decisiones urgentes, así como la evolución desde el ciclo de inteligencia tradicional hacia un enfoque de gestión de riesgos, integrando las funciones de inteligencia y gobernanza, en la búsqueda de una visión compartida del problema de seguridad a gestionar.

— Se abordará cómo la inteligencia artificial generativa transforma la detección, selección y análisis de información, permitiendo un acceso más rápido y amplio a fuentes diversas.

— Se estudiará con detenimiento la conciencia situacional en operaciones de guerra multidominio.

— Se analizará el surgimiento de la Ciberdefensa, que, gracias al desarrollo de tecnologías avanzadas, puede integrar la inteligencia de ciberamenazas para planificar y conducir operaciones defensivas.

— En un interesante trabajo, se pretenden presentar algunas de las herramientas que se utilizan a la hora de trabajar con las matrices de impacto y que permiten analizar las relaciones indirectas y clasificar las variables del sistema.

— Se intentará comprender cómo las nuevas tecnologías aplicadas a los medios de obtención pueden ayudar ante el desafío de algunos países proliferantes cuyas actividades nucleares parecen alejarse del curso pacífico.

— Se examinará el impacto que las nuevas tecnologías producen en cada fase del proceso JISR (TCPED), así como los retos derivados de su uso.

— Se tratará de trasladar los cambios tecnológicos a la conducción de operaciones ISR en el ámbito marítimo, detallando las particularidades que ofrece debido a la singular organización de una fuerza naval en un Mando Componente Marítimo.

— Nos sumergiremos en la Inteligencia Narrativa (NARINT), herramienta crucial para comprender y contrarrestar la guerra de información, centrándonos en el contexto de guerra de Rusia contra Ucrania desde 2014.

— Por último, se repasará el impacto de las nuevas tecnologías en el analista, que se ve bombardeado por enormes cantidades de información procedentes de fuentes abiertas.

Para concluir esta presentación, es de justicia expresar nuestro agradecimiento a todos los expertos que, con sus aportaciones, contribuyen a que esta publicación se consolide como una plataforma de referencia desde la cual impulsar el desarrollo y la eficacia de la inteligencia.

La transformación de la inteligencia en la seguridad y defensa de Europa: desafíos y oportunidades en la era digital

Carlos Hugo Fernández-Roca Suárez

Resumen

La inteligencia en seguridad y defensa está experimentando una profunda transformación impulsada por la aceleración tecnológica de la cuarta revolución industrial, caracterizada por avances notables en digitalización, automatización, inteligencia artificial y gestión masiva de datos. Este salto tecnológico, sumado a un escenario geopolítico cada vez más desafiante, sobre todo, tras la agresión rusa contra Ucrania, obliga a Europa a reforzar urgentemente sus capacidades estratégicas de forma coordinada y efectiva.

En este nuevo contexto, la inteligencia artificial emerge como motor fundamental del cambio, revolucionando la obtención, análisis y difusión de inteligencia militar, así como la automatización eficiente de procesos estratégicos y tácticos. Ejemplos internacionales relevantes, como la «guerra algorítmica» del Project Maven en Estados Unidos, ilustran cómo la inteligencia artificial incrementa significativamente la capacidad de anticipación y reacción frente a amenazas actuales y futuras.

La Unión Europea avanza decididamente hacia la consecución de una soberanía tecnológica que garantice plenamente su autonomía estratégica. Con este propósito, iniciativas clave como el programa «Preparación 2030» —inicialmente anunciado como ReArm Europe— y el Fondo Europeo de Defensa impulsan inversiones orientadas al desarrollo de tecnologías emergentes, fortaleciendo así la base industrial europea y reduciendo las dependencias externas en un contexto internacional cada vez más exigente y competitivo.

Palabras clave

Inteligencia artificial (IA), Soberanía tecnológica, Autonomía estratégica, Cuarta revolución industrial y Defensa europea.

The transformation of intelligence in Europe's security and defence: challenges and opportunities in the digital age

Abstract

Intelligence in security and defense is undergoing a profound transformation driven by the technological acceleration of the Fourth Industrial Revolution, characterized by significant advances in digitalization, automation, artificial intelligence, and large-scale data management. This technological leap, combined with an increasingly challenging geopolitical landscape —especially following Russia's aggression against Ukraine— compels Europe to urgently strengthen its strategic capabilities in a coordinated and effective manner.

In this new context, artificial intelligence emerges as a fundamental driver of change, revolutionizing the collection, analysis, and dissemination of military intelligence, as well as efficiently automating strategic and tactical processes. Relevant international examples, such as the «algorithmic warfare» of Project Maven in the United States, demonstrate how artificial intelligence significantly enhances capabilities for anticipation and reaction to current and future threats.

The European Union is decisively progressing toward achieving technological sovereignty that fully guarantees its strategic autonomy. To this end, key initiatives such as the «Preparation 2030» program —initially announced as ReArm Europe— and the European Defence Fund promote investments aimed at developing emerging technologies, thus strengthening Europe's industrial base and reducing external dependencies in an increasingly demanding and competitive international environment.

Keywords

Artificial Intelligence (AI), Technological Sovereignty, Strategic Autonomy, Fourth Industrial Revolution, and European Defence.

1 Introducción

La seguridad y la defensa de Europa están inmersas en una profunda transformación, impulsada por avances tecnológicos sin precedentes en el ámbito digital. La acelerada evolución de la cuarta revolución industrial —caracterizada por avances en digitalización, automatización, datos masivos e inteligencia artificial (en adelante, IA)— está alterando la forma en que se recopila, analiza y emplea la inteligencia en el ámbito militar y estratégico. Estos desarrollos tecnológicos, junto con un entorno geopolítico más desafiante tras acontecimientos como la agresión rusa a Ucrania, han convencido a Europa de la necesidad de reforzar sus capacidades de seguridad y defensa de manera urgente y coordinada (Consejo Europeo, 2022).

Los gobiernos de la Unión Europea (en adelante, UE) han reconocido que invertir en tecnologías emergentes y en la base industrial de defensa es esencial para mejorar la capacidad europea, asumir una mayor cuota de la carga en la seguridad transatlántica y reducir dependencias críticas en materia de tecnología y armamento (Fiott, 2024). En este contexto, instituciones europeas y Estados miembros están emprendiendo reformas y planes ambiciosos para modernizar la inteligencia de defensa, incorporando IA y otras tecnologías disruptivas, al tiempo que promueven la soberanía tecnológica europea como un objetivo común que refuerza, y no contradice, la identidad y los intereses nacionales.

Este artículo analiza dicha transformación de la inteligencia en Europa, abarcando el impacto de la Cuarta Revolución Industrial, el papel central de la IA, las respuestas institucionales —como el plan ReArm Europe—, ejemplos concretos de aplicación tecnológica y la búsqueda de autonomía tecnológica.

2 Impactos de la Cuarta Revolución Industrial en la inteligencia de defensa

La denominada cuarta revolución industrial (en adelante, 4RI) ha sido descrita como un cambio de época de naturaleza disruptiva que difumina las fronteras entre lo físico y lo digital, lo civil y lo militar, la paz y el conflicto (Fojón, 2018). Al igual que revoluciones industriales previas transformaron la conducción de la guerra, la 4RI está introduciendo tecnologías avanzadas —como sistemas autónomos, *big data*, computación en la nube, Internet de las Cosas y aprendizaje automático— que plantean tanto oportunidades como retos para la defensa. En el ámbito de la inteligencia militar y estratégica, estos cambios implican la capacidad de procesar volúmenes masivos de información en tiempo real, provenientes de fuentes cada vez más diversas —sensores remotos, redes sociales, imágenes satelitales comerciales—, así como la automatización de tareas analíticas rutinarias mediante algoritmos.

Las fuerzas armadas y agencias de inteligencia europeas deben adaptarse a este nuevo entorno tecnológico para mantener la superioridad informativa y la capacidad de anticipación. Esto supone transformar doctrinas y procedimientos de inteligencia tradicionales. Por ejemplo, la proliferación de sensores avanzados y plataformas no tripuladas aumenta, de forma exponencial, los datos recabados —señales, imágenes, comunicaciones—, lo que exige nuevas herramientas de fusión de datos y análisis apoyadas en IA para extraer información relevante. A su vez, actores no estatales y potencias rivales también acceden a tecnologías de doble uso asequibles —como drones o software de ciberataque— que «democratizan» el acceso al poder disruptivo, obligando a las agencias europeas a acelerar su innovación (Fojón, 2018). En definitiva, la 4RI está alterando los cimientos de la inteligencia de seguridad y defensa, haciendo obsoletos métodos tradicionales y requiriendo inversiones en nuevas capacidades técnicas, organizativas y humanas.

Un ejemplo ilustrativo es el concepto de «guerra algorítmica» desarrollado, inicialmente, por el Departamento de Defensa de EE. UU., donde se emplean algoritmos para multiplicar las opciones y acelerar la toma de decisiones en el campo de batalla (Fojón, 2018). Iniciativas pioneras como el Project Maven estadounidense —que aplica aprendizaje automático para analizar imágenes de inteligencia (IMINT) y detectar objetivos— han servido de referencia sobre cómo la automatización inteligente puede elevar la eficacia de la inteligencia militar. Europa ha tomado nota de estas tendencias: España ha evaluado las lecciones de Maven para considerar aplicaciones similares en nuestras fuerzas armadas (Fojón, 2018). La implantación de herramientas derivadas de la 4RI conlleva también interrogantes éticos y doctrinales —por ejemplo, sobre el grado de autonomía permisible en sistemas de armas inteligentes o la confiabilidad de una decisión tomada por una máquina—, debates que están muy presentes en el entorno europeo, donde impera un enfoque humano-céntrico en el uso de la IA (Csernatoni, 2023).

3 La inteligencia artificial como factor transformador

Entre las tecnologías de la 4RI, la IA destaca como el motor central de transformación de la inteligencia en seguridad y defensa. La IA —entendida, en términos generales, como sistemas informáticos capaces de realizar tareas que normalmente requieren inteligencia humana, aprendiendo de la experiencia (Fiott y Lindstrom, 2018)— se ha convertido en una herramienta estratégica de primer orden en los ámbitos militar y de seguridad (Csernatoni, 2023). Potencias como Estados Unidos y China ya integran la IA en sus doctrinas de defensa, considerándola un elemento clave de superioridad tecnológica y alertando incluso de una posible nueva carrera armamentística en este terreno (Csernatoni, 2023). En Europa, aunque su desarrollo ha

sido más lento, existe una conciencia creciente sobre el potencial revolucionario de la IA en el ámbito de la defensa. Por un lado, puede ofrecer ventajas significativas en inteligencia —como el análisis automatizado de amenazas, la simulación de escenarios o el apoyo a la toma de decisiones—; por otro, suscita preocupaciones éticas y de seguridad —como los sesgos algorítmicos, la autonomía letal o las vulnerabilidades cibernéticas, que exigen un marco normativo equilibrado y adaptado a los desafíos emergentes—.

En el campo de la inteligencia militar, la IA promete acelerar y optimizar todo el ciclo de inteligencia: desde la fase de obtención de datos —mediante algoritmos capaces de rastrear fuentes abiertas o gestionar enjambres de sensores—, pasando por el análisis —que incluye el filtrado inteligente de información relevante, el reconocimiento automático de patrones en imágenes o interceptaciones, y la detección de anomalías—, hasta la distribución y explotación de la inteligencia, a través de sistemas de apoyo a la decisión que ofrecen a analistas y mandos opciones óptimas generadas a partir del procesamiento de grandes volúmenes de datos.

Por ejemplo, algoritmos de aprendizaje profundo aplicados a imágenes satelitales pueden identificar movimientos de equipos militares adversarios con mucha mayor rapidez que analistas los humanos, permitiendo alertas tempranas. Del mismo modo, herramientas de procesamiento de lenguaje natural pueden clasificar y traducir automáticamente comunicaciones interceptadas, aumentando la eficiencia de la inteligencia de señales.

Estas capacidades podrían mejorar la detección de amenazas, la protección y la preparación ante riesgos emergentes (Fiott y Lindstrom, 2018), reforzando así la seguridad colectiva europea.

No obstante, los efectos de la IA no son unívocamente positivos ni plenamente conocidos. Existe cierto consenso en que, al menos en el corto plazo, la IA actuará como «facilitador estratégico» más que como sustituto total de la inteligencia humana (Fiott y Lindstrom, 2018). Es decir, la autonomía de los sistemas de IA seguirá siendo limitada y el factor humano continuará siendo crítico en la supervisión de algoritmos y en la toma de decisiones finales.

De hecho, la UE ha subrayado la importancia de mantener «control humano significativo» sobre los sistemas de armas autónomos y la inteligencia artificial militar, atendiendo a consideraciones éticas y legales (Parlamento Europeo, 2020). A medida que la IA avanza, Europa enfrenta el reto de aprovechar sus ventajas sin incurrir en riesgos inaceptables: por ejemplo, asegurar que un sistema de IA no introduzca sesgos o errores sistemáticos en el análisis de inteligencia, o que preserve su integridad operativa ante intentos de manipulación, como los ataques que buscan engañar a los algoritmos de reconocimiento.

Por otra parte, la inteligencia artificial no solo actúa como herramienta, sino que también se está consolidando como un objetivo estratégico y un nuevo campo de confrontación. Su progresiva militarización —que abarca aplicaciones ofensivas como los ciberataques, la desinformación potenciada por IA o los vehículos armados no tripulados— obliga a los servicios de inteligencia europeos a desarrollar capacidades específicas de detección, prevención y respuesta (Csernatoni, 2023). Este dilema refuerza la necesidad de que Europa no se quede atrás en el dominio de la IA aplicada a defensa, pero a la vez lidere su uso responsable y conforme al derecho internacional.

En la actualidad, las instituciones de la UE reconocen que la IA es un arma de doble filo: pude reforzar la seguridad —por ejemplo, en tareas de vigilancia y alerta temprana—, pero también plantea amenazas si se emplea de forma maliciosa o escapa al control humano (Csernatoni, 2023). Por ello, la Unión aboga por una IA «fiable, ética y segura», incluso en entornos militares, integrando estos principios en sus políticas y proyectos de investigación vinculados a la defensa.

4 Respuestas institucionales de Europa: del Plan ReArm Europe a la Estrategia Industrial de Defensa

Conscientes de la magnitud del desafío tecnológico, las instituciones europeas han articulado en los últimos años una serie de respuestas estratégicas e iniciativas políticas para transformar sus capacidades en materia de inteligencia, seguridad y defensa. Un hito importante fue la adopción de la Brújula Estratégica de la UE en marzo de 2022, la cual delineó una visión común de seguridad y defensa para la próxima década, enfatizando, entre otros aspectos, la necesidad de mejorar la inteligencia compartida y anticipativa (Consejo de la UE, 2022).

En concreto, la Brújula destacó la creación de mecanismos como la Capacidad Única de Análisis de Inteligencia (*Single Intelligence Analysis Capacity, SIAC*), orientados a integrar mejor la información procedente de los Estados miembros y proporcionar evaluaciones de amenazas más sólidas a nivel de la UE (Consejo de la UE, 2022). Este enfoque estratégico sentó las bases para posteriores planes más específicos en materia de capacidades y tecnología.

Tras la invasión de Ucrania en 2022, la UE ha dado un paso significativo al reconocer que debía «rearmarse» y fortalecer su postura defensiva de manera acelerada para 2030. La presidenta de la Comisión Europea, Ursula von der Leyen, abogó por movilizar recursos a una escala inédita para dotar a Europa de una disuasión creíble antes del final de la década. Fruto de esta voluntad política, la Comisión presentó el plan conocido, inicialmente, como ReArm Europe, un ambicioso programa dirigido a concentrar y coordinar la

inversión en defensa por parte de los Estados miembros, contando con el apoyo de fondos europeos (Comisión Europea, 2025).

Actualmente, esta iniciativa ha adoptado la denominación «Preparación 2030», debido a las reticencias mostradas por algunos países, entre ellos, España e Italia, respecto al término original, considerado demasiado belicista o sensible desde una perspectiva política y social.

Este plan prevé movilizar más de 800 000 millones de euros en inversión en defensa acumulada hasta 2030. Su objetivo es reducir las divergencias entre los Estados miembros y aprovechar las economías de escala del mercado común. Entre los objetivos concretos de la iniciativa ReArm Europe se encuentran: elevar al 50 % la proporción del gasto en adquisiciones militares destinada a proveedores europeos —fortaleciendo así la Base Industrial y Tecnológica de la Defensa Europea (en adelante, BITDE)— y lograr que, al menos el 35 % de las nuevas capacidades, se adquieran de forma conjunta entre varios Estados miembros, frente al escaso 18 % actual (Fiott, 2024).

Asimismo, se prevé un aumento significativo en el intercambio de armamento y componentes entre países europeos. Si se alcanzan estos objetivos, Europa no solo avanzaría en su autonomía tecnológica, sino que también corregiría deficiencias estructurales de larga data en áreas clave —como las comunicaciones seguras, la vigilancia espacial, la defensa aérea o la ciberdefensa—, muchas de las cuales dependen directamente de capacidades avanzadas de inteligencia. Aunque, a mi juicio, habría que considerar cómo introducir de manera más clara el concepto de soberanía estratégica de las naciones que, en tanto Estados soberanos, conforman Europa.

En paralelo al plan ReArm Europe, la UE ha desplegado instrumentos financieros e industriales para respaldar la innovación tecnológica en defensa. Destaca, particularmente, el Fondo Europeo de Defensa (en adelante, FED), operativo desde 2021, que cuenta con un presupuesto de alrededor de 8000 millones de euros hasta 2027, dedicado a impulsar proyectos colaborativos de investigación y desarrollo militar (Fiott, 2023).

El FED representa la primera vez que la Unión, a través de su presupuesto comunitario, invierte directamente en capacidades de defensa, lo que la convierte ya en uno de los mayores financiadores de I+D en este ámbito a nivel europeo. De ese total, unos 2700 millones se orientan a la investigación innovadora —incluyendo tecnologías disruptivas como inteligencia artificial, microelectrónica, materiales avanzados, entre otras— y 5300 millones al desarrollo de prototipos y a la consolidación de capacidades industriales (Comisión Europea, 2021).

El FED persigue un doble objetivo: fomentar la cooperación entre empresas y Estados miembros en el desarrollo de nuevos sistemas de defensa —evitando la fragmentación de esfuerzos nacionales— y reforzar la Base

Industrial y Tecnológica de la Defensa Europea (BITDE), de modo que Europa pueda abastecerse con medios propios sin depender sistemáticamente de proveedores extracomunitarios.

Este último punto es especialmente crítico: análisis previos revelaban que más del 60 % del gasto en adquisiciones de defensa de los países de la UE entre 2007 y 2016 se dirigió a importaciones militares de fuera de la Unión, principalmente de Estados Unidos (Comisión Europea, 2022). La guerra en Ucrania volvió a poner en evidencia esta dependencia, ya que una proporción aún mayor de las compras urgentes de armamento realizadas en 2022-2023 se efectuaron a proveedores no europeos, especialmente en lo relativo a sistemas de armas y misiles de fabricación estadounidense. Las instituciones comunitarias han advertido que esta situación es insostenible si Europa aspira a una verdadera autonomía estratégica (Comisión Europea, 2022).

Por ello, además del FED, se han puesto en marcha medidas complementarias como el Instrumento Europeo para Compras Conjuntas de Defensa a Corto Plazo (EDIRPA) y propuestas en materia de regulación orientadas a incentivar la adquisición de productos europeos —como, por ejemplo, exenciones fiscales aplicables a proyectos colaborativos dentro del mercado común—.

Otro componente institucional relevante es la Estrategia Industrial de Defensa Europea, publicada en marzo de 2024. Se trata de la primera estrategia integral de la UE centrada en su industria de defensa y surge como respuesta directa a las lecciones de la guerra en Ucrania (Fiott, 2024). Esta Estrategia Industrial pone énfasis en la preparación militar y en el desarrollo de capacidades de nueva generación, muchas de las cuales descansan en tecnologías emergentes.

Entre sus líneas de acción, destacan: la consolidación de la demanda agregada europea —mediante compras conjuntas—, el impulso a la innovación en áreas como la inteligencia artificial, la computación cuántica o el espacio, y la garantía de que la base industrial pueda escalar su producción rápidamente en caso de crisis (Fiott, 2024).

Aunque la estrategia es un paso positivo que demuestra una visión a nivel europeo, expertos señalan que también plantea incógnitas sobre su implementación efectiva y la coordinación con los esfuerzos nacionales (Fiott, 2024). Aun así, refleja la prioridad creciente otorgada a la tecnología de defensa en la agenda europea.

De manera complementaria, la UE y sus Estados miembros han fortalecido la colaboración con la OTAN en materia de innovación, buscando sinergias y división de tareas —por ejemplo, la OTAN ha lanzado su acelerador de innovación en Defensa para el Atlántico Norte y un Fondo de Innovación, mientras la UE se concentra en proyectos industriales y regulación—.

En síntesis, Europa ha pasado, en pocos años, de una posición rezagada a una actitud decididamente proactiva frente a la revolución tecnológica en el ámbito de la defensa. Iniciativas como el plan ReArm Europe, la activación del Fondo Europeo de Defensa y el impulso de nuevas estrategias industriales reflejan una clara voluntad de modernizar tanto las capacidades militares como los sistemas de inteligencia mediante la incorporación de IA y otras tecnologías avanzadas.

Todo ello responde, además, a un objetivo estratégico fundamental: salvaguardar la soberanía tecnológica europea. No obstante, desde nuestra perspectiva, esta aspiración debe ir acompañada de un firme compromiso con el respeto al interés nacional de cada Estado soberano. La construcción de una autonomía tecnológica compartida no puede ni debe producirse a expensas de las soberanías nacionales, sino que ha de sustentarse en formas de cooperación que reconozcan y respeten las prioridades específicas de cada nación.

5 Casos de aplicación tecnológica en inteligencia y defensa

La concreción de esta transformación tecnológica se observa en diversos proyectos y casos prácticos donde la IA y otras innovaciones se aplican ya en el ámbito de la inteligencia de seguridad y defensa europeas. Uno de los ejemplos más directos es el proyecto Artificial Intelligence for Defence (en adelante, AI4DEF), financiado en 2020 bajo el programa europeo EDIDP —Programa Europeo de Desarrollo Industrial de Defensa, precursor del FED—. El AI4DEF es un proyecto multinacional orientado a demostrar los beneficios de la IA en varias funciones militares, sobre todo, en mejorar la conciencia situacional, el análisis de inteligencia, vigilancia y reconocimiento (ISR) y la optimización de la planificación operativa (Comisión Europea, 2021).

Concretamente, AI4DEF está desarrollando una plataforma en la nube que integra algoritmos de inteligencia artificial para, por ejemplo, analizar en tiempo real imágenes captadas por vehículos aéreos no tripulados (UAV) e identificar objetivos de interés. Este proyecto ilustra cómo la IA puede tener un enfoque integrado y adaptable en el ámbito de la defensa, aplicándose en los dominios terrestre, aéreo y marítimo a desafíos como la detección automatizada de amenazas móviles, la segmentación tridimensional del terreno para operaciones urbanas o la fusión inteligente de datos procedentes de sensores heterogéneos (Comisión Europea, 2021).

Otra aplicación tecnológica clave se da en el procesamiento avanzado de imágenes satelitales y de reconocimiento. La UE cuenta con el Centro Satelital de la Unión Europea (en adelante, SatCen), ubicado en España, que proporciona análisis geoespacial a los Estados miembros y misiones de la Política Común de Seguridad y Defensa. Ante el creciente volumen

de imágenes de observación terrestre disponibles —incluyendo las del programa Copernicus de la UE y proveedores comerciales—, SatCen y la Agencia Europea de Defensa han impulsado estudios para integrar IA en los procesos de Imagery Intelligence (IMINT), a fin de automatizar la identificación de objetos, el cambio detectado en infraestructuras y la vigilancia de fronteras. Por ejemplo, los algoritmos de visión por computador pueden analizar miles de imágenes satelitales en busca de patrones —como concentraciones inusuales de vehículos o indicios de preparación militar— con una velocidad y precisión muy superiores a las de un equipo humano, lo que permite centrar los esfuerzos analíticos únicamente en aquellas alertas con mayor probabilidad de relevancia. Este tipo de herramientas ha cobrado especial importancia en conflictos recientes como el de Ucrania, donde la inteligencia de fuente abierta (OSINT) y las imágenes satelitales comerciales han desempeñado un papel fundamental en la monitorización de movimientos militares. A partir de esta experiencia, las agencias europeas aspiran a dotarse de plataformas basadas en inteligencia artificial capaces de filtrar el ruido informativo y extraer conocimiento útil y accionable a partir del vasto volumen de datos abiertos disponibles.

Asimismo, países europeos han comenzado a aplicar IA en apoyo a la inteligencia contra el terrorismo y el crimen organizado. Un caso es el uso de algoritmos para analizar comunicaciones en Internet y redes sociales con el fin de detectar señales precoces de radicalización o planificación de ataques. Existen proyectos piloto, a menudo en colaboración con agencias de seguridad interior, que combinan procesamiento de lenguaje natural en múltiples idiomas con técnicas de análisis de redes sociales para identificar perfiles potencialmente peligrosos, siempre respetando las leyes de protección de datos. Aunque se trata de un ámbito sensible, el uso de inteligencia artificial en funciones predictivas podría permitir a las unidades europeas de inteligencia priorizar investigaciones y prevenir actos violentos a partir de indicios que, de otro modo, quedarían ocultos entre enormes volúmenes de datos. Organismos como Europol ya han explorado herramientas de este tipo para cribar contenidos extremistas en línea, y a nivel nacional varios servicios de inteligencia están invirtiendo en capacidades avanzadas de análisis masivo de datos (*big data*). Esta evolución tecnológica ilustra cómo las fronteras entre la seguridad interior y exterior tienden a desdibujarse, una dinámica reconocida por la Brújula Estratégica (Consejo de la UE, 2022) y que demanda una cooperación interagencias cada vez más estrecha.

En el ámbito de los ejércitos de las naciones europeas, la adopción de tecnologías 4RI también es palpable. La robotización y los sistemas no tripulados son cada vez más comunes en misiones de reconocimiento e inteligencia. Por ejemplo, varios países de la OTAN desplegados en la región del Sahel han empleado minidrones para vigilancia aérea táctica, reduciendo el

riesgo para el personal y obteniendo inteligencia en tiempo real sobre movimientos insurgentes. En entornos urbanos complejos, donde los GPS pueden fallar y abundan obstáculos, se investigan soluciones de IA para mejorar la navegación autónoma de drones: En 2018, Francia financió, a través del organismo CEA/LIST —especializado en IA—, varios proyectos orientados a resolver la localización tridimensional precisa de vehículos aéreos no tripulados (UAV) en entornos urbanos densamente edificados, mediante la combinación de visión artificial y aprendizaje profundo (Ministère des Armées, 2019).

Este tipo de desafíos técnicos —como detectar y esquivar obstáculos en calles estrechas o identificar figuras humanas ocultas entre edificios— está siendo abordado mediante algoritmos entrenados para interpretar imágenes de vídeo en tiempo real. Los avances obtenidos no solo fortalecen las capacidades de reconocimiento militar, sino que también presentan un notable potencial de aplicación dual, por ejemplo, en la gestión de desastres o en la seguridad civil.

Cabe destacar, además, el ambicioso proyecto franco-germano-español del Sistema de Combate Aéreo del Futuro (FCAS), concebido como un «sistema de sistemas» que integrará un caza tripulado de sexta generación con enjambres de drones de combate y una «nube de combate» (*combat cloud*) que conectará sensores y operadores en tiempo real. Aunque todavía en fase conceptual, el FCAS incorpora de forma explícita el uso de IA y tecnologías de computación en la nube para facilitar la fusión masiva de datos y la asignación dinámica de objetivos entre plataformas.

Este programa, liderado por Francia, ejemplifica cómo la visión europea de superioridad aérea hacia 2040 y más allá depende estrechamente del aprovechamiento de capacidades avanzadas de IA —para la gestión cooperativa de sistemas no tripulados, la guerra electrónica cognitiva, entre otros— y de garantizar la plena interoperabilidad de sistemas autónomos. Si el FCAS tiene éxito, dotará a Europa de una arquitectura de inteligencia y mando distribuido altamente sofisticada, reduciendo significativamente su dependencia operativa de activos estadounidenses en escenarios futuros.

En suma, los casos citados —AI4DEF, SatCen con IA, análisis big data antiterrorista, drones autónomos o FCAS— demuestran la amplitud de ámbitos en que la tecnología está cambiando el quehacer de la inteligencia y la defensa europeas. Desde el nivel táctico hasta el estratégico, la IA, la robótica y las herramientas digitales están amplificando el alcance y la rapidez con que Europa puede obtener y explotar información de valor militar.

No obstante, esta revolución tecnológica requiere de una visión política y estratégica que garantice su viabilidad, lo que enlaza con el concepto de soberanía tecnológica discutido a continuación.

6 La búsqueda de la soberanía tecnológica europea

El impulso europeo por incorporar IA y tecnologías emergentes en defensa está estrechamente vinculado con la aspiración de lograr una mayor soberanía tecnológica. Este concepto se refiere a la capacidad de Europa para decidir y actuar de forma autónoma en el terreno tecnológico, controlando las cadenas de suministro críticas y reduciendo dependencias excesivas de potencias externas en ámbitos estratégicos (Ministère des Armées, 2019). En los últimos años, «soberanía tecnológica» y «autonomía estratégica» se han convertido en ejes discursivos centrales en la UE, impulsados por desafíos como la rivalidad comercial y geopolítica entre EE. UU. y China, las disrupciones en suministros —por ejemplo, Semiconductores— y la citada dependencia europea en defensa de proveedores extracomunitarios.

En materia de seguridad y defensa, la soberanía tecnológica implica que Europa pueda desarrollar y producir sus propias tecnologías críticas —desde IA y ciberseguridad hasta satélites, plataformas militares avanzadas o redes 5G seguras— sin verse sometida a vetos o vulnerabilidades externas. Ursula von der Leyen ha defendido esta idea en su mandato al frente de la Comisión, alineándola con la visión de una «Comisión Geopolítica» capaz de dotar a la UE de las herramientas para ser un actor estratégico por derecho propio (Csernatoni, 2023). La búsqueda de soberanía tecnológica ha motivado iniciativas como la identificación de «proyectos importantes de interés común europeo» (IPCEI) en campos como la microelectrónica y la nube, el Acta Europea de Chips para fomentar la producción de semiconductores en Europa, o la ya mencionada movilización de inversiones en defensa para fortalecer la BITDE. En defensa, en concreto la Declaración de Versalles de marzo 2022 —firmada por los jefes de Estado y de Gobierno de la UE— explicitó la necesidad de reforzar la base industrial y tecnológica de defensa europea y corregir dependencias estratégicas, listando sectores clave donde Europa debe garantizar el control.

La IA se considera precisamente uno de esos sectores críticos. El Gobierno francés llegó a afirmar en su Revisión Estratégica de Defensa y Seguridad Nacional 2017 que la pericia en IA sería una cuestión de soberanía en el futuro (Ministère des Armées, 2019). En línea con ello, Francia y otros países han abogado por que la UE trate a la IA militar y a las tecnologías profundas —*deep tech*— como un dominio de inversión prioritaria, para no quedar rezagados frente a Estados Unidos o China.

El discurso de la soberanía tecnológica también permea la narrativa sobre datos e inteligencia: se insiste en que Europa debe poder almacenar, procesar y extraer valor de sus datos —incluidos los datos de inteligencia— en infraestructuras seguras europeas, evitando dependencias de servicios en la nube extranjeros que podrían suponer riesgos de acceso o interrupción. Este es un argumento a favor de iniciativas

como (GAIA-X) —infraestructura de datos abierta— o de reforzar las capacidades propias en cifrado cuántico y ciberseguridad.

No obstante, lograr la soberanía tecnológica no significa aislarse: la UE reconoce que cooperar internacionalmente sigue siendo importante. Por ejemplo, se busca un equilibrio en el que Europa pueda «caminar con sus propios pies» en tecnología de defensa, pero a la vez interoperar plenamente con aliados de la OTAN. Tampoco todos los países de la UE comparten el mismo énfasis en la autonomía; mientras Francia, tradicionalmente, empuja una visión de «Europe puissance» capaz de actuar de forma autónoma, otras naciones ven esta autonomía de manera complementaria —no sustitutiva— con la alianza transatlántica. En cualquier caso, el concepto de soberanía tecnológica ha servido para orientar políticas concretas: la UE ha condicionado la financiación del FED a la participación mayoritaria de industrias de países miembros —evitando control de empresas desde el exterior—; igualmente, se están mapeando vulnerabilidades en suministros —por ejemplo, Europa importa drones de reconocimiento de proveedores israelíes o estadounidenses, lo que ha motivado proyectos para fabricar drones europeos—. El discurso estratégico europeo ahora liga claramente la superioridad tecnológica a la independencia estratégica: quien controle las tecnologías críticas, controlará en buena medida su destino en seguridad y defensa.

Frente a esta apuesta, surgen algunas dificultades. Desarrollar tecnologías punteras requiere enormes inversiones, coordinación y atracción de talento, en un contexto donde Europa compite con ecosistemas de innovación más dinámicos como Silicon Valley o Shenzhen. De igual modo, imponer «Buy European» en defensa puede elevar costes o retrasar capacidades si la industria europea no produce cierto equipamiento al ritmo requerido —por ejemplo, drones armados, donde hasta hace poco no había alternativa europea consolidada—.

Por ello, la soberanía tecnológica se plantea como un objetivo a alcanzar de forma gradual, combinando la cooperación entre los Estados miembros de la UE —para ganar masa crítica— con una colaboración externa selectiva allí donde sea necesario. En este contexto, el papel de Francia ha sido crucial, como se desarrollará en la siguiente sección, ya que ha actuado como catalizador de la autonomía tecnológica europea, impulsando proyectos industriales comunes y dando ejemplo mediante políticas nacionales ambiciosas en IA y defensa.

7 Aspectos normativos en la transformación digital de la seguridad y defensa en Europa

La transformación digital de la seguridad y la defensa europeas requieren un marco jurídico estructurado que regulen tanto los desarrollos tecnológicos disruptivos como la protección de las infraestructuras estratégicas.

La UE ha desplegado en los últimos años una serie de instrumentos normativos que buscan establecer un entorno regulado, coherente y seguro para la digitalización de servicios esenciales, incluidos aquellos con implicaciones en materia de inteligencia y soberanía tecnológica.

Uno de los desarrollos más relevantes es la Directiva (UE) 2022/2555[1], conocida como NIS 2.0, que sustituye y amplía la Directiva NIS original (2016/1148/UE). Este nuevo marco normativo establece requisitos más exigentes para entidades de sectores clave —entre ellos, el transporte, la energía, la Administración Pública y determinadas infraestructuras digitales—, e introduce obligaciones en materia de gestión de riesgos y notificación de incidentes. Aunque las actividades estrictamente relacionadas con la defensa nacional quedan excluidas de su ámbito de aplicación (art. 2.3), la directiva afecta indirectamente a operadores estratégicos que pueden colaborar con el sector de defensa o manejar información sensible.

Entre las novedades más significativas figura la creación de la Red Europea de Organizaciones de Enlace para Crisis Cibernéticas (EU-CyCLONe), prevista en su artículo 16, que facilita la coordinación operativa entre Estados miembros en caso de incidentes graves de ciberseguridad con posibles efectos transfronterizos. La aplicación efectiva de esta directiva depende de su transposición por parte de los Estados miembros. En el caso de España, esta adecuación encuentra una base ya avanzada en el Real Decreto 311/2022, que reforma el Esquema Nacional de Seguridad[2] (ENS) y anticipa principios de protección activa, supervisión continua y respuesta ante amenazas, en línea con los estándares comunitarios.

En paralelo, la UE ha formulado un enfoque jurídico integral para la regulación de la IA, mediante la Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial, conocido como Artificial Intelligence Act[3]. Este reglamento, aún en tramitación parlamentaria, introduce una clasificación basada en el nivel de riesgo del sistema de IA, estableciendo restricciones proporcionales según su impacto potencial en el marco del ejercicio de derechos fundamentales, seguridad pública o integridad institucional.

Los sistemas de inteligencia artificial clasificados como de alto riesgo —como los empleados en infraestructuras críticas, vigilancia biométrica o administración de justicia— deberán cumplir estrictas obligaciones en

[1] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para garantizar un elevado nivel común de ciberseguridad en toda la Unión (DOUE L 333/80, 27.12.2022).
[2] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. BOE n.º 106, de 4 de mayo de 2022.
[3] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (COM/2021/206 final).

cuanto a la calidad de los datos, la documentación técnica, la supervisión humana y la trazabilidad. Si bien el reglamento excluye formalmente de su ámbito de aplicación los usos militares y de defensa (art. 2.3), su impacto es significativo en contextos de doble uso o cooperación civil-militar, en especial, en relación con sistemas utilizados por autoridades públicas o contratistas que operan en entornos sensibles.

El reglamento prevé, asimismo, la creación de una Oficina Europea de inteligencia artificial, concebida como un órgano de supervisión y coordinación responsable de garantizar la correcta aplicación de la norma en todo el territorio de la Unión. Este organismo se configura como un elemento clave para asegurar el desarrollo ético y controlado de las tecnologías automatizadas, incluidas aquellas que pueden incidir directamente en funciones estatales esenciales.

En conjunto, el marco normativo europeo refleja una arquitectura legal orientada a garantizar un entorno digital controlado, conforme a estándares técnicos elevados y principios fundamentales del Derecho europeo. La interacción entre normativas como la NIS 2.0, el futuro Reglamento de IA y las propuestas sectoriales en materia digital, constituye un eje esencial para la evolución estratégica de las capacidades de inteligencia y defensa en la era tecnológica.

8 Escenarios prospectivos hacia 2040: el futuro de la inteligencia digital europea

Mirando hacia 2040, pueden vislumbrarse varios escenarios posibles para la inteligencia y la seguridad europea en función de cómo se gestionen las oportunidades y los riesgos actuales. A continuación, se plantean tres escenarios prospectivos que ilustran futuros plausibles del rol de la inteligencia digital en Europa, considerando variables tecnológicas, geopolíticas y normativas.

8.1 Escenario primero: autonomía e inteligencia europea integrada

En este futuro, la UE logra materializar con éxito sus planes de transformación. Para 2040, Europa dispone de una infraestructura digital de defensa plenamente interoperable y soberana: satélites europeos de próxima generación proporcionan vigilancia ubicua; redes seguras europeas de 5G/6G conectan sensores y centros de mando en tiempo real; y los Estados miembros comparten inteligencia a través de una plataforma común, robusta y protegida, evolución de la actual SIAC.

Este avance ha sido posible gracias a un enfoque que respeta y contempla la soberanía de las naciones. Los Gobiernos han sabido construir un futuro en el que los intereses nacionales no se diluyen, sino que convergen

y se refuerzan mutuamente en el marco de una cooperación voluntaria. Lejos de suponer una cesión de soberanía, la colaboración europea se ha convertido en una herramienta para fortalecer las capacidades nacionales y proyectarlas con mayor eficacia en un entorno internacional complejo.

La IA, desarrollada conforme a estos principios éticos, se emplea rutinariamente para anticipar crisis, detectar campañas de desinformación hostil y coordinar despliegues multinacionales. La UE ha establecido un Centro de Inteligencia Europeo permanente, donde analistas de todos los países trabajan juntos con acceso a bases de datos comunes, respetando los niveles de clasificación.

Gracias a la inversión sostenida en I+D, Europa ha mitigado sus dependencias estratégicas, produciendo localmente chips y sensores críticos, compitiendo en condiciones de igualdad con EE. UU. y Asia en áreas como ciberseguridad, robótica e IA militar (Csernatoni, 2023).

Desde el punto de vista político, la UE gana peso normativo y logra que su enfoque de «IA fiable» sea adoptado a nivel mundial en el ámbito armamentístico, contribuyendo así a evitar una carrera descontrolada hacia el desarrollo de armas autónomas. En este escenario, la inteligencia digital europea actúa como un multiplicador de seguridad: anticipa amenazas híbridas, facilita respuestas rápidas ante crisis y respalda la autonomía estratégica europea en la toma de decisiones internacionales.

Las iniciativas actuales, como la Brújula Estratégica y PESCO, se implementan con éxito, fortaleciendo la solidaridad entre los Estados miembros frente a amenazas externas y consolidando a la UE como un actor clave en la seguridad internacional.

8.2 Escenario segundo: dependencia persistente

En este escenario, los esfuerzos de integración en materia de defensa avanzan de forma limitada, en parte porque varios Estados miembros optan por reafirmar su soberanía en el ámbito de la seguridad y la defensa. Tras la crisis en Ucrania, se impone una lógica de acción nacional, en la que cada país fortalece sus capacidades con arreglo a sus propias evaluaciones estratégicas, estableciendo alianzas bilaterales y contratando directamente con proveedores internacionales según sus necesidades particulares.

Para 2040, la inteligencia europea permanece estructurada principalmente en torno a capacidades nacionales y la UE no ha conseguido consolidar un núcleo operativo común. La SIAC mantiene una función simbólica y de coordinación básica, pero no evoluciona hacia una plataforma plenamente integrada. Esta configuración permite a los Estados conservar el control sobre su información sensible, aunque dificulta respuestas colectivas rápidas ante crisis compartidas (Csernatoni, 2023).

En el plano tecnológico, Europa ha avanzado de manera prudente en el desarrollo de inteligencia artificial aplicada al ámbito militar, en parte debido a un enfoque excesivamente cauteloso en materia ética, lo que le resta competitividad frente a potencias como China, que se perfila para alcanzar la supremacía en IA militar hacia 2035 (Csernatoni, 2023).

Esta situación ha reforzado la dependencia estratégica respecto a Estados Unidos, limitando la capacidad de Europa para ejecutar operaciones complejas de forma plenamente autónoma. Como consecuencia, su margen de maniobra diplomática se ve reducido y ciertas vulnerabilidades persisten frente a actores internacionales con agendas más asertivas (Csernatoni, 2021).

8.3 Escenario tercero: cooperación condicionada

Este escenario, el más probable, sitúa a Europa en una posición intermedia. Para 2040, la UE ha alcanzado avances notables en integración tecnológica y de inteligencia, aunque persisten ciertas limitaciones estructurales. La seguridad común se sostiene mediante mecanismos como la Brújula Estratégica, renovada cada cinco años, si bien Europa continúa dependiendo parcialmente de importaciones en tecnologías críticas.

El desarrollo de la IA en Europa avanza principalmente en aplicaciones defensivas, evitando una carrera incontrolada hacia el armamento autónomo. Este enfoque es posible gracias a acuerdos internacionales promovidos por la propia UE, que han logrado establecer una regulación estricta sobre estas tecnologías (Calderón y Pedemonte, 2023).

La cooperación transatlántica se mantiene sólida, aunque adaptada a un nuevo equilibrio: EE. UU. sigue aportando inteligencia estratégica a escala mundial, mientras Europa contribuye con estabilidad regional y capacidades especializadas en inteligencia local. La OTAN, por su parte, incorpora estándares éticos europeos en el desarrollo de IA, lo que refuerza la confianza operativa entre aliados (Calderón y Pedemonte, 2023).

En el ámbito industrial, aunque EE. UU. conserva la supremacía en sectores clave, empresas europeas lideran nichos estratégicos como la ciberseguridad o los drones inteligentes no letales. En este contexto de competencia contenida, la UE ejerce una influencia significativa en la regulación internacional de la IA, contribuyendo a prevenir conflictos accidentales derivados de algoritmos no supervisados.

Europa, en definitiva, será más fuerte que en 2025, aunque seguirá manteniendo ciertas dependencias selectivas. Su inteligencia digital habrá alcanzado un nivel de eficacia considerable, si bien aún requerirá del respaldo de aliados para consolidar una soberanía plena.

Estos escenarios —aproximaciones analíticas— ponen de relieve que el futuro de la inteligencia europea dependerá en gran medida de las decisiones que se adopten hoy. La forma en que los Estados miembros equilibren cooperación y autonomía, inversión conjunta y prioridades nacionales, será decisiva para definir la dirección de ese futuro.

La variable determinante será la voluntad política de los Estados para sostener la inversión, preservar sus principios y articular formas de cooperación que sean compatibles con sus intereses nacionales. La inteligencia digital podrá convertirse en un factor de fortalecimiento o de exposición en materia de seguridad, según cómo se gestione. Por ello, imaginar estos futuros no es un ejercicio meramente especulativo, sino una herramienta estratégica para el presente: Europa no debe resignarse a que otros definan su destino, sino asumir con determinación la responsabilidad de construirlo desde la soberanía de sus naciones.

9 Conclusiones

La transformación de la inteligencia en la seguridad y defensa europea en la era digital es un proceso complejo y dinámico que responde directamente a los desafíos impuestos por la Cuarta Revolución Industrial y a la creciente sofisticación de amenazas híbridas y convencionales. La adopción generalizada de la IA, el *big data* y los sistemas autónomos está redefiniendo las capacidades y procedimientos operativos de las fuerzas armadas y agencias de inteligencia europeas, brindando oportunidades excepcionales para mejorar significativamente la eficacia, velocidad de reacción y precisión en operaciones.

Tanto la UE como sus naciones soberanas han identificado claramente estos beneficios potenciales, pero también reconocen plenamente los desafíos tecnológicos, éticos y políticos involucrados. Esto se ha traducido en la implementación de múltiples iniciativas estratégicas y programas de inversión, entre los que destacan la Brújula Estratégica, la Estrategia Industrial de Defensa, el Fondo Europeo de Defensa y proyectos clave como ReArm Europe, Eurodrone y el Sistema de Combate Aéreo Futuro (FCAS). Estos esfuerzos buscan consolidar la autonomía estratégica europea, reduciendo su dependencia tecnológica y operativa de países terceros, especialmente en áreas críticas como IA, ciberdefensa, tecnologías satelitales y vehículos no tripulados.

No obstante, Europa continúa enfrentando desafíos decisivos. Las diferencias entre naciones soberanas —resultado de trayectorias históricas, estructuras estratégicas y prioridades nacionales legítimas— constituyen una realidad estructural que influye directamente en la manera en que se articula la cooperación en materia de seguridad y defensa. Lejos de ser

un impedimento, puede convertirse en un factor de solidez si se gestiona desde el respeto mutuo y la voluntad de colaboración. No se trata de imponer uniformidad, sino de fomentar la cooperación desde el respeto a la soberanía nacional.

Hoy en día, la UE aún no ha logrado articular una doctrina clara y coherente sobre el uso militar de tecnologías emergentes como la inteligencia artificial, lo que amenaza con generar estrategias dispersas, ineficaces y condicionadas por lógicas burocráticas alejadas de las realidades nacionales. En un entorno tecnológico que evoluciona con rapidez, se impone la necesidad de una respuesta ágil y coordinada entre Estados soberanos, guiada por el interés nacional y no por agendas ajenas, para garantizar la defensa y la seguridad desde una auténtica Europa de las naciones.

Asimismo, será fundamental gestionar adecuadamente las relaciones estratégicas con aliados clave como Estados Unidos. La autonomía estratégica que Europa persigue no debe interpretarse como un distanciamiento, sino como una búsqueda de equilibrio, fortaleciendo capacidades propias que complementen las de la OTAN. Este enfoque implica un diálogo constante, una cooperación estrecha y reforzar la influencia europea en la regulación ética y el marco normativo internacional sobre el uso de la IA militar.

Europa dispone de activos fundamentales para afrontar estos retos con solidez: cuenta con talento científico de primer nivel, empresas tecnológicas competitivas, un mercado común consolidado y una tradición significativa de cooperación en materia de seguridad y defensa. El compromiso político y la implicación activa de países como Francia, Alemania, Italia y España constituyen una base firme para seguir impulsando esta transformación, a partir de capacidades nacionales que, al sumarse de forma voluntaria y coordinada, fortalecen el conjunto.

De cara a 2040, la inteligencia digital podría adquirir una relevancia estratégica equiparable al papel desempeñado por las armas nucleares en el siglo xx, redefiniendo equilibrios de poder y estrategias mundiales. Europa aspira a que esta inteligencia digital sirva como herramienta efectiva para salvaguardar la paz, promover valores democráticos y evitar convertirse en un instrumento de control totalitario o conflicto descontrolado. Para ello, será crucial mantener un enfoque centrado en las personas, asegurando mecanismos de control democrático y transparencia, en la mayor medida posible sin comprometer las necesidades legítimas de seguridad.

En definitiva, esta transformación —enmarcada en la era digital— constituye una oportunidad excepcional para fortalecer tanto la seguridad colectiva como la autonomía estratégica de las naciones soberanas europeas. Si bien persisten desafíos considerables, los avances alcanzados

evidencian una Europa en constante evolución, donde la cooperación se construye sobre la base del respeto a la soberanía nacional. Si se mantiene la voluntad política, se garantizan inversiones sostenidas en investigación y desarrollo y se consolida una visión común sobre el uso responsable de la tecnología, Europa estará en condiciones de llegar a 2040 con capacidades de inteligencia significativamente reforzadas, preparada para proteger de forma eficaz a sus ciudadanos, así como sus principios y valores, en un entorno internacional cada vez más dinámico e incierto.

Referencias bibliográficas

Ash Center. (2024). *AI, Digital Sovereignty, and the EU's Path Forward: A Case for Mission-Oriented Industrial Policy*. Harvard Kennedy School. [Consulta: 2025]. Disponible en: https://ash.harvard.edu/resources/ai-digital-sovereignty-and-the-eus-path-forward-a-case-for-mission-oriented-industrial-policy/

Calderón, I. y Pedemonte, C. (2023). NATO's AI strategy focuses on responsible use: AI chief. *NATO News*. [Consulta: 2025].

Comisión Europea. (2021). EDIDP 2020 – Artificial Intelligence: Project AI4DEF (Factsheet). Bruselas, DG DEFIS. [Consulta: 2025]. Disponible en: https://defence-industry-space.ec.europa.eu/system/files/2021-06/EDIDP2020_factsheet_AI_AI4DEF.pdfDefence Industry and Space

Comisión Europea. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (COM/2021/206 final). [Consulta: 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

Comisión Europea. (2022). *Joint Communication to the European Parliament and the Council on Defence Investment Gaps Analysis and Way Forward* [JOIN (2022) 24 final, 18 de mayo de 2022]. [Consulta: 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022JC0024EUR-Lex+1EUR-Lex+1

Comisión Europea. (2025). *White Paper on European Defence – Readiness 2030 (ReArm Europe Plan)*. Bruselas, Comisión Europea. [Consulta: 2025]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793European Commission+1European Commission+1

Consejo de la Unión Europea. (2022). Brújula Estratégica para la Seguridad y la Defensa. Bruselas, Consejo de la Unión Europea. [Consulta: 2025]. Disponible en: https://www.consilium.europa.eu/es/policies/strategic-compass/Consilium

Consejo Europeo. (2022). *Declaración de Versalles, 10-11 de marzo de 2022*. Bruselas, Consejo Europeo. [Consulta: 2025]. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2022/03/11/the-versailles-declaration-10-11032022/Consilium

Csernatoni, R. (2021). *Security 2040: Perils and Promise Over the Near Horizon*. Carnegie Europe. [Consulta: 2025]. Disponible en: https://carnegieeurope.eu/2021/03/25/security-2040-perils-and-promise-over-near-horizon-pub-84124

Csernatoni, R. (2023). Weaponizing Innovation? Mapping Artificial Intelligence-enabled Security and Defence in the EU. *Non-proliferation and Disarmament Papers*. Estocolmo, SIPRI. 84. [Consulta: 2025]. Disponible en: https://www.sipri.org/publications/2023/eu-non-proliferation-and-disarmament-papers/weaponizing-innovation-mapping-artificial-intelligence-enabled-security-and-defence-euSIPRI

Finabel. (s.f.). A Shift Towards Sovereign EU Military Capabilities? The Eurodrone Project Awaits Final Signature. The European Land Force Commanders Organisation. [Consulta: 2025]. Disponible en: https://finabel.org/a-shift-towards-sovereign-eu-military-capabilities-the-eurodrone-project-awaits-final-signature/finabel.org

Fiott, D. (2021). The European Front-Runners: France, Germany, Italy and Spain in PESCO. *European Foreign Affairs Review*. 26, pp. 87-110.

Fiott, D. (2023). *Investing and Innovating? Spain and the European Defence Fund*. Real Instituto Elcano. [Consulta: 2025]. Disponible en: https://www.realinstitutoelcano.org/en/analyses/investing-and-innovating-spain-and-the-european-defence-fund/Real Instituto Elcano

Fiott, D. (2024). *¿Más allá de la estrategia? Estrategia industrial y futuro de la defensa europea*. Real Instituto Elcano. [Consulta: 2025]. Disponible en: https://www.realinstitutoelcano.org/analisis/mas-alla-de-la-estrategia-estrategia-industrial-y-futuro-de-la-defensa-europea/ Real Instituto Elcano

Fiott, D. y Lindstrom, G. (2018). *Artificial Intelligence: What Implications for EU Security and Defence?* París, Instituto de Estudios de Seguridad de la UE. 18. [Consulta: 2025]. Disponible en: https://www.iss.europa.eu/publications/briefs/artificial-intelligence-what-implications-eu-security-and-defenceiss.europa.eu

Fojón, E. (2018). La cuarta revolución industrial, el «algoritmo de guerra» y su posible aplicación a la Defensa española. Real Instituto Elcano [en línea]. [Consulta: 2025]. Disponible en: https://www.realinstitutoelcano.org/analisis/la-cuarta-revolucion-industrial-el-algoritmo-de-guerra-y-su-posible-aplicacion-a-la-defensa-espanola/

Global X. (2023). *Rearming Europe Boosts Defense Tech*. [Consulta: 2025].

Gobierno de España. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*. 4 de mayo, núm. 106.

Ministère des Armées (Francia). (2019). *L'intelligence artificielle au service de la défense – Rapport de la Task Force IA*. París, Ministerio de las Fuerzas Armadas.

Ministerio para Europa y Asuntos Exteriores. (2022). *A Strategic Compass to Strengthen the Security and Defence of the European Union by 2030*. [Consulta: 2025].

OpenAI. (2024). *ChatGPT (modelo GPT-4)* [El texto ha sido revisado con apoyo de herramientas basadas en inteligencia artificial para mejorar la claridad y coherencia]. [Consulta: 2025]. Disponible en: https://chat.openai.com/

Parlamento Europeo. (2020). *Report on Artificial Intelligence in a Digital Age – Civil and Military* [2020/2266 (INI), 19 de abril de 2021]. Bruselas.

PESCO. (s.f.). *Joint EU Intelligence School (JEIS)*. [Consulta: 2025].

Politico. (2023). Brussels Rebrands "Rearm Europe" After Backlash from Italy and Spain. *Politico*. [Consulta: 2025].

SpringerLink. (2023). *Waking Up Slowly: Defense AI in Spain*. [Consulta: 2025].

Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para garantizar un elevado nivel común de ciberseguridad en toda la Unión. *Diario Oficial de la Unión Europea*.27 de diciembre, L 333/80.

Conductual explorer: una solución autónoma frente al desafío del entorno cognitivo

Pablo Caneda González
María Porrar Santisteban
Álvaro Álvarez Álvarez

Resumen

En el tiempo de hiperconectividad en el que vivimos, los medios por los cuales las personas se comunican son, principalmente, digitales y accesibles por cualquier usuario de la red. Esto pone a nuestro alcance un sinfín de opiniones y publicaciones subjetivas al alcance de la pantalla de nuestro dispositivo. En el ámbito cognitivo relativo a la influencia y la inteligencia, supone un reto el aprovechamiento de este flujo de información, ya que no son cantidades de datos procesables por uno o varios recursos humanos en un espacio de tiempo razonable.

A tal efecto, surge la iniciativa, dentro del ámbito de las FAS y, más concretamente, en el área de la influencia e inteligencia de nivel operacional, de desarrollar de manera autónoma, sin apoyo de agentes externos y con recursos limitados, una solución tecnológica a la que se ha bautizado como Conductual Explorer, que permita manejar vastas cantidades de datos obtenidas de medios de en formato digital o redes sociales de un entorno geográfico o social delimitado.

El análisis y almacenamiento de toda esta información, permite hacer un seguimiento del entorno informativo objetivo a lo largo del tiempo, pudiendo detectar tendencias y narrativas y su evolución en los periodos temporales deseados. El procesamiento de esta información será de gran utilidad en el apoyo a la toma de decisiones al nivel al que nos desempeñamos.

Palabras clave

Redes sociales, Fuentes abiertas, Influencia, Inteligencia, Inteligencia artificial.

Behavioral explorer: an autonomous solution to the challenge of the cognitive environment

Abstract

In today's era of hyperconnectivity, digital communication channels are widely accessible to any internet user, exposing individuals to an overwhelming volume of subjective opinions and publications, instantly available at the touch of a screen. In the cognitive domain of influence and intelligence, leveraging this vast flow of information presents a significant challenge, as the sheer volume of data surpasses the processing capacity of human analysts within a reasonable timeframe.

To address this challenge, within the framework of the Armed Forces —specifically in the field of operational-level influence and intelligence— a fully autonomous technological solution has been developed without external support and with limited resources. This solution, known as Conductual Explorer, facilitates the processing of vast amounts of data obtained from digital and social media within a specified geographical or social context.

By analyzing and storing this information, the system enables continuous monitoring of the targeted informational landscape over time, allowing for the identification of emerging trends, narratives, and their evolution across selected timeframes. The insights derived from this process provide valuable decision-making support at the operational level.

Keywords

Social media, Open sources, Influence, Intelligence, artificial intelligence.

1 Introducción

«Al tomar posesión de su dignidad, César fue el primero que estableció que se llevaría un diario de todos los actos del senado y del pueblo, y que este diario se haría público».

Según cuenta Suetonio, en el año 59 a. C., Julio Cesar da la orden de publicar las actas diurnas (Acta diurna populi Romani), expuestas de forma periódica en lugares públicos, tenían la finalidad de proporcionar a la ciudadanía romana un canal de información más preciso que los chismes y cotilleos que viajaban de boca en boca por las intrincadas redes de la compleja vida social romana.

Consideradas por muchos como el primer medio de comunicación escrito y, por otros, como la primera publicación oficial a modo de primigenio boletín oficial del Estado, pronto se consolidaron como una herramienta para influir en la opinión pública. Como afirma el emperador Augusto, sucesor de César, es innegable su utilidad como herramienta de propaganda al servicio del Estado.

Desde entonces, la relevancia de la capacidad de influir en audiencias ha crecido paralelamente a la complejidad y tamaño de las organizaciones humanas y de forma más acusada en la actualidad, con la irrupción de nuevas tecnologías.

Hoy en día, los medios de comunicación tradicionales se integran con nuevas formas de difusión de información, nuevas aplicaciones y redes sociales permiten a millones de usuarios participar en la generación y difusión de contenidos de forma descentralizada. Esta ingente producción unida a la hiperconectividad generada en entornos digitales, es capaz de producir o modificar rápidamente corrientes de opinión que deben ser tenidas muy en cuenta en el estudio de la nueva meta-geopolítica.

En el actual contexto de conflictos híbridos, la «zona gris» se ha consolidado como un espacio de disputa estratégica donde las narrativas, la desinformación y la manipulación de la opinión pública desempeñan un papel crucial. La proliferación de plataformas digitales ha transformado el entorno informativo en un campo de batalla no convencional, en el que actores estatales y no estatales emplean tácticas de guerra cognitiva para influir en la percepción de la realidad. En este escenario, la capacidad para analizar el sentimiento en redes sociales (RRSS) y medios de comunicación (MMCC), así como clasificar grandes volúmenes de datos de manera eficiente, se convierte en un recurso clave para la defensa y la seguridad nacional.

Según nuestra doctrina, la inteligencia engloba una serie de actividades que permiten obtener una visión integral y actualizada del entorno donde

se desarrollan las operaciones, la necesidad de obtener una visión integral del multidominio, obliga a contemplar dentro de las capacidades de inteligencia herramientas de análisis de nuevos ámbitos como, por ejemplo, el pujante dominio cognitivo.

El estudio y conocimiento de las condiciones socioculturales de determinado entorno permitirá encontrar indicadores en el dominio cognitivo que servirán de alerta ante posibles crisis o amenazas a la seguridad.

La inteligencia militar, en posesión de su dignidad, debe innovar y adaptarse a un nuevo contexto, como ya hiciera Julio Cesar al establecer las actas diurnas en la antigua Roma.

En el ámbito de la defensa, son ampliamente conocidas las enormes posibilidades de la observación en fuentes abiertas, que nos puede permitir obtener con rapidez la información necesaria para producir inteligencia básica sobre cualquier parte del mundo y puede servir de apoyo en la comprensión profunda del entorno operativo, así como para detectar tendencias y corrientes de pensamiento en una parte o un todo de una sociedad.

La actualización de nuevas capacidades lleva aparejados algunos desafíos. El gran volumen de información que se debe manejar supone un desafío para los analistas, la necesidad de filtrar información incorrecta, desinformación intencionada o tendenciosa requiere personal experimentado y con un adiestramiento específico, lo que se traduce en muchos recursos humanos y de tiempo.

Para paliar estos inconvenientes, se convierte en necesaria una estrecha colaboración entre el analista, conocedor del producto necesario para determinar tendencias y corrientes en un entorno social y el experto en tratamiento de datos, conocedor de técnicas que permiten obtener, almacenar y procesar grandes cantidades de datos.

Durante el desarrollo de Conductual Explorer se han tenido en cuenta tanto aspectos técnicos como necesidades y puntos de vista del analista, tratando de adaptar al máximo el potencial de la herramienta a las necesidades de análisis.

1.1 Motivación: resolver necesidades internas con creatividad y bajo coste

En el caso concreto que se va a desarrollar en este artículo, para hacer frente a este desafío de procesar grandes cantidades de información de fuentes abiertas, surge la necesidad de desarrollar herramientas que permitan interpretar la dinámica del entorno informacional de manera sistemática y eficiente. Los métodos tradicionales de análisis presentan limitaciones en términos de escalabilidad y rapidez, lo que dificulta la obtención de

inteligencia procesable en tiempo real. La solución que aquí se presenta responde a esta problemática mediante un enfoque innovador y de bajo coste, basado en la automatización y el uso de inteligencia artificial para la extracción y clasificación de datos y para la extracción de estadísticas y métricas ilustrativas del análisis del entorno informativo que se está realizando.

Este código, desarrollado íntegramente en lenguaje de programación Python, se ha desarrollado con el enfoque de ser una herramienta OSINT (Open-Source Intelligence). Ha sido diseñado para facilitar la labor de analistas e investigadores en el ámbito de la seguridad y la defensa. Su propósito es ofrecer una alternativa accesible y adaptable a los requerimientos específicos de diferentes contextos operativos, sin depender de infraestructuras costosas o soluciones comerciales privativas. Al combinar técnicas avanzadas de procesamiento del lenguaje natural (PLN), modelos de inteligencia artificial de *machine learning* y *deep learning*, así como técnicas de programación tradicional, la herramienta permite no solo analizar el sentimiento predominante en el entorno digital, sino también estructurar y categorizar grandes volúmenes de información provenientes de RRSS y MMCC con un alto grado de precisión y exponer los resultados de una manera fácilmente comprensible. Al mismo tiempo, es un ejemplo de aplicación de tecnologías programáticas avanzadas como solución a un problema concreto, empleando el recurso técnico adecuado para resolver cada arista del problema. Esto último pone en valor la idea de que las soluciones programáticas son un medio y no un fin y que no siempre la solución más moderna es la más adecuada para afrontar un problema.

1.2 Contexto del proyecto y su relevancia

El uso de información digital en escenarios de zona gris ha demostrado ser un factor determinante en la configuración de estrategias militares, diplomáticas y de seguridad. El conflicto en zona gris se caracteriza por la ausencia de confrontación directa, siendo el dominio de la información un elemento central en la lucha por la influencia y la legitimidad. En este contexto, la capacidad de anticipar tendencias, detectar patrones de desinformación y analizar discursos en tiempo real permite a los actores gubernamentales y privados tomar decisiones fundamentadas y estratégicas.

Este proyecto nace de la necesidad de contar con una herramienta flexible y eficiente que permita a los analistas gestionar el creciente volumen de datos en el ciberespacio. Su implementación ofrece ventajas en la detección temprana de amenazas, el monitoreo de campañas de influencia y la evaluación del impacto de narrativas en distintos públicos objetivos. Además, su carácter modular permite su integración con otras herramientas OSINT, optimizando así el proceso de obtención de inteligencia en entornos de alta volatilidad y riesgo.

Con esta iniciativa, se busca fortalecer la capacidad analítica en el ámbito de la seguridad, proporcionando una solución efectiva y accesible para el estudio del entorno informativo digital en zonas de conflicto.

1.3 Objetivos y alcance del programa

El principal objetivo de este programa es proporcionar una herramienta OSINT capaz de recopilar, analizar y clasificar datos provenientes de RRSS y MMCC en zonas de conflicto o que sean de interés, con el fin de optimizar la toma de decisiones estratégicas en materia de seguridad y defensa. Para ello, la herramienta se basa en técnicas de PLN, permitiendo una evaluación automatizada del sentimiento predominante en el entorno digital y una segmentación eficiente de los datos según criterios específicos.

Objetivos específicos

- Automatización del análisis de sentimiento: implementar modelos de PLN para identificar y categorizar emociones y tendencias en el discurso digital.
- Clasificación avanzada de datos: desarrollar modelos de inteligencia artificial que permitan segmentar información de RRSS y MMCC en función de su relevancia y confiabilidad.
- Presentar los resultados de una manera comprensible, con estadísticas y métricas que permitan entender de manera sencilla los resultados del análisis y extraer conclusiones.
- Monitoreo en tiempo real: diseñar una estructura de actualización continua para detectar cambios en la narrativa digital y evaluar su impacto.
- Adaptabilidad y escalabilidad: crear un sistema modular que pueda ajustarse a distintos entornos operativos y requerimientos específicos.
- Integración con otras herramientas OSINT: facilitar la interoperabilidad con bases de datos y sistemas de análisis ya existentes para maximizar la eficiencia operativa.

Alcance del programa

El programa se ha diseñado con un enfoque flexible y modular, lo que permite su implementación en distintos escenarios y niveles de operación. Está orientado tanto a entidades gubernamentales como a organizaciones privadas interesadas en el monitoreo de la información digital en contextos de crisis o conflicto.

El sistema podrá ser utilizado para:

- Análisis de desinformación y propaganda: identificar campañas de influencia y estrategias de manipulación informativa en plataformas digitales.
- Evaluación del impacto de narrativas: determinar cómo ciertos discursos afectan la percepción pública y el comportamiento de la audiencia.
- Apoyo en la toma de decisiones estratégicas: proporcionar datos estructurados y análisis predictivos para mejorar la respuesta a amenazas emergentes.
- Seguimiento de dinámicas de conflicto: monitorear el desarrollo de crisis en tiempo real mediante el análisis de contenido digital.

Este enfoque integral busca dotar a los analistas de inteligencia de una herramienta que no solo simplifique la gestión de grandes volúmenes de información, sino que también proporciona capacidades avanzadas de análisis predictivo y estratégico para la comprensión del entorno informativo deseado.

2 Necesidad de un analista y creación de la base de datos

El uso de herramientas de inteligencia de fuentes abiertas (OSINT) ha adquirido una relevancia creciente en el ámbito del análisis de datos, proporcionando un apoyo significativo al analista, sin sustituir la labor esencial del factor humano. Si bien la automatización permite procesar grandes volúmenes de información con rapidez y eficiencia, la interpretación contextual y la definición de criterios de búsqueda siguen requiriendo la intervención humana para garantizar la precisión y fiabilidad de los datos recopilados.

Antes de la implementación de una herramienta OSINT, es necesario establecer un marco metodológico que garantice la calidad del análisis. La fase inicial implica delimitar el entorno informativo, definir el objetivo de búsqueda y estructurar la información a explotar en una base de datos robusta. La ausencia de alguno o varios de estos pasos previos incrementa el margen de error y puede derivar en la generación de resultados incompletos o imprecisos.

En este capítulo, se detallan los procedimientos esenciales para la recopilación y estructuración de datos, destacando la importancia del analista en la construcción de una base de datos que facilite el procesamiento de información y la obtención de resultados válidos. Además, se aportan ejemplos con casos concretos para cada etapa del procedimiento.

2.1 Análisis de la Zona: recopilación y estructuración de datos

La delimitación del entorno de información constituye el primer paso en el análisis OSINT, debiendo establecerse criterios claros para la recopilación de datos. Esta fase comprende la identificación de parámetros espaciales y temporales, la selección de fuentes y audiencias relevantes y la identificación de actores clave dentro del ecosistema digital objetivo.

La metodología de recopilación de datos se organiza en tres etapas fundamentales:

2.1.1 Definición del ámbito de estudio

La delimitación del análisis debe atender a una serie de factores clave que garantizan la precisión y relevancia de la información recopilada. En primer lugar, resulta fundamental establecer los parámetros espaciales y temporales, definiendo con claridad el objeto de estudio y el periodo de observación, lo que permite contextualizar de manera adecuada los datos obtenidos.

Asimismo, es necesario determinar el sector de interés, identificando el ámbito temático sobre el cual se desarrollará el análisis. Este puede situarse en dimensiones políticas, sociales, económicas o de seguridad, dependiendo del objetivo de la investigación.

Por último, la selección de plataformas y medios de comunicación relevantes constituye un aspecto esencial del proceso. La identificación de fuentes primarias y secundarias, tales como redes sociales, foros, blogs y medios digitales especializados, permite la recopilación de información representativa del ecosistema informativo analizado.

2.1.2 Selección y filtrado de fuentes de información

El correcto funcionamiento de la herramienta OSINT desarrollada depende en gran medida de la precisión y fiabilidad de los datos que alimentan su base de análisis. Aunque la recopilación de información es un proceso complejo, su eficacia radica en la labor previa del analista, quien debe definir criterios claros de selección y garantizar que las fuentes sean verificables y representativas del entorno informativo. Sin esta fase inicial, el margen de error se incrementa, afectando directamente la capacidad del programa para procesar y clasificar datos de manera precisa, ofreciendo unos resultados que pueden diferir de la realidad.

Para optimizar su rendimiento, la herramienta OSINT integra datos provenientes de medios de comunicación, redes sociales y fuentes abiertas, priorizando aquellas que cumplen con estándares de fiabilidad. Además,

emplea filtros automáticos y técnicas de normalización para minimizar ruido informativo, detectar patrones de comunicación y estructurar la información de manera coherente. En el caso de redes sociales, se analizan tendencias discursivas, uso de símbolos y *hashtags*, y, cuando es posible, datos geolocalizados para mejorar la contextualización.

La flexibilidad en la selección de datos es clave para adaptar la herramienta a distintos escenarios, permitiendo ajustar parámetros en función de la disponibilidad y calidad de la información. En este sentido, la labor del analista no solo define el punto de partida del proceso, sino que también optimiza el rendimiento del programa, asegurando que las predicciones y clasificaciones generadas sean lo más precisas y útiles posible.

2.1.3 Identificación de actores clave

Dentro del ecosistema digital, ciertos actores poseen un papel determinante en la difusión y amplificación de la información, influyendo en la construcción de narrativas y en la percepción pública de los acontecimientos. La identificación de estos agentes es un paso esencial en el análisis OSINT, ya que permite comprender cómo se propagan los discursos, quiénes los generan y qué impacto tienen dentro del entorno informativo.

Para ello, la herramienta OSINT implementa un proceso de segmentación de usuarios por nivel de influencia, diferenciando entre actores gubernamentales, medios de comunicación, líderes de opinión y comunidades digitales. Esta clasificación facilita la detección de fuentes clave dentro de cada categoría y permite analizar su rol en la difusión de la información, ya sea como emisores primarios, amplificadores o agentes de contranarrativa.

Además, se lleva a cabo un análisis de interacción y alcance, que evalúa la capacidad de cada actor para generar reacciones dentro del ecosistema digital. Este proceso considera métricas como la frecuencia de publicación, el número de interacciones (comentarios, compartidos, reacciones) y el alcance del contenido. A través de estos indicadores, la herramienta puede identificar patrones de difusión y detectar tendencias emergentes, lo que resulta fundamental para anticipar el impacto de ciertos discursos y evaluar su nivel de penetración en distintos segmentos de la audiencia.

La combinación de estas metodologías permite a la herramienta OSINT no solo mapear el flujo de información dentro del ecosistema digital, sino también optimizar la precisión del análisis, distinguiendo entre actores con verdadera capacidad de influencia y aquellos cuya presencia es circunstancial o de menor relevancia.

Ejemplo aplicado: análisis de la percepción de la UME y el Ejército español en la Comunidad Valenciana tras la DANA

En este caso, el analista debe recopilar datos sobre cómo se ha percibido la intervención de la UME y del Ejército Español tras la crisis de la DANA.

Delimitación geográfica y sectorial

Para garantizar la precisión del análisis, se ha delimitado la zona geográfica y el ámbito de estudio en función de la zona de operación y la temática de interés. En este caso, la investigación se centra en la Comunidad Valenciana, con un enfoque en la percepción mediática y social de la intervención de las fuerzas militares, diferenciando la cobertura y el discurso en torno a la Unidad Militar de Emergencias (UME) y el Ejército español en el contexto de la DANA.

Fuentes de Información

La recopilación de datos se ha realizado a partir de fuentes digitales representativas del ecosistema informativo valenciano. Se han seleccionado los siguientes canales para garantizar una visión integral del discurso mediático y ciudadano:

— Medios digitales: se han analizado artículos y reportajes publicados en *Levante-EMV*, *Las Provincias*, *À Punt* e *Información Alicante*, debido a su relevancia en la cobertura informativa regional.

— Red social X: se han recopilado publicaciones de ciudadanos, periodistas y actores políticos con el fin de evaluar la conversación digital y su impacto en la percepción pública.

— Telegram: se han extraído publicaciones de cuentas clave con el ánimo de analizar y clasificar sus mensajes.

— Plataformas comunitarias: se han examinado debates y opiniones en grupos de Facebook y foros locales, permitiendo identificar la percepción de la ciudadanía fuera de los canales mediáticos convencionales.

Filtrado y Normalización de Datos

Dado el gran volumen de información recopilada, ha sido necesario implementar un proceso de filtrado y normalización de datos con el objetivo de garantizar la pertinencia y la calidad del análisis. Este proceso ha comprendido las siguientes etapas:

— Eliminación de publicaciones irrelevantes: se han descartado contenidos que no guardan relación directa con la DANA o con la intervención de las fuerzas militares, reduciendo el ruido informativo.

— Normalización de datos: se ha realizado la estandarización de fechas, formatos y categorías, asegurando la coherencia de la información y su compatibilidad con la herramienta OSINT desarrollada.

2.2 Herramientas empleadas en el análisis inicial

Una vez que el analista ha realizado una búsqueda precisa de fuentes y actores clave, estos se introducen en herramientas especializadas para la extracción automatizada de datos, optimizando el proceso de recopilación. Para ello, se emplean soluciones comerciales y de acceso abierto que permiten obtener información estructurada de diversas plataformas.

Entre estas herramientas se incluyen técnicas de *web scraping*, que permiten extraer contenido de sitios web de interés, APIs de redes sociales, que facilitan la recopilación de publicaciones y metadatos de plataformas como Telegram o TikTok y plataformas de agregación de noticias, que centralizan información proveniente de diferentes medios.

Si bien la construcción de la base de datos se realiza manualmente, el analista puede apoyarse en hojas de cálculo avanzadas, *software* de gestión de datos y sistemas de etiquetado automático, lo que facilita la organización y segmentación de la información recopilada, asegurando su coherencia y utilidad para el análisis posterior.

Ejemplo aplicado: uso de herramientas para analizar la percepción de la UME y el Ejército español

En este caso, una vez que el analista ha identificado las fuentes clave, se emplean herramientas especializadas para la extracción de datos y su posterior análisis. Para ello, se pueden utilizar:

— Técnicas de *web scraping*: se han aplicado métodos de extracción automatizada de datos para recopilar artículos de medios digitales sobre la DANA en la Comunidad Valenciana, permitiendo un análisis exhaustivo de la cobertura informativa.

— APIs de redes sociales: se han utilizado interfaces de programación de aplicaciones (APIs) para identificar menciones y patrones discursivos en plataformas como Telegram, con el objetivo de analizar la conversación digital en torno a la UME y el Ejército español. Esta metodología permite acceder a publicaciones en tiempo real y evaluar la interacción de los usuarios con determinados discursos.

— Plataformas de agregación de noticias: se han empleado herramientas especializadas que centralizan información de diversos medios, facilitando la detección de tendencias informativas y la identificación de narrativas predominantes en el contexto de la DANA.

2.3 Construcción de una base de datos

Una vez recopilada la información, es fundamental estructurarla y consolidarla en una base de datos robusta que garantice su almacenamiento seguro y facilite su explotación eficiente en el análisis OSINT. La calidad y organización de esta base de datos determinarán, en gran medida, la precisión de los resultados obtenidos por la herramienta, ya que un cribado deficiente puede derivar en errores de interpretación, sesgos o pérdida de información relevante.

Para optimizar su funcionamiento, la base de datos debe cumplir con una serie de criterios de organización que permitan una gestión eficaz de los datos recopilados. En primer lugar, la estructura de almacenamiento debe contemplar una categorización detallada basada en fecha, fuente, tipo de contenido y nivel de relevancia. Esto permite establecer filtros que agilicen el acceso a la información y faciliten la identificación de patrones dentro del conjunto de datos.

El etiquetado de información es otro aspecto clave en la optimización del almacenamiento. El uso de palabras clave, *hashtags* y categorías contribuye a mejorar la segmentación y búsqueda de datos dentro del repositorio de almacenamiento, permitiendo una indexación más precisa de los elementos disponibles. La integración de múltiples formatos es también un requisito indispensable, dado que la información recopilada puede presentarse en diversos tipos de archivos, incluyendo texto, imágenes, videos y archivos de audio. La capacidad de almacenar y procesar estos formatos garantiza que la herramienta pueda analizar datos heterogéneos sin limitaciones estructurales.

Además de la organización, la seguridad y mantenimiento de la base de datos es un factor crítico para garantizar su fiabilidad y continuidad operativa. La protección de datos es prioritaria, por lo que se implementan medidas para prevenir la manipulación de la información y evitar pérdidas accidentales. Esto implica la aplicación de protocolos de autenticación, control de acceso y auditorías periódicas para verificar la integridad de los registros.

Asimismo, la base de datos debe contar con un sistema de actualización continua, que permita la incorporación de nuevas fuentes de información y la eliminación de datos obsoletos. Este proceso asegura que el análisis realizado por la herramienta OSINT se base siempre en información actualizada y relevante, evitando sesgos provocados por el uso de datos desactualizados o irrelevantes.

En conjunto, estos criterios permiten la construcción de una base de datos estructurada, segura y adaptable, garantizando que la herramienta pueda procesar información de manera eficiente y ofrecer análisis precisos basados en datos de calidad.

Por último, almacenar de manera estructurada los datos recopilados de fuentes abiertas, así como los resultados obtenidos de los análisis y clasificaciones realizadas por el programa o el analista, será fundamental a la hora de generar o refinar modelos de IA, ya que estos modelos requieren de cantidades considerables de datos etiquetados. Estos modelos realizan tareas fundamentales a la hora de llevar a cabo los análisis, como se detallará más adelante.

Ejemplo aplicado: construcción de la base de datos sobre la percepción de la UME y el Ejército español en la Comunidad Valenciana

El analista debe diseñar una base de datos estructurada que garantice la organización eficiente de la información y facilite su explotación en fases posteriores del análisis OSINT. Para ello, la base de datos debe incluir:

- Relación de usuarios clave de redes sociales y medios de comunicación relevantes para el análisis.
- Registro de menciones en medios de comunicación, incorporando datos clave como la fecha de publicación, la fuente y la categoría de información, lo que permitirá evaluar la cobertura mediática y su evolución en el tiempo.
- Análisis de publicaciones en redes sociales, con una recopilación sistemática de contenido asociado a hashtags relevantes, palabras y emoticonos utilizados o métricas de interacción, posibilitando la identificación de tendencias y el impacto de determinados discursos en la conversación digital.
- Categorización por percepción pública, segmentando el contenido según su tono positivo, negativo o neutro, con el objetivo de evaluar la orientación predominante en la narrativa mediática y social.

Una base de datos densamente poblada y bien estructurada es fundamental para la implementación de herramientas analíticas avanzadas, ya que permite la detección de patrones de opinión, el análisis de tendencias y la evaluación del impacto de narrativas específicas en el ecosistema informativo.

3 Códigos desarrollados y su funcionamiento

3.1 Código 1: análisis de sentimiento del entorno informativo

3.1.1 Objetivo y lógica detrás del análisis

El análisis de sentimiento es una técnica fundamental en el procesamiento de información en entornos digitales, utilizada para evaluar la percepción y actitud expresada en publicaciones de redes sociales (RRSS) y

medios de comunicación (MMCC). Su aplicación en la herramienta OSINT desarrollada tiene como objetivo principal determinar la orientación emocional y narrativa del contenido analizado, proporcionando una visión estructurada sobre cómo se perciben determinados eventos, actores o temas dentro de un ecosistema informativo.

El propósito del análisis de sentimiento en este contexto es clasificar y cuantificar el tono predominante en las publicaciones asociadas a una operación o estudio específico. Para ello, se emplean modelos avanzados de PLN que asignan valores a las publicaciones en función de su carga emocional, segmentándolas en tres categorías principales:

— Positivas: contenido con una percepción favorable hacia el tema analizado.

— Negativas: publicaciones con un tono crítico, adverso o hostil.

— Neutras: información sin carga emocional evidente o con un tono equilibrado.

La lógica subyacente de este análisis radica en la necesidad de comprender la dinámica del discurso digital, identificando tendencias, patrones de polarización y posibles intentos de manipulación informativa. Gracias a esta metodología, es posible detectar cambios en la percepción pública, evaluar el impacto de ciertas narrativas y establecer correlaciones entre eventos específicos y la reacción del ecosistema digital.

Además, este enfoque no solo permite la monitorización en tiempo real, sino que también aporta información estratégica para la toma de decisiones, facilitando la adaptación de mensajes, la identificación de riesgos comunicacionales y el desarrollo de estrategias de respuesta basadas en datos objetivos.

3.1.2 Técnicas utilizadas: procesamiento del lenguaje natural (PLN) y clasificación por taxonomías

El análisis de sentimiento implementado en este código se basa en técnicas avanzadas de PLN, permitiendo que los algoritmos comprendan, procesen y clasifiquen textos en lenguaje natural de manera estructurada y precisa. Se ha utilizado, en principio, un modelo de *deep learning* entrenado para determinar el sentimiento de un texto.

Para llevar a cabo este análisis, primero se realiza una fase de preprocesamiento del texto, donde se eliminan caracteres especiales, emojis y signos de puntuación que podrían generar ruido en los resultados. Además, el texto se convierte a minúsculas para evitar discrepancias debidas a la capitalización y se eliminan las palabras vacías (*stopwords*), aquellas que no aportan información relevante, como artículos y conjunciones.

Una vez limpiado el texto, este debe transformarse en una representación numérica comprensible para los modelos de análisis. Para ello, se emplean técnicas como TF-IDF (Term Frequency-Inverse Document Frequency), que pondera la relevancia de las palabras en un conjunto de textos.

Para la fase de clasificación del sentimiento, se procesa el texto mediante un modelo entrenado para clasificación de sentimiento con base en el modelo BERT de clasificación de textos. BERT es un modelo de *deep learning* el cual se ha afinado para la clasificación deseada en este caso. De esta manera, se consigue asignar una categoría al texto procesado de cada publicación: positivo, cuando el contenido transmite una percepción favorable; negativo, cuando el tono es crítico o adverso; y neutro, cuando no hay una carga emocional predominante.

Los resultados del análisis se presentan mediante diversas representaciones visuales que facilitan la interpretación de los datos. Se utilizan gráficos de barras para mostrar el volumen de publicaciones en cada categoría, diagramas circulares que reflejan la proporción relativa de cada tipo de sentimiento y mapas de calor que posicionan a los actores clave dentro del ecosistema informativo en función de su favorabilidad u hostilidad, así como de su nivel de relevancia.

3.1.3 Ejemplo práctico y resultados esperados

El sistema desarrollado clasifica todas las publicaciones y noticias en función de criterios predefinidos por el analista, que tienen gran peso a la hora de entrenar el modelo de clasificación de texto utilizado, determinando el grado de favorabilidad o desfavorabilidad hacia el objetivo de la operación que esté siendo objeto de análisis.

Análisis de sentimientos en publicaciones

En la primera imagen proporcionada, se observa la distribución del sentimiento de las publicaciones analizadas. En este gráfico se presentan dos representaciones:

— Diagrama de barras: muestra la cantidad absoluta de publicaciones positivas, negativas y neutras. En la gráfica, se observa que la mayoría de las publicaciones son neutras, seguidas por las negativas y, en menor medida, las positivas.

— Gráfico circular: expresa la proporción porcentual de cada categoría. En este caso, se visualiza que el 77,4 % del contenido es neutro, el 13,2 % negativo y solo el 9,4 % positivo.

En la segunda figura, se presenta un gráfico de barras apiladas, donde se analizan palabras clave específicas determinadas por el analista, que han sido encontradas en las publicaciones mediante algoritmos tradicionales de programación y su asociación con un sentimiento determinado. En este análisis se destacan:

— El volumen de menciones de cada término en las publicaciones analizadas.

— La proporción de sentimiento (positivo, negativo o neutro) de cada palabra clave.

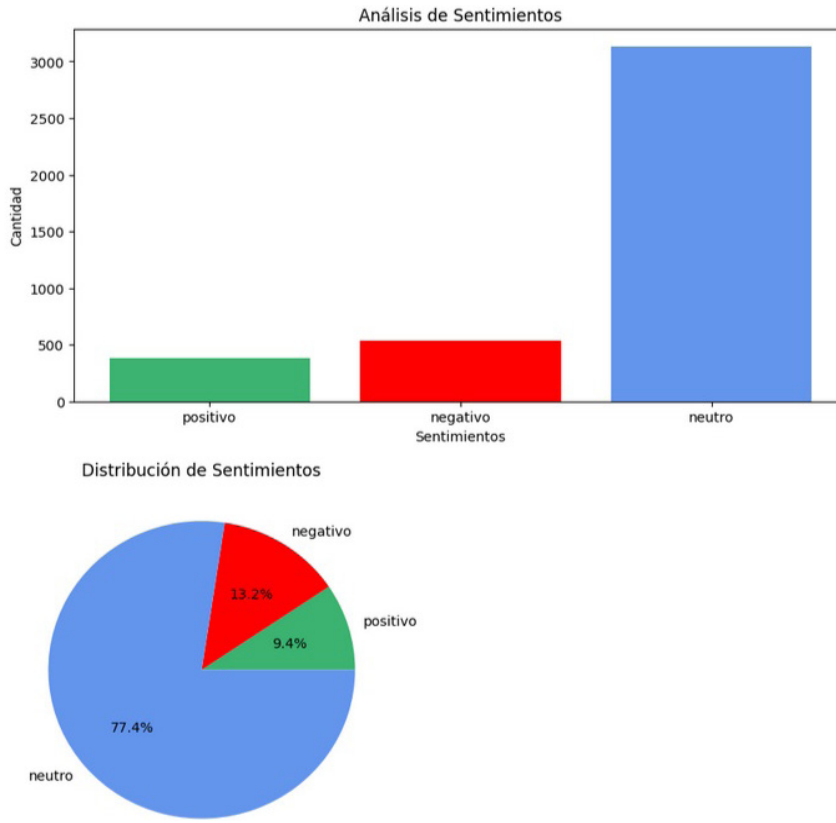


Figura 1. Gráficos de resultados de análisis de sentimiento. Elaboración propia

Este tipo de análisis permite identificar términos con una alta carga emocional negativa, los cuales pueden señalar la presencia de conflictos o controversias. Asimismo, facilita la evaluación de la percepción de conceptos clave dentro del ecosistema informativo, permitiendo un análisis más profundo de su impacto. Además, contribuye a la detección de oportunidades

estratégicas para influir en la narrativa digital a través de acciones comunicacionales dirigidas.

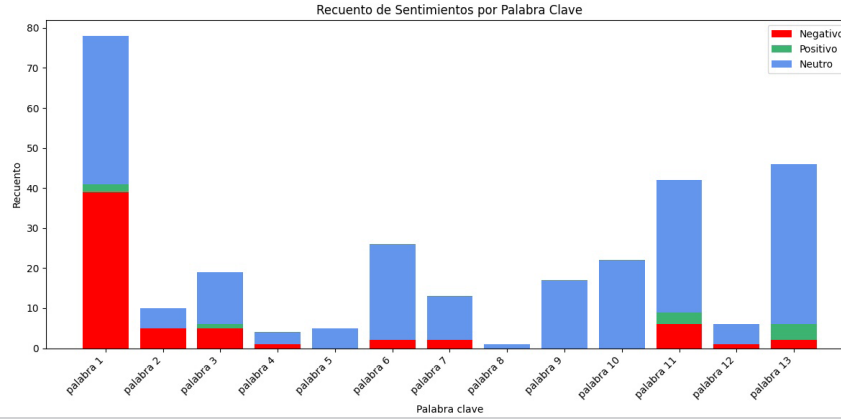


Figura 2. Gráfico de barras de resultados de análisis de sentimiento por palabras clave. Elaboración Propia

Por último, el mapa de calor (*heatmap*) utilizado en este análisis posiciona a los actores clave en función de dos variables fundamentales: su hostilidad o favorabilidad hacia el tema de interés objeto del análisis, representado según su posición en el eje x, y su relevancia dentro del entorno informativo, representado según la posición en el eje y. Esta representación gráfica permite identificar patrones de polarización y priorizar aquellos actores con mayor impacto en la conversación digital. Cada medio viene representado por una etiqueta con un número.

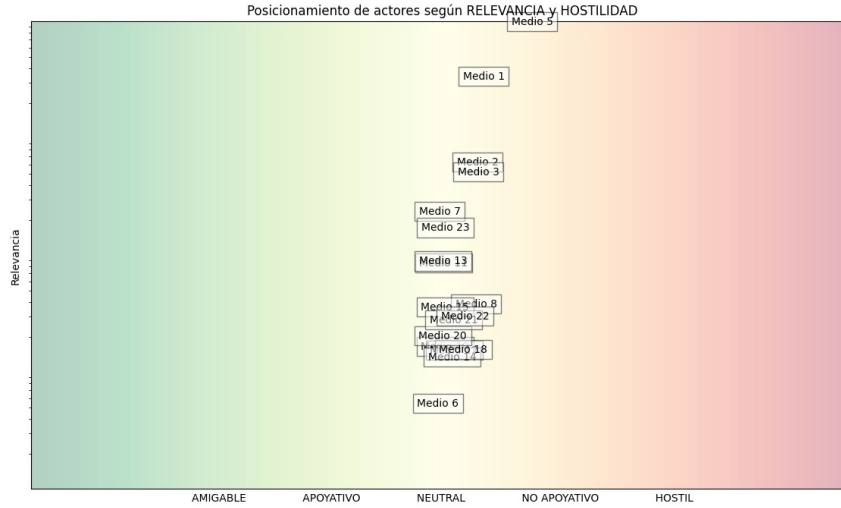


Figura 3. Mapa de calor, eje e indica relevancia, posición en eje x indica nivel de hostilidad. Elaboración propia

Para evitar que las diferencias de relevancia entre medios de comunicación y usuarios de redes sociales distorsionen la visualización, el eje y, que representa este valor, se encuentra en escala logarítmica. Dado que en entornos digitales la distribución de la relevancia suele ser altamente desigual —con algunos actores alcanzando audiencias masivas mientras que otros tienen una visibilidad considerablemente menor—, la escala logarítmica permite suavizar estas discrepancias y representar de manera más equilibrada el peso de cada actor dentro del entorno analizado.

En el caso de los medios de comunicación, la relevancia se mide a través del número de visualizaciones semanales o mensuales, extraídas mediante técnicas de *web scraping* sobre sitios web que ofrecen estos datos de manera abierta. Para los usuarios de redes sociales, la métrica utilizada es el *engagement*, que incluye interacciones como comentarios, compartidos y reacciones, proporcionando un indicador más preciso de su impacto en la difusión de narrativas.

La disposición de los actores en el mapa permite una interpretación clara de su alineación y nivel de influencia. Aquellos situados en la zona de mayor hostilidad y relevancia representan un riesgo informativo significativo, ya que tienen una gran capacidad de difusión de contenidos contrarios a la narrativa de interés. En contraste, los actores con alta relevancia y una postura neutral o favorable pueden representar aliados estratégicos o espacios de oportunidad para influir en la conversación digital.

Este tipo de visualización es esencial para la toma de decisiones estratégicas en operaciones de monitoreo informativo y gestión de la reputación digital, ya que proporciona un análisis detallado de los agentes que moldean la percepción pública y facilita el desarrollo de estrategias de comunicación adaptadas a la dinámica del ecosistema digital.

3.2 Código 2: clasificación de redes sociales y MMCC con machine learning

3.2.1 Definición de categorías y enfoque clasificatorio

El segundo módulo de la herramienta OSINT se centra en la clasificación automatizada de contenido digital en redes sociales y medios de comunicación, utilizando técnicas avanzadas de *machine learning*. Este proceso permite segmentar grandes volúmenes de datos de manera estructurada, facilitando la identificación de narrativas, tendencias y potenciales campañas de influencia dentro del entorno informativo analizado.

Dado el crecimiento exponencial del flujo de información en plataformas digitales, la capacidad de analizar y clasificar contenido de manera automatizada resulta esencial para la toma de decisiones estratégicas. La implementación de algoritmos de aprendizaje automático permite superar las limitaciones de los análisis manuales, dotando al sistema de una mayor capacidad de escalabilidad y precisión en la detección de patrones discursivos.

La eficacia del proceso de clasificación depende de una fase preliminar de análisis en la que el analista determina criterios fundamentales como:

— Selección de fuentes clave: medios de comunicación tradicionales, plataformas alternativas, redes sociales y foros especializados.

— Identificación de actores relevantes: perfiles influyentes, medios con alto impacto, comunidades digitales y usuarios anónimos con actividad significativa.

— Definición de la audiencia objetivo: usuarios afectados por la narrativa analizada y potenciales receptores de campañas informativas o de desinformación.

— Contextualización del análisis: delimitación de la zona de interés, coyuntura política, social o económica y el propósito estratégico del estudio.

Estos factores permiten establecer una taxonomía clasificatoria, asegurando que el modelo de *machine learning* se entrene con datos alineados a los objetivos del análisis. La segmentación se realiza en función de distintas categorías, que pueden organizarse bajo diversos enfoques, tales como:

— Temática del contenido: clasificación en función de áreas como política, seguridad, conflictos, economía o desinformación.

— Intención comunicativa: diferenciación entre contenido meramente informativo, artículos de opinión, discursos propagandísticos o estrategias de manipulación.

— Tipo de fuente: distinción entre medios oficiales, plataformas de comunicación alternativas, redes sociales y foros especializados.

— Relevancia y alcance: evaluación de la influencia de cada fuente dentro del entorno digital, considerando métricas como *engagement*, tráfico web y nivel de interacción.

La implementación de estos criterios permite que el modelo de *machine learning* identifique con precisión la estructura del discurso digital en la zona de interés, diferenciando entre contenido legítimo, narrativas emergentes y posibles intentos de manipulación informativa.

El gráfico circular presentado en la figura refleja la segmentación del contenido en función de las categorías predefinidas. Cada segmento representa una proporción del volumen total de publicaciones clasificadas dentro de cada tema de interés y permite al analista visualizar la distribución temática del discurso digital.

3.2.2 Algoritmos y modelos implementados

Para lograr la clasificación de las publicaciones con base en las taxonomías definidas por el analista, se ha entrenado, con una gran cantidad de datos, un modelo de *machine learning* que permita automatizar el proceso de categorización. Esto ha requerido un trabajo previo de etiquetado manual de lotes de publicaciones relativos al entorno digital objeto del análisis. Este modelo se ha ido refinando a medida que se han ido teniendo más datos para su entrenamiento y sus resultados siempre están supervisados por el analista, para determinar si la clasificación que se está haciendo de las publicaciones es correcta.

De esta forma se consigue automatizar un proceso tedioso de clasificación manual de grandes cantidades de publicaciones.

Una vez utilizado el modelo sobre un lote de publicaciones y los resultados han sido contrastados y ajustados, en el caso de que fuera necesario por el analista, se almacenan en la base de datos, con la certeza de que son completamente fiables. De esta manera, se podrá seguir refinando el modelo al entrenarlo con más lotes de datos etiquetados, de manera que, con el tiempo, la precisión de este pueda converger a un valor que se aproxime al 100 %.

3.2.3 Resultados esperados de un supuesto práctico

Una vez se clasifican las publicaciones con el apoyo del modelo de *machine learning*, la herramienta expone gráficamente los resultados para obtener una visualización de las temáticas tratadas en el entorno digital objetivo con base en las taxonomías concebidas.

En este caso, se exponen en un gráfico circular como el que se muestra en la figura siguiente. No deben sacarse conclusiones de los resultados, solo se muestran para exponer las capacidades de la herramienta.

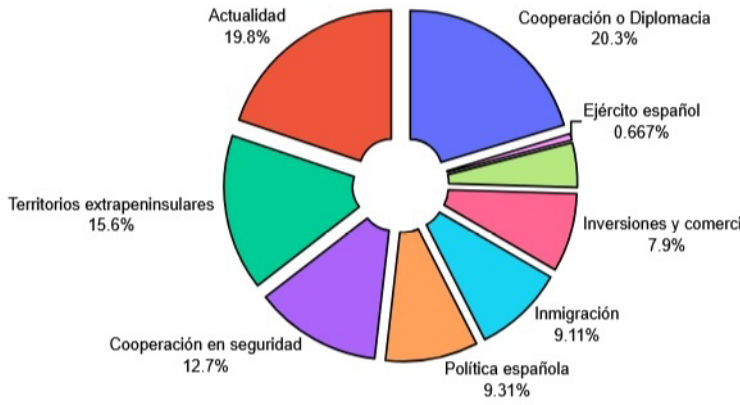


Figura 4. Gráfico de resultados de clasificación en taxonomías. Elaboración propia.

3.3 Código 3: clasificación de contenido en TikTok en varias fases

La clasificación del contenido en TikTok dentro de la herramienta OSINT desarrollada se estructura en tres fases o filtros, los cuales corresponden a distintas etapas de extracción y procesamiento de datos. Estos filtros permiten segmentar y analizar el contenido de manera progresiva, asegurando una clasificación eficiente y adaptada a los objetivos de la operación.

Antes de aplicar estos filtros, se carga en la herramienta una base de datos con usuarios previamente seleccionados. La selección de esta muestra puede variar en función del enfoque del análisis, pudiendo ser una muestra sesgada o concreta, si se quiere centrar en un nicho específico o una muestra más representativa y aleatoria, manteniendo siempre unos criterios mínimos de relevancia.

Para realizar este procesamiento de información de la red social TikTok, se han empleado métodos de *web scraping* para extraer los datos de descripción, comentarios y ubicación del vídeo de cada una de las publicaciones de los usuarios seleccionados. Además, se ha descargado y procesado del vídeo mediante un modelo de *deep learning* para la detección de objetos en imágenes.

Cada fase de clasificación de contenido desarrollada a continuación corresponde a un filtro progresivo en la detección de contenido relevante en TikTok:

3.3.1. Filtrado por *hashtags* y taxonomías en la descripción del vídeo

En la primera fase, la herramienta analiza la descripción de los videos publicados por los usuarios seleccionados, buscando *hashtags* o palabras clave predefinidas por el analista. Esta clasificación inicial permite una primera segmentación del contenido en función de las etiquetas que los propios creadores utilizan para categorizar sus publicaciones. El resultado de este análisis es una tabla en la que aparece el nombre de usuario, la URL de la publicación, la descripción y las palabras clave que se han encontrado en la descripción de la publicación, incluidas las que aparezcan como *hashtag*.

La información contenida en esta tabla se puede representar en gráficos como se ha hecho con los resultados de los análisis anteriores o se puede utilizar para detectar las publicaciones que sean más interesantes para analizar el entorno que esté siendo objeto de estudio. Por el momento, no se han desarrollado representaciones gráficas específicas para esta información en la herramienta que puedan ser expuestos en este artículo.

3.3.2 Filtrado por análisis de comentarios

En la segunda fase, se analizan los comentarios de los vídeos identificados en la primera fase, buscando menciones a *hashtags* o palabras clave que no estén necesariamente en la descripción, pero que puedan contextualizar el contenido. Esta fase permite ampliar el rango de detección y capturar contenido relevante que no haya sido etiquetado explícitamente por el creador del vídeo.

El resultado de este análisis consiste en una nueva columna en la tabla mencionada en el apartado anterior en la que se indica qué palabras clave y en qué cantidad se han encontrado al procesar los comentarios de la publicación.

Es importante destacar que las tres fases no son excluyentes entre sí. Si en una fase no se encuentran resultados, la herramienta sigue procesando el vídeo en los siguientes filtros hasta completar el análisis. La exclusión solo ocurre cuando, tras aplicar las tres fases, no se detecta ninguna coincidencia con los criterios establecidos.

3.3.3 Filtrado por fotogramas mediante procesado de imágenes con *deep learning*

En la tercera fase, se procede a detectar los emoticonos de interés que estén presentes en el vídeo de la publicación. Para ello, se ha entrenado un modelo de *deep learning* que detecta ciertos emoticonos en imágenes. Más concretamente, la bandera de España y de la Unión Europea. Para cada caso se deberá entrenar un modelo que detecte los emoticonos deseados.

Para poder procesar el vídeo de la publicación de TIkTok, la herramienta primero obtiene la ubicación del vídeo mediante técnicas de *web scraping* y lo descarga. Después, separa el vídeo en fotogramas y los procesa uno a uno con el modelo de detección de emoticonos, escribiendo en una nueva columna de la tabla mencionada con anterioridad si ha encontrado los emoticonos de interés.

El resultado del procesamiento de un fotograma de un vídeo por el modelo *deep learning*, es de manera visual, el que se expone en la siguiente figura:

En la figura, se indica que se ha detectado un emoticono de la bandera de España con una precisión en la detección del 91,2 %. Estos datos serán los que se guarden en la fila correspondiente a la publicación junto con el análisis de palabras de la descripción y los comentarios.

Este procedimiento permite detectar mensajes inscritos en los vídeos de la red social, práctica que es bastante habitual en este entorno.

Por último, respecto a este análisis del vídeo de la publicación, hay que destacar que el entrenamiento del modelo para detectar emoticonos en los fotogramas del vídeo requiere de un trabajo previo de etiquetado de imágenes que permitan entrenar el modelo. La recopilación y el etiquetado de estas imágenes para entrenamiento son el paso más crítico para tener un modelo de detección preciso y funcional.

Figura 5. Resultado de procesado de detección de objetos. Elaboración propia

4 Conclusiones y aprendizajes

4.1 Impacto del programa en la organización

El desarrollo e implementación del programa OSINT basado en técnicas de PLN, inteligencia artificial y programación tradicional ha demostrado ser una herramienta muy eficiente para el análisis del entorno de la información en escenarios digitales. Su integración dentro de procesos de inteligencia ha permitido optimizar el monitoreo y clasificación de grandes volúmenes de datos, facilitando la detección de tendencias y narrativas de manera automatizada.

Uno de los principales impactos del programa ha sido la reducción del tiempo requerido para procesar grandes cantidades de información de fuentes abiertas, lo que ha mejorado la capacidad de reacción y toma de decisiones estratégicas, además de permitir un mejor aprovechamiento de los recursos humanos de la unidad. Asimismo, su modularidad y adaptabilidad han hecho posible su implementación en diversos contextos operativos, lo que lo convierte en una solución flexible y escalable.

Por otra parte, la combinación de metodologías analíticas y el conocimiento experto de analistas ha permitido afinar los resultados y mejorar la precisión del análisis, minimizando sesgos y asegurando que la información obtenida sea útil y de relevancia para la toma de decisiones.

4.2 Principales aprendizajes y contribuciones

El desarrollo del programa ha proporcionado una serie de aprendizajes clave en el ámbito de la inteligencia de fuentes abiertas y la automatización de análisis de información:

- Importancia del diseño metodológico: la eficacia del programa depende en gran medida de la correcta estructuración del proceso de recopilación, filtrado y análisis de datos. Definir criterios claros desde el inicio es esencial para garantizar la calidad de los resultados.
- Colaboración interdisciplinaria: la integración de analistas con expertos en procesamiento de datos ha sido fundamental para ajustar los modelos y mejorar su precisión. La sinergia entre conocimientos operacionales y técnicos permite desarrollar herramientas más robustas y adaptadas a necesidades específicas.
- Desafíos en la clasificación automatizada: la ambigüedad del lenguaje en redes sociales y la constante evolución de términos y expresiones requieren una actualización continua de los modelos de clasificación y análisis de sentimiento. La implementación de enfoques híbridos ha demostrado ser una solución eficaz para abordar este desafío.
- Escalabilidad y adaptabilidad: la flexibilidad del programa ha permitido su ajuste a distintos entornos y escenarios, lo que evidencia la importancia de diseñar soluciones tecnológicas modulares que puedan evolucionar junto con los requerimientos operativos.
- Impacto estratégico del análisis de datos: la capacidad de identificar patrones, tendencias y actores clave dentro del ecosistema informativo ha reforzado la utilidad del OSINT en la toma de decisiones. La detección temprana de campañas de desinformación o cambios en la percepción pública es un recurso valioso en la gestión de crisis y operaciones de seguridad.

— Combinación de distintas tecnologías: la elaboración de esta herramienta sirve como buen ejemplo de empleo de distintas tecnologías para resolver las distintas partes del problema que enfrenta. De esta forma, se ha optado por la solución más conveniente según las necesidades, coexistiendo en la herramienta tanto modelos de inteligencia artificial de *machine learning* y *deep learning* como técnicas de *web scraping* o filtrado por palabras clave realizado por algoritmos tradicionales de programación.

4.3 Próximos pasos y mejoras propuestas

Para maximizar el potencial del programa, se podrían sondear las siguientes líneas de mejora y desarrollo:

— Mejoras en la precisión del análisis de sentimiento: implementación de modelos más avanzados, para una clasificación más precisa y adaptable al contexto.

— Integración con fuentes de datos adicionales: expansión del alcance del programa mediante la incorporación de nuevas plataformas digitales y medios de comunicación, mejorando la cobertura del análisis.

— Automatización del proceso de actualización: desarrollo de un sistema que permita la actualización automática de taxonomías, términos clave y patrones de clasificación según las tendencias emergentes.

— Optimización del rendimiento y escalabilidad: mejora en la infraestructura de almacenamiento y procesamiento de datos para permitir la gestión eficiente de volúmenes crecientes de información.

— Capacitación continua del personal: fomento de programas de formación para analistas y expertos en datos, garantizando una actualización constante en técnicas de análisis y procesamiento de información.

Además, se puede tratar de combinar distintos módulos del programa con el objetivo de llegar a análisis más avanzados, como pudiera ser el uso del modelo que clasifica el sentimiento de textos con los comentarios de las publicaciones de TikTok accedidos mediante *web scraping*.

En conclusión, este programa representa un avance significativo en la aplicación de OSINT en entornos estratégicos, proporcionando una herramienta eficaz para el análisis y la toma de decisiones en contextos de crisis y seguridad. Su desarrollo y mejora continua permitirán fortalecer su impacto y ampliar su aplicabilidad en distintos ámbitos operativos. Para concluir, este desarrollo realizado con recursos limitados demuestra que las soluciones tecnológicas son accesibles y se puede sacar partido de ellas de manera autónoma si se alinean los recursos humanos disponibles de manera adecuada.

Inteligencia posnormal: gestión de riesgos en la zona gris

Jesús Hernández Álvarez

Resumen

Este artículo cuestiona el paradigma tradicional de la inteligencia, surgido durante la Guerra Fría, analizando su transformación en el contexto de un entorno global en rápida evolución, caracterizado por la incertidumbre y la complejidad de los tiempos posnormales, abogando por un nuevo paradigma más adaptativo, multidisciplinar y cooperativo, que integre fuentes abiertas y una comunidad de inteligencia extendida.

Se explora la ciencia posnormal como marco conceptual para abordar problemas con hechos inciertos, valores en conflicto y decisiones urgentes, así como la evolución desde el ciclo de inteligencia tradicional hacia un enfoque de gestión de riesgos, integrando las funciones de inteligencia y gobernanza, en la búsqueda de una visión compartida del problema de seguridad a gestionar.

Asimismo, se subraya la importancia de comprender y mitigar las limitaciones cognitivas como los sesgos, fomentando el pensamiento sistémico y la modelización compleja asistida por IA para mejorar la conciencia situacional. Por último, se destaca la necesidad de proteger el ámbito cognitivo como un activo crucial frente a las estrategias híbridas en la zona gris, delineando posibles vectores de innovación para los Servicios de Inteligencia e Información del Estado en un entorno posnormal, lo que daría lugar a varios escenarios de evolución.

Palabras clave

Innovación, Servicios de inteligencia, Servicios de información, Evolución, Gobernanza.

Post-normal intelligence: risk management in the gray area

Abstract

This article questions the traditional intelligence paradigm that emerged during the Cold War, analyzing its transformation in the context of a rapidly evolving global environment characterized by the uncertainty and complexity of post-normal times. It advocates for a new, more adaptive, multidisciplinary, and cooperative paradigm that integrates open sources and an extended intelligence community.

It explores post-normal science as a conceptual framework for addressing problems with uncertain facts, conflicting values, and urgent decisions. It also explores the evolution from the traditional intelligence cycle to a risk management approach, integrating intelligence and governance functions in the pursuit of a shared vision of the security problem to be managed.

It also highlights the importance of understanding and mitigating cognitive limitations such as biases, fostering systems thinking and complex AI-assisted modeling to improve situational awareness. Finally, the need to protect the cognitive domain as a crucial asset against hybrid strategies in the gray zone is highlighted, outlining possible vectors of innovation for State Intelligence and Information Services in a post-normal environment, which would give rise to several evolutionary scenarios.

Keywords

Innovation, Intelligence services, Information services, Evolution, Governance.

1 Introducción

Cuando se habla de innovación en el ámbito de la seguridad y la defensa, se suele pensar rápidamente en la de tipo tecnológico. En este sentido, es cierto que la innovación, que requiere una combinación de avances incrementales y tecnologías emergentes con capacidades disruptivas, actualmente se está centrando en los macrodatos y el análisis avanzado, la inteligencia artificial (IA), los sistemas autónomos, las tecnologías cuánticas, las tecnologías del espacio, las armas hipersónicas, las biotecnologías y tecnologías de mejora humana y los materiales avanzados y nuevas técnicas de fabricación (Martín Palma, 2023).

Además, en un entorno de tensiones geopolíticas, hay que resaltar el conflicto como motor de cambio, sobre todo, en cinco áreas: cambios sociológicos, tecnológicos, doctrinales, políticos y económicos. En este sentido, se podría entender el conflicto como el resultado de una mala adaptación a cambios previos, en un ciclo continuo de desadaptación-conflicto-adaptación (Frías Sánchez, 2023)

En este contexto y en lo que se refiere a la inteligencia, el presente artículo se centra más en aspectos doctrinales, conceptuales y metodológicos que en aspectos tecnológicos, que pueden ser relevantes en la transformación de los procesos y estructuras de los Servicios de Inteligencia e Información del Estado.

La Estrategia de Seguridad Nacional de 2021 se enfoca en una serie de vectores de transformación que, en los últimos años, han experimentado una aceleración notable y que han venido a cambiar el entorno estratégico. Se señala que el orden global y el paradigma socioeconómico liberal se encuentran en un periodo de cambio, sin que aún se haya definido con claridad el nuevo panorama del sistema internacional. Los principales vectores de transformación identificados son: el contexto geopolítico, el entorno socioeconómico, la transformación digital y la transición ecológica.

Igualmente, el sistema de prospectiva de la Unión Europea identifica catorce megatendencias que están moldeando el mundo en el momento de redactar este artículo. Estas incluyen la aceleración del cambio tecnológico y la hiperconectividad, el agravamiento de la escasez de recursos, la naturaleza cambiante del trabajo, una reconfiguración del paradigma de la seguridad, el cambio climático y la degradación ambiental, la continuación del proceso de urbanización, la diversificación de la educación y el aprendizaje, la ampliación de las desigualdades, la expansión de la influencia del este y del sur, el aumento del consumo, los crecientes desequilibrios demográficos, la creciente influencia de nuevos sistemas de gobierno, la relevancia de la migración y los cambios en los desafíos de salud.

Aunque estas tendencias globales y vectores de transformación pueden parecer distantes, sus efectos son palpables en la vida cotidiana y, en ocasiones, de manera dramática. Basta con recordar algunos acontecimientos significativos de los últimos cinco años: la pandemia de 2020, la retirada de tropas occidentales de Afganistán y el regreso al Gobierno de los talibanes en 2021, la invasión rusa de Ucrania en febrero de 2022, el lanzamiento de la IA generativa ChatGPT en noviembre de 2022, el ataque de Hamás en octubre de 2023, el intercambio de misiles entre Israel e Irán en 2024, la victoria de Donald Trump en las elecciones de EE. UU. en noviembre de 2024, la creciente polarización ideológica del nuevo Parlamento Europeo a finales de 2024, la caída del régimen sirio en diciembre de 2024 y el acercamiento del presidente de EE. UU. a Rusia en 2025.

La concentración de estos hechos y circunstancias de relevancia internacional en un periodo tan breve de tiempo nos convierte en testigos directos de un mundo en rápida transformación. Este cambio estructural en el sistema internacional está haciendo temblar las placas tectónicas de nuestra realidad, que, aunque parecían sólidas, se han estado deslizando de manera inadvertida hacia un futuro incierto.

La incertidumbre generalizada que producen estos hechos no hace sino reforzar la percepción del ciudadano de a pie de que el mundo es demasiado complejo para comprenderlo y es imposible analizarlo «racionalmente». Sin embargo, las organizaciones de inteligencia, que tienen como principal misión despejar estas mismas incertidumbres y complejidades para ofrecer los mejores cursos de acción, también se encuentran en mayor o menor medida abrumadas por la tarea.

Con este panorama de fondo, ha cobrado fuerza un concepto estratégico de primer orden, la *Zona Gris*, un espacio dentro del espectro del conflicto que está entre la competencia pacífica y la guerra, caracterizado por la ambigüedad, las estrategias multidimensionales (híbridas), intereses sustanciales en juego y la implementación gradual de estrategias para conseguir objetivos a largo plazo (Jordán, 2018). Este espacio es una zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre Estados (*bona fide*) que, pese a alterar notablemente la paz, no cruzan los umbrales que permitirían o exigirían una respuesta armada (Ministerio de Defensa, 2018).

Este escenario de confrontación ya está identificado por la Estrategia de Seguridad Nacional 2021 en mayor o menor medida, puesto que esta pone en relación las estrategias híbridas con los riesgos y amenazas en varios niveles de correspondencia: muy alta para la tensión estratégica y regional, el espionaje e injerencias desde el exterior, las campañas de desinformación, las amenazas a las infraestructuras críticas, la vulnerabilidad del ciberespacio, la inestabilidad económica y financiera y, por último, la

vulnerabilidad energética. En un nivel menor de relación con las estrategias híbridas, se situarían el terrorismo y la radicalización violenta, la vulnerabilidad del espacio marítimo, la vulnerabilidad del espacio aeroespacial, el crimen organizado y la delincuencia grave y, por último, la proliferación de armas de destrucción masiva.

En este contexto de confrontación en la zona gris en el que los componentes fundamentales de la Seguridad Nacional, concretamente la Defensa Nacional, la Seguridad Pública y la Acción Exterior, están tan interrelacionados, surge una pregunta: *¿es necesaria algún tipo de innovación por parte de los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, para seguir apoyando permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización*? (art. 9 de la Ley de Seguridad Nacional).

La facilidad para formular esta pregunta contrasta con la dificultad para responderla, algo que este artículo no pretende hacer con rigor, sino que busca solo introducir una serie de elementos para alimentar la reflexión estratégica.

2 Ciencia posnormal

Es conocido que el ciclo de Inteligencia comparte con el método científico su enfoque sistemático y analítico, pero difieren en objetivos y aplicación. Mientras la ciencia busca verdades universales mediante el planteamiento inicial de hipótesis falsables y la posterior experimentación reproducible, la Inteligencia genera conocimiento práctico para decisiones urgentes, trabajando con datos incompletos y priorizando la acción sobre la perfección metodológica. Ambos usan procesos estructurados, pero el Ciclo de Inteligencia es más flexible, permitiendo saltar etapas ante emergencias.

En cuanto al contexto y rigor, hay que decir que el método científico exige controles estrictos y replicabilidad, mientras la Inteligencia opera en entornos dinámicos donde la incertidumbre es inherente. Por ejemplo, un científico descartaría datos no verificables, pero un analista de Inteligencia podría usarlos para prevenir una amenaza inmediata asumiendo ciertos riesgos. En esencia, la Inteligencia adapta el rigor científico a realidades donde la velocidad y la utilidad operativa son críticas.

Sin embargo, la distancia entre la Inteligencia y la ciencia parece acortarse en los últimos años. El contexto de cambio al que a diario se enfrentan las organizaciones de Inteligencia también ha sido motivo de discusión científica no tanto desde un punto de vista técnico, sino epistemológico. En las últimas décadas han aparecido planteamientos teóricos y metodológicos

que cuestionan la forma habitual de hacer ciencia, como pueden ser el Modo 2, la ciencia posacadémica y la ciencia posnormal (Jiménez-Buedo and Vielba, 2009).

Durante los últimos tres siglos, de forma progresiva, se puso a la ciencia en un lugar central, atribuyéndole la capacidad de proporcionar evidencia cuantitativa, objetiva y neutral, así como un creciente poder explicativo. El modelo tradicional de resolución de problemas suponía la estricta separación entre hechos (el territorio de la ciencia) y valores (el territorio de la gobernanza), y concebía un proceso en el que, obtenida la verdad, se procedía a la acción política para el bien común. La idea era sencilla: a) cualquier problema práctico-político se puede traducir como un problema técnico-científico y b) la resolución del problema técnico-científico resuelve el problema práctico-político. (Hidalgo y Funtowicz, 2024).

Sin embargo, en el año 1993, Silvio Funtowicz y Jerome Ravetz acuñaron el término ciencia posnormal —CPN— para referirse a una nueva manera de afrontar los problemas científicos en situaciones concretas, situando su enfoque a caballo entre la ciencia y la gobernanza. La CPN se define por cuatro características principales: *los hechos son inciertos; existe una pluralidad de valores, usualmente en conflicto; lo que se pone en juego es potencialmente muy elevado y las decisiones son urgentes*. Como se puede ver, estos presupuestos son los que caracterizan muchos de los entornos de operaciones que los Servicios de Inteligencia y de Información vienen enfrentando desde hace años.

En este enfoque, la atención se desplaza de la búsqueda de una verdad única definida por la ciencia hacia la calidad de los procesos de construcción del conocimiento en relación con un propósito social y políticamente determinado. En este sentido, la CPN reconoce como paritario el conocimiento creado fuera del ámbito científico, incluyendo el conocimiento práctico, la experiencia, asumiendo que no basta solo con «saber qué», sino que también es necesario «saber cómo». Desde esta perspectiva, y en el ámbito de la seguridad y la defensa, podría interpretarse que la CPN estaría poniendo al mismo nivel a los científicos y a los analistas de Inteligencia en lo que a producción de conocimiento de calidad se refiere.

Esta concepción paritaria del conocimiento se materializaría, según los autores, en una «comunidad extendida de pares» o «comunidad extendida de evaluación», que amplía la evaluación de la calidad del conocimiento más allá de los expertos de cada una de las disciplinas científicas. En contextos posnormales, la participación, la inclusión y la diversidad de voces contribuyen a la evaluación de la calidad del conocimiento.

El desafío estaría en cómo crear esta extensión de la comunidad de pares en situaciones de conflicto real, reconociendo que las transformaciones

sociales emergen de estos procesos. La CPN propone una reforma donde la extensión democrática del derecho al conocimiento no solo es ética y políticamente eficaz, sino que también «potencia la calidad de la evidencia tecnocientífica» para la acción orientada al bien común.

En definitiva, la CPN plantea que el modelo moderno de resolución de problemas basado en la predicción y el control es obsoleto. Esto requiere asumir la imposibilidad de predecir y justificar la acción política únicamente sobre predicciones, orientándose hacia una «ciencia de la anticipación responsable» que se ocupe de la calidad de los procesos de funcionamiento de las instituciones. Así, y en última instancia, ante la inevitabilidad del error o la aparición de hechos inesperados, la atención debería centrarse en gestionar los fracasos «con legitimidad político-institucional».

La asunción de cierta inevitabilidad y la imposibilidad de la ciencia para hacer predicciones fiables frente a problemas altamente complejos ya fue apuntada en 2007 por Nassim Nicholas Taleb, quien revitalizó el concepto de «cisne negro» para referirse a eventos raros e impredecibles que tienen un impacto significativo, argumentando que estos eventos son inevitables y que nuestra percepción de ellos cambia después de que ocurran, tendiendo a creer que eran más predecibles o inevitables de lo que, en realidad, eran en el momento en el que se produjeron (sesgo retrospectivo). Además, y al igual que la CPN, este autor apuntó en 2012 que el esfuerzo social debe ir dirigido a reforzar nuestras capacidades para soportar lo impredecible, acuñando el concepto de «antifrágil» para describir sistemas que no solo resisten el caos, sino que también se benefician de él, mejorando en cada iteración de enfrentamiento a la adversidad.

Sin embargo, hay que tener en cuenta que a la metáfora del «cisne negro» se contrapone la del «elefante negro», que describe problemas evidentes y conocidos por todos, con consecuencias potencialmente devastadoras, pero que son ignorados, de manera que la falta de acción o voluntad para enfrentarlos convierte su impacto en una crisis inevitable, ¿podríamos identificar nuestros propios elefantes negros?

Hasta aquí, se podrían extraer algunas conclusiones parciales si se aplica el marco conceptual propuesto por la CPN al contexto de funcionamiento de los Servicios de Inteligencia e Información: a) reforzar la capacidad para generar conocimiento mediante la creación de una comunidad extendida de expertos teóricos y prácticos; b) poner el foco en la calidad de los procesos de generación de conocimiento mientras se asumen las dificultades para predecir la evolución de determinados entornos, y c) que los efectos perjudiciales de la complejidad y la incertidumbre han alcanzado tal nivel que ha sido objeto de estudio científico, lo que demuestra el punto de transformación en el que se encuentra el mundo que nos rodea.

Complementando el marco conceptual de la CPN surge la *Teoría de los Tiempos Posnormales* (Sardar, 2019), que define con más detalle las situaciones de aplicación de la CPN, caracterizándolas por las cuatro S (en inglés) y las tres C:

— 4S: velocidad (todo se acelera), escala (los eventos adquieren una dimensión global), simultaneidad (las crisis ocurren al mismo tiempo) y alcance (penetrando incluso las partes más remotas del planeta).

— 3C: complejidad (sistemas interconectados e interdependientes), contradicciones (demandas contrapuestas e intereses antagónicos) y caos (pequeños eventos pueden desencadenar cambios enormes e impredecibles).

Los tiempos posnormales, según el autor, se manifiestan en diversos ámbitos. En la política, se observa el auge del populismo, la polarización y la crisis de la gobernanza. En la economía, el capitalismo desenfrenado conduce a una creciente desigualdad y a una incertidumbre radical. La tecnología, si bien ofrece oportunidades, también presenta riesgos como la manipulación, la pérdida de privacidad y el aumento del caos. La sociedad se enfrenta a la erosión de la confianza en las instituciones, la fragmentación y la difusión de la posverdad. Incluso la religión experimenta nuevas formas y tensiones en este contexto.

La teoría centra su atención en tres conceptos: la incertidumbre, la ignorancia y el horizonte temporal (los llamados Tres Mañanas), de manera que cada tipo de incertidumbre está intrínsecamente asociado a una categoría específica de ignorancia, lo que ayuda a comprender mejor la naturaleza de lo desconocido en cada horizonte temporal:

— La *Incertidumbre Superficial*, propia del *Presente Extendido*, se vincula con la *Ignorancia Simple*. En este horizonte, si bien la dirección general de los cambios puede ser previsible, se desconoce la magnitud y la probabilidad exactas de los eventos. Esta ignorancia es simple en el sentido de que se refiere a la ausencia de conocimiento sobre aspectos específicos, pero se considera superable a través de la recopilación de información, la investigación y el aprendizaje. Este es el ámbito propio de la ciencia tradicional.

— La *Incertidumbre Poco Profunda*, característica de los *Futuros Familiares*, se relaciona con la *Ignorancia Vencible*. Aquí nos enfrentamos a una amplia gama de futuros posibles y la dirección del cambio es menos clara. La ignorancia es vencible porque, aunque no se sepa qué preguntas hacer en el presente, se reconoce que las respuestas a esas preguntas solo podrán encontrarse en el futuro, a medida que se experimente las consecuencias de las tendencias y los desarrollos actuales. Este es el ámbito propio de la aplicación de

conocimientos adaptados a cada situación por parte de consultores profesionales.

— La *Incertidumbre Profunda*, que define los *Futuros Impensados*, se asocia con la *Ignorancia Invencible*. En este horizonte, se desconoce por completo la naturaleza, la dirección y el impacto de los cambios, y nuestra propia forma de entender el mundo puede ser inadecuada. Esta ignorancia es invencible porque representa la ignorancia de nuestra propia ignorancia, aquello que no se sabe y que está fuera de los marcos de pensamiento convencionales. Abordar esta ignorancia requiere un replanteamiento fundamental de nuestras suposiciones y de la visión del mundo, siendo el ámbito propio de la ciencia posnormal, que recomienda potenciar la generación de conocimiento por parte de comunidades extendidas de expertos que se centren en la calidad de la generación del conocimiento, antes que en la predictibilidad del entorno.

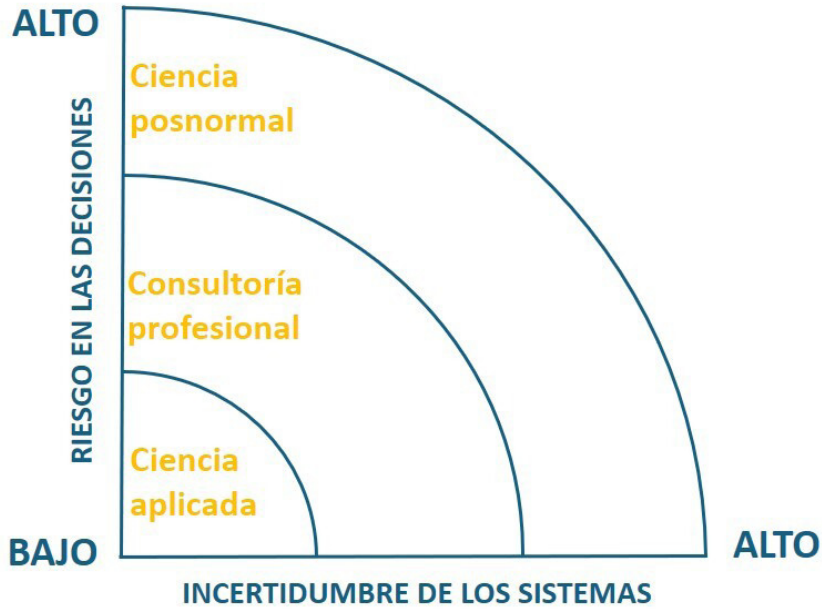


Figura 1: Relación entre incertidumbre y riesgo (elaboración propia)

En resumen, el nivel de profundidad de la incertidumbre refleja el grado en que nuestra ignorancia nos impide comprender el futuro. A medida que nos movemos del Presente Extendido hacia los Futuros Impensados, la incertidumbre se vuelve más profunda y el tipo de ignorancia al que nos enfrentamos se vuelve más fundamental, requiriendo estrategias cada vez más radicales para su comprensión y gestión.

Complementando las conclusiones parciales enumeradas con anterioridad se podría decir: a) que la ciencia posnormal es una especie de «extensión» de la ciencia tradicional; b) que una buena definición de las características de los problemas es clave para determinar la forma de abordarlos, situando las labores de inteligencia entre los límites de la consultoría experta y la ciencia posnormal; c) tratar de utilizar procedimientos propios de la ciencia aplicada a situaciones posnormales puede no ser el mejor enfoque.

3 Del ciclo de la inteligencia a la gestión del riesgo

Para una revisión crítica del ciclo de inteligencia, principal marco conceptual para comprender el proceso de producción de Inteligencia en seguridad y defensa se puede seguir a Javier Jordán (Jordán, 2016). Su análisis reconoce que el modelo del ciclo, a pesar de ser sencillo, lógico y fácil de comprender y recordar, así como de guardar cierta correspondencia con la organización interna de los servicios de inteligencia, es criticado por simplificar en exceso la realidad y no reflejar con precisión el proceso real de producción de inteligencia. El texto señala varias incongruencias entre el modelo ideal y la práctica real, ente otros: a) en la fase de dirección, los objetivos no siempre son claros y a menudo son los técnicos quienes impulsan el proceso; b) las fases de obtención y elaboración no son estrictamente secuenciales, sino que operan de forma paralela e interactiva; c) en la difusión, la información bruta puede llegar a los decisores sin análisis previo, y d) la inteligencia elaborada puede ser ignorada si contradice el marco ideológico del decisor político.

Además, cada fase del ciclo enfrenta limitaciones específicas, como restricciones presupuestarias, problemas de procesamiento de datos, limitaciones legales y dificultades de coordinación. Jordán menciona modelos alternativos, como el modelo de Treverton y Gabbard, que introduce la noción de «atajos» entre las fases; el modelo multiestratos de Lowenthal que subraya la importancia de la retroalimentación continua a lo largo del ciclo y, finalmente, describe la Inteligencia Centrada en el Objetivo (Target-Centric Intelligence) de Clark, que propone un enfoque en red donde todos los participantes colaboran en la construcción de una imagen compartida del objetivo. Los tres modelos alternativos reflejan la complejidad y la naturaleza no lineal del proceso real de Inteligencia. En conclusión, aunque el modelo tradicional del Ciclo de Inteligencia tiene valor pedagógico, es necesario considerar enfoques más flexibles que incorporen la interacción constante y la retroalimentación entre las diferentes etapas para comprender mejor el funcionamiento real de los servicios de Inteligencia.

Por otro lado, hay que decir que en las cuatro fases básicas del Ciclo no se tiene en cuenta el proceso de toma de decisiones en sí mismo, dado

que este acaba con la difusión de la Inteligencia hacia el decisor. Desde un punto de vista conceptual, existiría una clara brecha entre el conocimiento generado para resolver un problema de Inteligencia, las decisiones que se toman para resolverlo y el impacto de las decisiones en el propio problema. Recogiendo la propuesta de Clark, no se podría crear una imagen compartida del problema de Inteligencia si no existe un marco conceptual que englobe a todos los actores intervinientes, incluidos los que toman las decisiones.

Desde un enfoque policial, el Modelo 4-I (Intención, Interpretación, Influencia e Impacto) propuesto por Jerry H. Ratcliffe, desarrolla el marco conceptual para explicar la dinámica entre los actores clave en la producción y aplicación de inteligencia criminal, destacando cómo interactúan analistas, tomadores de decisiones y el entorno criminal (OSCE, 2020).

Figura 2. Modelo 4i (adaptado de Ratcliffe)

Sin embargo, no hay que olvidar que el Ciclo de Inteligencia, en última instancia, está subordinado a un proceso mayor de gestión de la seguridad y la defensa. Es precisamente en este punto donde la ciencia posnormal de Funtowicz y Ravetz plantea una nueva forma de afrontar los tiempos posnormales, justo en el punto donde el conocimiento científico/técnico y la gobernanza se dan la mano. Así, la pregunta no sería tanto ¿si el Ciclo de Inteligencia describe correctamente la actividad de los Servicios de Inteligencia e Información del Estado?, sino ¿cómo establecer un marco conceptual en el que se integre la actividad de estos junto con las actividades de gestión de los problemas de seguridad y defensa?

Una aproximación que puede poner en relación el conocimiento científico/técnico con el de los criterios de gobernanza podría ser la ofrecida por el marco conceptual establecido por la *norma UNE-ISO 31 000 Gestión de Riesgos*. La norma presenta las directrices generales para la gestión de cualquier riesgo por parte de organizaciones públicas o privadas, proponiendo un mapa de procesos.

Aplicando dicho mapa para la gestión por parte del Sistema de Seguridad Nacional (SSN) de los riesgos contemplados en la Estrategia de Seguridad Nacional y, entendiendo que los Servicios de Inteligencia e Información del Estado son un subsistema del SSN, se obtendría un marco conceptual que integraría tanto al subsistema de Inteligencia, como a los decisores y las medidas implementadas para reducir dichos riesgos, facilitando a todos los participantes compartir la misma visión del problema de seguridad a resolver como apuntaba Clark.

Basado en el que propone la norma UNE-ISO 31 000 a continuación se muestra el mapa de procesos (adaptado por el autor) que muestra la interrelación iterativa de procesos y su adaptación al funcionamiento del SSN:

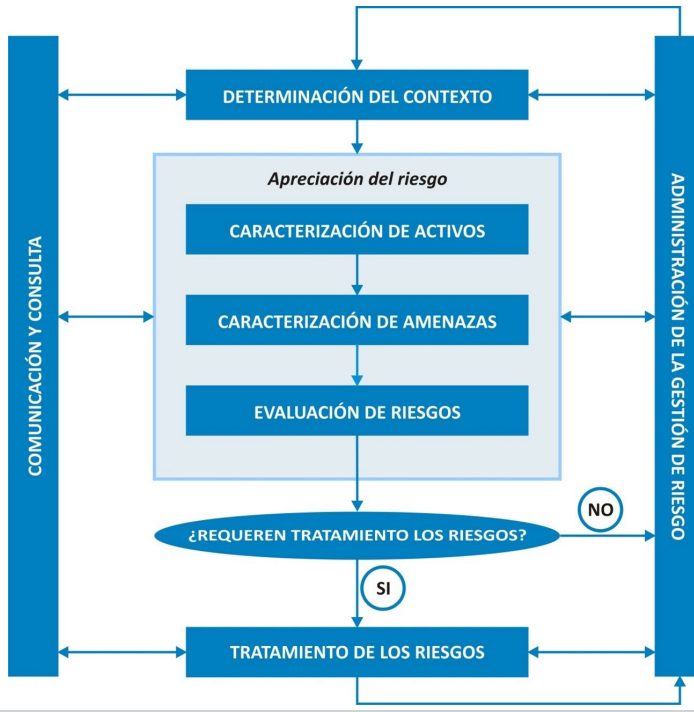


Figura 3: Mapa de procesos de gestión del riesgo (adaptado de norma UNE-ISO 31000)

— *Definición del contexto*: define el alcance de la gestión del riesgo, su ámbito geográfico, temporal y dominio donde se materializan los efectos, considerando factores internos al SSN y externos (entorno estratégico), estableciendo criterios de riesgo (umbrales de tolerancia) para evaluar su importancia, así como la definición de las normas y valores aplicables, también los actores del SSN implicados en cualquiera de los procesos de gestión de ese riesgo en concreto. En este proceso, estaría incluida la fase de Dirección del Ciclo de Inteligencia.

— *Comunicación y consulta*: implica a las partes tanto internas como externas al SSN relacionadas con la obtención e intercambio iterativo de información relevante aplicables al riesgo en cuestión. Este proceso sería asimilable al de Obtención del Ciclo de Inteligencia.

— *Apreciación del riesgo*: medidas de identificación, análisis y valoración del riesgo que puede implicar:

  - Caracterizar activos: identificación, análisis y valoración de los activos en riesgo. Implica determinar la criticidad o importancia relativa de los mismos, así como sus vulnerabilidades, dando lugar a un mapa de activos a proteger.
  - Caracterizar amenazas: identificar, analizar y valorar las amenazas que generan el riesgo. Implicaría la determinación de su peligrosidad, capacidad e intención para materializar el riesgo, dando lugar a un cuadro de amenazas.
  - Evaluar el riesgo, que implicaría establecer las hipótesis pertinentes que ponen en relación el riesgo en cuestión con las amenazas y los activos. La evaluación del riesgo respecto a los criterios establecidos por el SSN permite establecer prioridades de actuación identificando los riesgos que se pueden asumir y aquellos que deben ser tratados.

  Este proceso sería asimilable a la fase de Elaboración del Ciclo de Inteligencia e iría íntimamente ligada a la elaboración de productos de inteligencia para su Difusión a los responsables del siguiente proceso.

— *Administración y Gestión del Riesgo*: proceso en el que los responsables de la gestión y administración del riesgo en sus distintas perspectivas hacen un seguimiento y revisión de este, tomando las decisiones pertinentes apoyados por los informes de inteligencia recibidos.

— *Tratamiento del riesgo*: proceso por el que se establecen las condiciones para aplicar las medidas, así como su propia aplicación, tanto de carácter operativo como estratégico, orientadas a prevenir o

evitar la aparición del riesgo, la protección de los activos, la neutralización de las amenazas, así como las medidas tendentes a reducir los efectos o impacto del riesgo en caso de producirse.

Desde el punto de vista de la gestión pública, la definición de un mapa de procesos único para todo el SSN abre la puerta a establecer políticas claras de calidad en el funcionamiento de cada proceso, con independencia de los actores que participen en cada uno de ellos, lo que sin duda alguna redundaría en la calidad del conocimiento generado, lo que a su vez apunta en la dirección indicada por la ciencia posnormal.

Es importante recordar que el mapa de procesos es un modelo genérico que se aplica a riesgos concretos con sus propias características, de esta forma, se podrían definir los mapas de procesos que fueran necesarios para gestionar los dieciséis riesgos y amenazas priorizados en la Estrategia de Seguridad Nacional.

Sin embargo, desde la perspectiva de la generación de comunidades extendidas de iguales, quedaría por determinar qué actores deberían incorporarse al mapa de procesos, a lo que se tratará de responder más adelante. En todo caso, y sobre todo en una creciente hostilidad en la zona gris donde se entremezclan la Defensa Nacional, la Seguridad Pública y la Acción Exterior, parece prioritario la intensificación de la colaboración entre todos los Servicios de Inteligencia y Seguridad del Estado.

4 Inteligencia y cognición

Otro de los campos en los que el desarrollo científico ha favorecido la innovación en lo que a producción de Inteligencia se refiere ha sido las ciencias cognitivas. La analogía del ordenador, ampliamente utilizada desde hace décadas, compara el funcionamiento de la mente humana con el de una computadora, sugiriendo que ambos sistemas procesan información de manera similar. Esta analogía, cuestionada desde algunos aspectos, ha servido de modelo conceptual para numerosos avances en las ciencias cognitivas que, en el ámbito de la Inteligencia, han tenido un especial impacto en la fase de Elaboración. A continuación, se hacen algunas reflexiones al respecto, apuntando ciertas vías de mejora, que, en términos generales, ya se han iniciado. Para ello, se hará una breve mención a los sesgos cognitivos, el pensamiento sistémico, los modelos mentales y la conciencia situacional.

4.1 Sesgos cognitivos

Siguiendo la tesis doctoral de Claudio Payá (Payá Santos, 2017) sobre los sesgos cognitivos del analista de Inteligencia, se puede decir que los sesgos cognitivos son errores sistemáticos y predecibles en el procesamiento de la información, inherentes a la estructura de la mente humana y

que pueden afectar la objetividad del análisis. Estos sesgos no son simples errores aleatorios, sino patrones de pensamiento que pueden conducir a conclusiones erróneas, incluso cuando el analista es consciente de su posible influencia.

Es importante resaltar el trabajo de Herbert Simon y el concepto de «racionalidad limitada», que desafió los límites de la racionalidad humana, demostrando que las personas no siempre optan por la elección que maximiza sus intereses. Simon argumentó que, frente a la complejidad del mundo, los seres humanos no pueden alcanzar un ideal de racionalidad perfecta y que, en lugar de ello, las personas utilizan diversas estrategias para simplificar su entorno. Más adelante, los trabajos de Kahneman y Tversky sobre heurísticos y sesgos abundaron en los límites de la racionalidad proponiendo dos sistemas de razonamiento:

— *Sistema Uno*: intuitivo, rápido e inconsciente, basado en heurísticas y emociones, que opera automáticamente, proponiendo respuestas rápidas al Sistema Dos y que es propenso a errores sistemáticos o sesgos.

— *Sistema Dos*: deliberado, lento y consciente, basado en la lógica y el esfuerzo cognitivo. Aunque más preciso, también está limitado por la capacidad mental. Un Sistema Dos perezoso hace que se racionalicen directamente las propuestas automáticas generadas por el Sistema Uno.

En el contexto del análisis de Inteligencia, estos sesgos pueden tener un impacto significativo. Pueden llevar a un cierre prematuro, donde los analistas llegan a conclusiones rápidamente sin explorar todas las posibilidades. La presencia de incertidumbre, la posibilidad de engaño por parte de adversarios y la tendencia a buscar información que confirme las hipótesis preexistentes (sesgo de confirmación) son factores que exacerban la influencia de los sesgos. La presión del tiempo y la necesidad de precisión también pueden intensificar estas limitaciones cognitivas.

Para mitigar el impacto negativo de los sesgos cognitivos en el análisis de inteligencia, se suelen utilizar las *Técnicas de Análisis Estructurado (TAE),* ampliamente difundidas desde 2011 gracias a la obra de Richards J. Heuer y Randolph H. Pherson. Estas técnicas están diseñadas para hacer más transparentes los argumentos analíticos, las suposiciones y las lagunas de inteligencia, ayudando a prevenir respuestas automáticas que puedan comprometer la solidez del análisis. Las técnicas, que tienen distintas aplicaciones, proporcionan un marco estructurado y están diseñadas para: descomponer problemas complejos en pequeños problemas de análisis más manejables; explicitar el proceso de análisis para convertirlo en un trabajo colaborativo; desafiar las hipótesis de trabajo, forzando una

justificación consciente de las conclusiones, forzando la incorporación de hipótesis alternativas; estimular la capacidad de prever e imaginar lo inesperado, impulsando la consideración de nuevas perspectivas e ideas para evitar el pensamiento único, etc.

Si bien es verdad que las TAE han venido a proporcionar una buena caja de herramientas a los analistas de Inteligencia, no es menos cierto que por mucha pericia que tenga, un albañil necesita de un arquitecto para tener la visión global del proyecto en el que está trabajando. Esta globalidad nos lo proporciona el pensamiento sistémico.

4.2 Pensamiento lineal vs. sistémico

Otra de las limitaciones del sistema cognitivo humano es la tendencia al pensamiento lineal. Sin embargo, en este contexto de creciente complejidad global, la manera en que se abordan y se resuelven problemas ha cobrado una importancia crítica. El pensamiento lineal, caracterizado por un enfoque secuencial y analítico, ha sido el paradigma dominante durante décadas. No obstante, el pensamiento sistémico, que considera las interrelaciones y los patrones emergentes, ha ganado prominencia como una alternativa más holística y global. Los resultados indican que el pensamiento lineal es más efectivo en problemas bien definidos y de alcance limitado, mientras que el pensamiento sistémico muestra ventajas significativas en la resolución de problemas complejos e interconectados, sobre todo cuando existe un enfoque transdisciplinar (Lorenzo-Penalva, 2023).

La Teoría General de Sistemas, base del pensamiento sistémico, fue desarrollada por Ludwig von Bertalanffy en la década de 1940 y formalizada en 1969, proponiendo una visión holística de los sistemas naturales y sociales. Este biólogo austriaco concibió un enfoque interdisciplinario que considera los sistemas como conjuntos de elementos interrelacionados, enfatizando las propiedades emergentes que surgen de estas interacciones: el sistema es más que la suma de sus partes.

El modelado de un sistema empieza por establecer su estructura, identificando primero sus elementos de forma analítica (descomposición), para, posteriormente, establecer las relaciones entre los mismos en un esfuerzo de síntesis (integración). Estas relaciones se suelen representar mediante un diagrama de influencias, positivas o negativas, hasta el punto de que casi todo lo que nos rodea se puede entender como un sistema, e incluso como un sistema dentro de un sistema mayor (sistemas anidados).

Observando detenidamente un sistema, se pueden identificar bucles de realimentación, ya sean positivos o negativos. Un bucle de realimentación no deja de ser una cadena cerrada de influencias que empiezan y acaban en una misma variable. Un bucle de realimentación positiva tiende

a desestabilizar el sistema hasta que encuentra algún tipo de límite, generalmente un bucle de realimentación negativa, que tiende a estabilizar el sistema. Esta visión no lineal de los sistemas permite empezar a intuir la complejidad de estos, a la que se suma el retardo que los impactos de unas variables tienen en otras (Aracil J, 1995).

Esta metodología se ha aplicado para el análisis de problemas de seguridad, como la lucha contraterrorista (Pajares de Mena, 2010). Por ejemplo, tomando la variable «oportunidad política» definida por Sidney Tarrow para explicar el surgimiento y fortalecimiento del terrorismo como variable explicativa (Tarrow, 1994), se puede definir un sistema básico de confrontación terrorista/antiterrorista en el que las variables que conforman las capacidades terroristas constituyen el bucle de realimentación positivo que desestabiliza el sistema dado que: a más desestabilización (oportunidad política para los terroristas)→ más radicalización→ más capacidad terrorista→ más ataques → más desestabilización. Por otro lado, el bucle de realimentación negativo, formado por las variables que soportan las capacidades contraterroristas, establece básicamente que: a más desestabilización (oportunidad política para los terroristas)→ más capacidades contraterroristas→ menos capacidades terroristas→ menos ataques→ menor desestabilización. En el caso de ETA, la variable de salida, n.º de víctimas mortales, mostraría el estado del sistema caracterizado por una gráfica sigmoidal, inicialmente ascendente cuando prima el bucle positivo terrorista y descendente cuando prima el bucle negativo contraterrorista (Penalva Lucas, 2023).

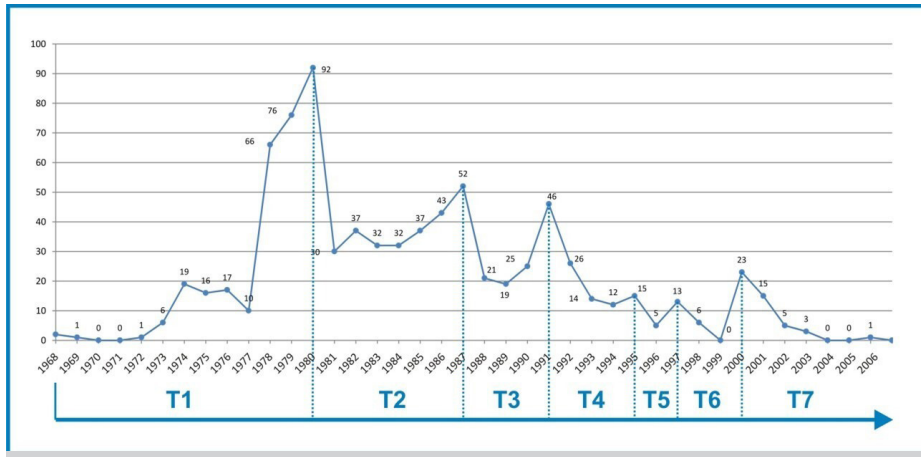


Figura 4: Víctimas mortales de ETA (elaboración propia)

Por otro lado, la dinámica de sistemas, especialmente los equilibrios inestables entre bucles de realimentación positivos y negativos, proporciona la metodología para explicar el hecho de que tras las revueltas árabes que se iniciaron a finales de 2010, surgiera la conformación de una

ventana de oportunidad para que surgiera DAESH, el grupo terrorista más letal conocido hasta la fecha. El surgimiento de una nueva «oportunidad política», en términos de Tarrow, ocasionada por dichas revueltas hicieron que los equilibrios terrorismo/contraterrorismo conseguidos hasta la fecha en algunos países del mundo árabe se vieran rápidamente modificados.

La desaparición, transformación o reducción de capacidades de los aparatos de seguridad de algunos de estos países supuso la desaparición de los límites de contención de una actividad terrorista latente en la zona. A la inestabilidad social y política generada por las revueltas en esos países, los grupos terroristas añadieron su propia desestabilización, realimentando el sistema hasta el punto llevar el caos a niveles de guerra civil en alguno de ellos. Por su parte, los aparatos de seguridad de estos países, incapaces de compensar las dinámicas ya generadas, tuvieron que ser apoyados por la Comunidad Internacional para contener la insurgencia terrorista, sobre todo, en Siria/Irak.

Los retardos en la toma de decisiones y en las estrategias a seguir, la falta de compromiso internacional inicial por la cantidad de recursos necesarios para gestionar de forma eficaz las distintas crisis, así como la incorporación de actores internacionales con sus propias dinámicas enfrentadas como Irán-Arabia Saudí, EE. UU. y Rusia, ofrecieron al yihadismo internacional el tiempo suficiente (retardo) para configurarse y adaptarse a una nueva realidad dando como resultado el surgimiento de DAESH.

Por otro lado, hay que considerar que las lógicas acción-reacción, relativamente simples en el caso de un sistema terrorista/contraterrorista, favorecen, en cierta manera, la predicción de la evolución del sistema. Sin embargo, si se quiere determinar la estructura de un sistema más complejo y ser capaz de predecir en cierto modo su comportamiento futuro, es importante establecer las normas que rigen las relaciones entre sus partes, así como las limitaciones existentes. Un buen ejemplo pueden ser las relaciones sistémicas que se pueden encontrar en el plano de las *relaciones internacionales*, en el que el motor de la dinámica del sistema internacional se verá condicionado por las relaciones de poder relativo entre los distintos actores componentes de este. Siguiendo las tesis neorrealistas de Kenneth Waltz, el sistema se mantendrá estable en la medida en que las estrategias de los actores sean estables porque no haya incentivos para cambiarlas, considerando las acciones de los demás. Los principios que regirían el sistema de relaciones internacionales (Jordán, 2022) son básicamente:

1. Anarquía: la ausencia de una autoridad central es el principio ordenador del sistema internacional. Esto significa que no hay una autoridad que regule las relaciones entre los Estados, lo que lleva a un entorno de autodefensa donde cada Estado debe asegurar su propia supervivencia.

2. Unidades Funcionalmente Similares: los Estados son unidades funcionalmente similares, ya que no se especializan en funciones específicas como lo hacen en sistemas jerárquicos. Esto se debe a que ningún Estado quiere depender de otros para su supervivencia.
3. Distribución de Capacidades: la estructura del sistema internacional también se define por la distribución de capacidades entre los Estados. Esta distribución puede ser bipolar, multipolar o unipolar, lo que afecta a la estabilidad del sistema.
4. Seguridad como Objetivo Principal: los Estados buscan asegurar su supervivencia y seguridad por encima de otros objetivos. Esto limita la cooperación y crea competencia por la seguridad.
5. Equilibrio de Poder: los Estados tienden a equilibrar el poder entre sí para mantener la estabilidad en el sistema internacional.

Independientemente de la existencia de otros modelos sobre relaciones internacionales, el modelo de Waltz ayuda a ejemplificar el modelado de sistemas complejos de los que se pueden derivar problemas de seguridad, pero que vienen sustentados por un marco conceptual previo que determina las normas de funcionamiento del sistema establecidas por la investigación científica. En este sentido, la modelización basada en modelos conceptuales sólidos es básica.

4.3 Modelos mentales vs. modelos conceptuales

Relacionado con el apartado anterior, hay que tener en cuenta desde el punto de vista cognitivo los *modelos mentales*, que son representaciones internas y personales de la realidad externa que utilizan los individuos para comprender el mundo, razonar y tomar decisiones. Son construcciones idiosincráticas, incompletas, inestables y básicamente funcionales que se basan en la percepción individual y están influenciados por factores como la experiencia, el conocimiento previo, las creencias y las emociones del analista. Su principal objetivo es la funcionalidad, lo que a menudo prima sobre la exactitud. En contraste, los *modelos conceptuales* son representaciones externas, bien delimitadas, definidas y compartidas por una comunidad científica. Son coherentes con el conocimiento aceptado por esa comunidad y se distinguen de los modelos mentales por su carácter objetivo y consensuado.

En el análisis de Inteligencia, los analistas, de forma inevitable, elaboran y emplean modelos mentales para simplificar la complejidad de la realidad. Sin embargo, esta misma característica puede convertirse en una fuente significativa de error, puesto que la naturaleza subjetiva

e incompleta de los modelos mentales puede llevar a que diferentes analistas desarrollen representaciones distintas de un mismo fenómeno. Además, la resistencia al cambio de estos modelos puede dificultar la adaptación a nueva información, provocando que se ignoren o se interpreten de forma sesgada datos que no encajan con el modelo preexistente. Este sesgo de confirmación puede llevar a los analistas a sobrevalorar la información que confirma sus modelos y a descartar la que los contradice. En última instancia, el uso de modelos mentales incompletos, limitados o inadecuados puede conducir a hipótesis, estimaciones y predicciones erróneas, lo que puede resultar en fallos de Inteligencia con graves consecuencias.

Por lo tanto, es crucial que los analistas sean conscientes de sus propios modelos mentales y de cómo estos pueden influir en su análisis. En este sentido, la solución propuesta se centra en el entrenamiento para reconocer los propios modelos mentales, comprender cómo influyen en el procesamiento de la información, mantener una mente abierta, cuestionar las creencias y valorar diferentes perspectivas (Antonio Martínez-Sánchez, 2014) y, sobre todo, incorporar modelos conceptuales sólidos generados por la comunidad científica y compartirlos con la Comunidad de Inteligencia.

4.4 Conciencia situacional

Como última referencia al ámbito cognitivo tras los sesgos, el pensamiento sistémico y los modelos mentales, hay que hablar de la conciencia situacional (CS) que afecta fundamentalmente a los responsables de la toma de decisiones. Para ello, se sigue el modelo de Mica Endsley (Endsley, 2000) que la define como «la percepción de los elementos en el entorno dentro de un volumen de tiempo y espacio, la comprensión de su significado y la proyección de su estado en el futuro cercano», de tal manera que la CS es un estado de conocimiento crucial para una toma de decisiones eficaz en entornos dinámicos. Sin embargo, hay que decir que la CS es un estado de conocimiento separado de la toma de decisiones ya que es posible tener una CS perfecta y tomar una decisión incorrecta, o viceversa. A pesar de todo, una buena CS aumenta la probabilidad de tomar buenas decisiones. También hay que decir que el verdadero reto radica en encontrar la información necesaria cuando se necesita, asumiendo que más datos no equivale a más información.

Si bien es cierto que el concepto de CS es muy usado en tareas con un alto componente de destrezas motrices y rendimiento en entornos muy dinámicos, como pilotos, controladores aéreos y medicina, la aplicación que se va a hacer de la CS está más enfocada hacia una CS de los decisores que tienen que resolver problemas de seguridad. La CS se estructura en tres

niveles interdependientes en los que los elementos cognitivos tienen un gran peso:

— Nivel 1: percepción de los elementos en la situación actual. Este nivel implica la detección y monitorización de la información relevante del entorno por parte del decisor, que no está libre de sesgos.

— Nivel 2: comprensión de la situación actual. Este nivel va más allá de la simple percepción e implica la integración, interpretación y evaluación del significado de los elementos percibidos en relación con las metas y objetivos del decisor.

— Nivel 3: proyección del estado futuro. El nivel más alto de CS implica la capacidad de anticipar eventos y dinámicas futuras basándose en la comprensión actual de la situación, lo que permitiría una toma de decisiones oportuna en el momento actual, pero anticipando sus efectos sen el futuro inmediato.

En el corazón del modelo de Endsley, se encuentran los modelos mentales, que, como ya se ha dicho, son estructuras de conocimiento almacenadas en la memoria a largo plazo que representan la comprensión de un individuo sobre un sistema o entorno y las relaciones entre sus componentes. Además de guiar la atención (Nivel 1) y facilitar la distinción entre las señales de interés y el ruido, los modelos mentales proporcionan un marco para la interpretación y la integración de la información percibida, facilitando la comprensión (Nivel 2), ayudando a determinar la relevancia de la información en relación con las metas. Los modelos mentales también son esenciales para la proyección (Nivel 3), ya que permiten anticipar estados futuros del sistema basándose en su estado actual y la comprensión de su dinámica interna.

Con todo, los esfuerzos deben ir encaminados a mejorar de manera continua la CS de los decisores, abordando estos factores cognitivos y apoyando la interiorización de modelos conceptuales precisos y adaptativos. Si bien, hay que ser consciente de que la labor va a ser especialmente compleja, si no imposible, en circunstancias posnormales cuando los hechos son inciertos; existe una pluralidad de valores en juego, usualmente en conflicto; lo que se pone en riesgo es potencialmente muy elevado; y las decisiones son urgentes.

5 Sistemas evolutivos

Llegados a este punto, parece claro que los Servicios de Inteligencia e Información del Estado deben transformarse y adaptarse al nuevo entorno de operaciones tal y como vienen haciendo desde hace años. Quizá uno de los casos más claros sea cómo España ha luchado contra el terrorismo

desde sus inicios en el siglo XIX, evolucionando para enfrentar las oleadas terroristas identificadas por Rapoport que han afectado a nuestro país: la anarquista (siglos XIX-XX), la de la nueva izquierda (segunda mitad del XX) y la religiosa (siglo XXI).

Sin embargo, las características de los tiempos posnormales, como la velocidad, la escala, simultaneidad y alcance de los cambios (4S), así como la complejidad, contradicciones y el caos (3C) que lo acompañan, hacen dudar del alcance y velocidad de la transformación necesaria para adaptarse a un entorno tan incierto.

Ante la incertidumbre que acompaña a la situación, puede ser útil seguir al prospectivista Jan Huston y su *Teoría de los Sistemas Evolutivos* (Huston, 1992, 2005) que postula que todos los sistemas en evolución, como los biológicos o sociales, experimentan cambios y transformaciones siguiendo una secuencia fundamental de cinco etapas:

— *Emergencia*: el inicio o aparición de un nuevo sistema.

— *Desarrollo*: un periodo de crecimiento y organización interna del sistema.

— *Madurez*: la fase en la que el sistema alcanza un estado de funcionamiento óptimo dentro de sus parámetros existentes.

— *Desestabilización*: una etapa caracterizada por el aumento de la complejidad interna y la creciente dificultad para mantener la estabilidad. Se identifican situaciones *críticas*, en las que el sistema es cada vez más sensible a los cambios, y *supercríticas*, en las que el sistema experimenta una complejidad excesiva e inmanejable.

— *Ruptura Transformacional*: un punto crítico donde el sistema se transforma, lo que puede resultar en su extinción o en el surgimiento de un sistema nuevo y diferente. Las opciones de transformación se limitan a tres niveles: superior (con potencial para una nueva secuencia evolutiva), lateral e inferior (ambas conduciendo a la extinción a diferentes ritmos).

En el caso que nos ocupa, se asume que los Servicios de Inteligencia e Información del Estado, entendidos como un subsistema del SSN, estarían saliendo de una fase de Madurez hacia una fase de Desestabilización ocasionada por el nuevo entorno estratégico, marcado por una reorganización del Sistema Internacional y una creciente tensión geopolítica que está afectando a los sistemas de seguridad, defensa e inteligencia a nivel europeo y mundial.

Antes de la ruptura transformacional, un sistema desestabilizado atraviesa fases de criticidad y supercriticidad, volviéndose cada vez más

sensible a los cambios internos y externos hasta experimentar una complejidad excesiva. Durante la fase supercrítica, el tipo de acciones predominantes determina el resultado de la transformación:

— *Acciones de Optimización*: se centran en explotar el funcionamiento del sistema existente con las mismas acciones conservadoras que llevaron a la supercriticidad. Esto limita las opciones transformacionales a niveles laterales o inferiores, conduciendo eventualmente a la extinción.

— *Acciones de Amplificación*: implican la exploración de acciones nuevas o novedosas para posibilitar opciones de alcanzar un nivel superior, caracterizadas por nuevas estructuras organizativas y simplificación de procesos capaces de absorber la complejidad.

En los sistemas evolutivos, procesar información es vital para la adaptación: mayor capacidad de análisis permite anticipar cambios y diseñar respuestas flexibles. Cuando un sistema alcanza un umbral crítico (sobrecarga informativa o incompatibilidad con estructuras existentes), se desestabiliza, generando caos que fuerza su reorganización en un orden más complejo. La desestabilización no es un fracaso, sino una fase de innovación donde el sistema evoluciona al ser capaz de integrar y gestionar de forma eficiente cada vez más información.

Algunos autores apuntan a conceptualizar las amenazas a la Seguridad Nacional como sistemas complejos sociales, proponiendo el uso de técnicas analíticas estructuradas (TAE), el modelado de sistemas y la inteligencia artificial (IA) como principales herramientas para su estudio (Gil Armario, 2024). Considerando que las amenazas actuales se caracterizan por su dinamismo, interdependencia, complejidad tecnológica y estrategias híbridas, el autor apunta a un cambio de paradigma en la inteligencia, en el que se pase de un modelado de los sistemas de forma cualitativa mediante TAE a un modelado mixto, mediante el modelado asistido por IA y con equipos multidisciplinares para enfrentar los desafíos del siglo XXI.

En este punto, surgen varias preguntas: ¿qué tipo de acciones deberían adoptar los Servicios de Inteligencia e Información del Estado para evolucionar hacia estados superiores de eficiencia que garanticen su adaptación? ¿acciones de *optimización?*, es decir, más de lo mismo mediante pequeños avances incrementales ¿acciones de *amplificación* mediante cambios más disruptivos y atrevidos? ¿Sabríamos distinguir qué medidas son de un tipo y de otro? ¿es suficiente con la integración de la IA en los procesos de trabajo? ¿más TAE? ¿mejores modelos conceptuales? ¿mejor modelado de sistemas complejos? ¿un nuevo mapa de procesos de gestión del riesgo? ¿una reestructuración de los Servicios de Inteligencia e Información del Estado?

6 Un nuevo paradigma en la Inteligencia

Desde posiciones ajenas a la ciencia posnormal, son varias las voces que reclaman desde hace años una revisión del marco conceptual sobre el que se ha venido sustentando la Inteligencia tradicional (Lahneman, 2010) (Arcos, Antón, 2010), si bien recientemente se han recogido esas y otras aportaciones (Ivars Pérez, 2023), para apuntar propuestas sobre un nuevo paradigma de inteligencia, sin embargo, en la exposición se seguirá, en especial, a Lahneman.

En el ámbito de la seguridad y la defensa, la Inteligencia ha sido históricamente una herramienta crucial para los Estados en la garantía de su supervivencia y la consecución de objetivos políticos. Sin embargo, las amenazas a los Estados han evolucionado significativamente a lo largo del tiempo, influenciadas por el devenir histórico, los avances tecnológicos y eventos trascendentales como el fin de la Guerra Fría y la globalización. Esta situación ha llevado a que diversos autores hayan concluido que el paradigma tradicional de la Inteligencia está obsoleto y es necesario uno nuevo.

La Inteligencia tradicional o Viejo Paradigma se desarrolló de manera significativa durante la Guerra Fría y la labor de los analistas se asemejaba a la resolución de un rompecabezas centrado en el descubrimiento de secretos, con un interés limitado en la información de fuentes abiertas. Las amenazas, originadas por adversarios estatales con pautas de comportamiento simétricas y nítidas, hacían que predominara la Inteligencia militar.

Sin embargo, el contexto actual, debido a su complejidad, contradicción y caos, difiere sustancialmente del periodo de la Guerra Fría. El concepto de seguridad se ha ampliado para integrar factores económicos, migratorios, informativos, energéticos, etc. Las amenazas han devenido transnacionales y multicausales, con actores estatales, no estatales e incluso institucionales, lo que dificulta la distinción entre amenazas internas y externas. La velocidad del cambio es alta y la predictibilidad baja, lo que exige una adaptación de los métodos de Inteligencia.

Ante este nuevo escenario, Lahneman plantea un Nuevo Paradigma de la Inteligencia, basado en la interpretación adaptativa de la información, en un enfoque más proactivo, multidisciplinar y cooperativo. Ello implica la construcción de modelos complejos con información principalmente procedente de fuentes abiertas, lo que requeriría extender la comunidad de Inteligencia y la inclusión de diversos actores de la Administración Pública, la sociedad civil y el mundo empresarial para lograr un enfoque holístico e integrador en el análisis de la realidad, lo que supondría un alto nivel de intercambio de información de forma voluntaria y una gran confianza mutua. El autor apuesta por la integración de dos flujos principales de información, la tradicionalmente secreta proporcionada por la comunidad de Inteligencia

y otro flujo de información abierta pero evaluada, de manera que resulte en información confiable de alto valor. En definitiva, Lahneman destaca el dilema entre el secreto del paradigma tradicional y la apertura necesaria para una interpretación adaptativa de una realidad que evoluciona rápido y que deja un gran rastro de información útil al alcance de todos.

Por su parte, otros autores han fusionado las ideas de Lahneman con los conceptos de los tiempos posnormales (Serra and Sardar, 2017), dando como resultado una síntesis interesante que da una conclusión clara, la necesidad de ampliar el número de actores implicados en la producción de inteligencia. Si por un lado la ciencia posnormal reconoce como paritario el conocimiento creado fuera del ámbito científico, incluyendo el conocimiento práctico, por otro Lahneman aboga por ampliar la comunidad de Inteligencia fusionando información procedente de fuentes abiertas con alto valor añadido.

7 El ámbito cognitivo como activo a proteger

Por último, se introduce un último elemento de discusión en cuanto a la necesidad de transformación de los Servicios de Inteligencia e Información del Estado se refiere: *el ámbito cognitivo*. El nuevo entorno de operaciones se caracteriza por la incorporación del ámbito cognitivo a los dominios de operaciones, sumándose al terrestre, aeroespacial, marítimo y ciberespacio. En esencia, se puede considerar el multidominio como un concepto innovador que EE. UU. desarrolló para adaptarse a los nuevos escenarios operativos, en los que hay que coordinar los efectos de las distintas capacidades militares en distintos planos o dominios para alcanzar ventajas operacionales o estratégicas (Gutierrez de León, 2023).

Por su parte, la doctrina de las Fuerzas Armadas concibe el ámbito cognitivo como «[...] el ámbito intangible inherente al ser humano, considerado de forma individual, socializada u organizada y es consustancial a su capacidad de juicio y de toma de decisiones. Este ámbito alcanza a las voluntades de todas las personas afectadas por el conflicto y a los sistemas de inteligencia artificial, por lo que impregna al resto de ámbitos. Su principal limitación es que para operar en él se manejan aspectos intangibles y de difícil evaluación, como los valores, las percepciones, la conciencia, las actitudes y los prejuicios. Se entiende por percepción la interpretación subjetiva, elaboración personal o representación mental, fruto de la interiorización de la información y los estímulos recibidos del entorno. Este ámbito permite a las Fuerzas Armadas alcanzar objetivos que quedan fuera del alcance de otros, mediante el empleo de técnicas de comunicación, la ciencia psicológica y otras ciencias sociales.» (Ministerio de Defensa, 2018).

Su introducción en la discusión no atiende a la necesidad de desarrollar operaciones militares en el ámbito cognitivo, para lo que se puede seguir

a Donoso (Donoso, 2020), sino por la necesidad de adaptar las capacidades del SSN para protegerlo, habida cuenta de que el sistema de creencias y valores de una sociedad democrática es uno de sus principales activos. El ámbito cognitivo, fortaleza de las democracias liberales, ha devenido en vulnerabilidad en el contexto de la revolución digital, lo que está siendo aprovechado por actores hostiles en un contexto de confrontación en la zona gris. Así, la adaptación de los Servicios de Inteligencia e Información del Estado a este nuevo entorno es crucial; debiendo encontrar estrategias efectivas para gestionar los riesgos de desinformación, radicalización, polarización, desafección política, pérdida de confianza en las instituciones, negacionismo científico, etc., todo ello en un contexto de libertad ideológica propio de una democracia liberal, lo que lo convierte en un auténtico desafío posnormal a nuestra seguridad.

8 Conclusiones: escenarios de innovación

Al principio del artículo nos preguntábamos si es necesaria algún tipo de innovación por parte de los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, para seguir apoyando permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización. En mi humilde opinión, que representa solo al autor y no a la institución a la que pertenece, durante el artículo se han identificado varias vías de mejora, muchas de ellas complementarias.

Dada la creciente hostilidad en la zona gris, donde se entremezclan la Defensa Nacional, la Seguridad Pública y la Acción Exterior, parece prioritaria la intensificación de la colaboración entre todos los Servicios de Inteligencia y Seguridad del Estado.

Si se asumen mínimamente los planteamientos posnormales se podría reforzar la capacidad para generar conocimiento mediante la creación de una comunidad extendida de expertos teóricos y prácticos; poner el foco en la calidad de los procesos de generación de conocimiento mientras se asumen las dificultades para predecir la evolución de determinados entornos y; aprender a identificar los tipos de incertidumbre a los que nos enfrentamos para adecuar las estrategias a seguir. En este sentido, sería interesante explorar el papel que la Oficina Nacional de Asesoramiento Científico (ONAC) podría llegar a tener, si bien es cierto que se tendría que complementar con la colaboración con los departamentos de seguridad e inteligencia de sectores estratégicos, muchos de ellos de carácter privado.

Desde el punto de vista de la gestión de procesos, resultaría interesante encontrar un punto de unión entre las actividades de Inteligencia (Ciclo de Inteligencia) y la gestión de los problemas de seguridad (gobernanza), centrando la atención en la calidad de los procesos de elaboración de conocimiento. En este sentido, el enfoque de la gestión del riesgo puede ser una vía que explorar, permitiendo el modelado de un sistema de riesgos interrelacionados que favorecería la conciencia situacional.

En lo que a Inteligencia y cognición se refiere, la reducción del impacto de las limitaciones cognitivas vendría de la mano de las TAE; las mejoras en la modelización de los sistemas, especialmente con la ayuda de la IA y; la incorporación de marcos conceptuales sólidos que puedan ser compartidos por los Servicios de Información e Información del Estado. Todo ello iría encaminado a mejorar no solo la elaboración de Inteligencia, sino la construcción de una consciencia situacional en el decisor que favorezca la toma de decisiones más adecuadas a cada situación.

En lo que se refiere al estado evolutivo de la Comunidad de Inteligencia española, está claro que todos sus componentes están tratando de adaptarse a un nuevo entorno estratégico. En este sentido, la innovación mediante avances incrementales parece una estrategia viable en circunstancias normales, pero se corre el riesgo de que los tiempos posnormales nos sorprendan con los deberes a medio hacer y con poco tiempo para reaccionar. Por otro lado, los cambios arriesgados y disruptivos tampoco son propios en la Administración Pública, donde la vocación de continuidad y estabilidad es un valor seguro que garantiza el funcionamiento del Estado a largo plazo. En todo caso, más allá de las adaptaciones de cada actor, la respuesta global del SSN no puede ser más que sistémica y debe tener en cuenta creciente interacción de los componentes fundamentales de la Seguridad Nacional en un contexto de creciente hostilidad que no se ve en Europa desde hace ochenta años.

En cuanto al equilibrio de información cerrada/abierta, el uso de fuentes abiertas para elaborar Inteligencia, tanto operativa como estratégica, se ha incrementado sobremanera en los últimos años, si bien resulta interesante la propuesta de aumentar la reserva de Inteligencia mediante expertos ajenos a la Comunidad de Inteligencia, generando un flujo de información confiable de carácter abierto.

Por último, dada la creciente importancia del ámbito cognitivo en las estrategias híbridas que se desarrollan en la zona gris, se propone la mejora de la protección del ámbito cognitivo en un contexto de revolución digital, desarrollando estrategias adaptadas a una sociedad liberal democrática que permitan gestionar adecuadamente los riesgos de desinformación, radicalización, polarización, etc.

Llegados a este punto, se pueden resumir una serie de vectores de innovación que pueden orientar el futuro de transformación de los Servicios de Inteligencia e Información del Estado:

- Integración de procesos de Inteligencia y gobernanza: gestión del riesgo como marco conceptual de las políticas públicas de seguridad.
- Foco en lo que se puede hacer (elefantes negros) y no tanto en lo que es difícil de predecir (cisnes negros): calidad y resiliencia de los procesos de Inteligencia.
- Marcos conceptuales sólidos compartidos por la Comunidad de Inteligencia.
- Gestión de las incertidumbres (superficial, poco profunda y profunda) de la manera más idónea: ciencia aplicada vs. posnormalidad.
- Integración de las ciencias cognitivas: TAE, modelado de sistemas, etc.
- Integración de procesos y mejora de la Conciencia Situacional de los decisores.
- Comunidades extendidas de Inteligencia.
- Simplificación y eficiencia de las estructuras de Inteligencia.
- Ámbito cognitivo como nuevo ámbito de confrontación: mejora de las capacidades de análisis y estrategias de acción en entornos democráticos.
- Fusión de capacidades de Inteligencia en la zona gris: coordinación y colaboración de los componentes fundamentales de la Seguridad Nacional.
- Innovación tecnológica: especialmente integración de la IA en procesos rutinarios, modelado de sistemas, etc.
- Flujos de información: generación de conocimiento mediante fuentes abiertas confiables.

Muchos de estos vectores de innovación ya forman parte de las líneas de acción de los Servicios de Inteligencia e Información del Estado, si bien, otros posiblemente no. La combinación de estos vectores ya sea de forma incremental o mediante saltos disruptivos pueden llegar a generar tres escenarios (Curry y Hodgson, 2008):

1. **Horizonte 1. Sistema dominante**: representa el presente y las prácticas mayoritarias ya vigentes en el SSN y su subsistema de Inteligencia. Se caracteriza por un alto grado de estabilidad y efectividad estratégica, aunque con el tiempo puede perder su adecuación al entorno posnormal, enfrentando dificultades de adaptación.

2. **Horizonte 2. Transición e innovación**: es un periodo intermedio entre el horizonte 1 y 3. Se caracteriza por la coexistencia de elementos del sistema dominante con innovaciones disruptivas. Este horizonte es ambiguo y turbulento, lleno de experimentación, creatividad y debates sobre el cambio. Algunas innovaciones pueden ser absorbidas por el sistema dominante, mientras que otras logran abrir camino hacia transformaciones más profundas.
3. **Horizonte 3. Futuro transformador**: representa una visión transformadora y un nuevo paradigma que, en su caso, reemplaza al sistema dominante actual. Este horizonte surge como respuesta a las deficiencias del horizonte 1, incorporando las innovaciones exitosas del 2. Aunque, inicialmente, es una posibilidad apenas percibida, con el tiempo se consolida como el nuevo sistema dominante gracias a su capacidad para adaptarse mejor al entorno cambiante.

En todo caso, el propio camino de transformación que recorra el subsistema de Inteligencia entra dentro de las incertidumbres poco profundas que solo el tiempo despejará.

Bibliografía

Antonio Martínez-Sánchez, J. (2014). *The Use of Mental Models as a Source of Error in the Analysis of Intelligence*.

Aracil, J. (1995). *Dinámica de sistemas*.

Arcos, R. y Antón, J. (2010). *Reservas de Inteligencia: hacia una Comunidad ampliada de Inteligencia*.

Curry, A. y Hodgson, A. (2008). *Seeing in Multiple Horizons: Connecting Futures to Strategy*, *Journal of Futures Studies*.

Donoso, D. (2020). Aspectos psicológicos en el ámbito cognitivo de las operaciones militares. *Implicaciones del ámbito cognitivo en las Operaciones Militares*, pp. 21-45.

Endsley, M. R. (2000). *Situation Awareness Analysis and Measurement*. Lawrence Erlbaum Associates. [Consulta: 2025]. Disponible en: https://www.researchgate.net/publication/292771806

Frías Sánchez, C. (2023). El conflicto como motor de cambio. En: Ministerio de Defensa (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministerio de Defensa, pp. 153-162.

Gil Armario, J. M. (2024). La comprensión de las amenazas a la Seguridad Nacional como sistemas complejos sociales. Aplicación de las técnicas analíticas estructuradas, modelado de sistemas e inteligencia artificial. *Cuadernos de Inteligencia*. 2, pp. 49-74.

Gutiérrez de León, B. (2023). Las operaciones multidominio. En: Ministerio de Defensa (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministerio de Defensa, pp. 131-152.

Hidalgo, C. y Funtowicz, S. (2024). Epistemología política. Ciencia con la gente. *Revista iberoamericana de ciencia tecnología y sociedad*. 19(55), pp. 215-228. DOI: https://doi.org/10.52712/issn.1850-0013-454

Huston, J. (1992). *What are the greatest challenges for evolutionary theory in our times?*

Huston, J. (2005). *Which Way is Up?*

Ivars Pérez, J. (2023). Una aproximación teórica al viejo y nuevo paradigma de inteligencia para la seguridad. *Disjuntiva. Crítica de les Ciències Socials*. 4(1), p. 39. DOI: https://doi.org/10.14198/disjuntiva2023.4.1.3

Jiménez-Buedo, M. y Vielba, I. R. (2009). ¿Más allá de la ciencia académica?: Modo 2, ciencia posacadémica y ciencia posnormal. *Arbor*, pp. 721-737. DOI: https://doi.org/10.3989/arbor.2009.738n1048

Jordán, J. (2016). *Una revisión del ciclo de Inteligencia*. [Consulta: 2025]. Disponible en: http://www.seguridadinternacional.es

Jordán, J. (2018). The international conflict in the gray zone: A theoretical proposal from the offensive realism perspective. *Revista Española de Ciencia Politica*. 48, pp. 129-151. DOI: https://doi.org/10.21308/recp.48.05

Jordán, J. (2022). *Teorías realistas para comprender la política internacional*, *Global Strategy Report*, *N.º 4*. [Consulta: 10 marzo 2025]. Disponible en: https://global-strategy.org/teorias-realistas-para-comprender-la-politica-internacional/

Lahneman, W. J. (2010). The Need for a New Intelligence Paradigm. *International Journal of Intelligence and CounterIntelligence*. 23(2), pp. 201-225. DOI: https://doi.org/10.1080/08850600903565589

Lorenzo-Penalva, J. (2023). Inteligencia estratégica, transdisciplinariedad y sistemas complejos adaptativos. *Cuadernos de Inteligencia*. 1, pp. 51-61.

Martín Palma, R. J. (2023). Las tecnologías del futuro de la seguridad y la defensa. En: Ministerio de Defensa (ed.). *XXX Curso Internacional de Defensa. Los motores de cambio de la seguridad y la defensa*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2018). *PDC-01 (A) Doctrina para el empleo de las FAS*. [Consulta: 2025]. Disponible en: https://publicaciones.defensa.gob.es/

OSCE. (2020). *Guía de la OSCE sobre actividad policial basada en la inteligencia*. [Consulta: 22 febrero 2025]. Disponible en: https://www.osce.org/es/secretariat/455536

Pajares de Mena, M. D. M. (2010). *Dinámica de organizaciones terroristas domésticas*.

Paya Santos, C. (2017). *Aproximación transversal a los sesgos cognitivos del analista de inteligencia*.

Penalva Lucas, J. (2023). Análisis de modelos matemáticos aplicados a la lucha contra el terrorismo y los extremismos violentos. *Revista Política y Estrategia*. 140, pp. 35-62. DOI: https://doi.org/10.26797/rpye.vi140.1008

Sardar, Z. (2019). *The Postnormal Times Reader*. [Consulta: 2025]. Disponible en: https://www.cppfs.org/

Serra, J. y Sardar, Z. (2017). Intelligence in Postnormal Times. *World Futures Review*. 9(3), pp. 159-179. DOI: https://doi.org/10.1177/1946756717709277

Tarrow, S. (1994). *El poder en movimiento: Movimientos sociales, acción colectiva y política*.

Una experiencia real de uso de la IA en el análisis de fuentes abiertas: la factoría de análisis del Centro de Análisis y Prospectiva de la Guardia Civil

Enrique Ávila Gómez
Lorenzo Luna Zambrana

Resumen

El documento examina el uso de la inteligencia artificial (IA) en el análisis de inteligencia de fuentes abiertas, enfocándose en la experiencia del Centro de Análisis y Prospectiva (CAP) de la Guardia Civil.

Aborda cómo la IA generativa transforma la detección, selección y análisis de información, permitiendo un acceso más rápido y amplio a fuentes diversas.

Sin embargo, se señalan los desafíos, en especial, las «alucinaciones» de la IA, y se exploran estrategias para mitigar estos riesgos, como el uso de grafos de conocimiento y la validación humana.

El texto destaca la importancia del talento humano en la revisión y verificación de la información, así como la necesidad de adaptarse al cambio tecnológico para mejorar la precisión y eficiencia en la toma de decisiones estratégicas.

Además, enfatiza la necesidad de una visión holística y multidisciplinaria en el análisis de inteligencia, incorporando diversos modelos culturales para reducir sesgos.

Palabras clave

Prospectiva, Análisis, IA, Alucinaciones, Sesgos.

A real experience of the use of ia in open source analysis: the analysis factory of the Civil Guard's analysis and forecasting centre

Abstract

The document examines the use of Artificial Intelligence (AI) in open source intelligence analysis, focusing on the experience of the Center for Analysis and Foresight (CAP) of the Guardia Civil.

It addresses how generative AI transforms the detection, selection and analysis of information, allowing faster and broader access to diverse sources.

However, challenges are pointed out, especially AI «hallucinations», and strategies to mitigate these risks are explored, such as the use of knowledge graphs and human validation.

The text highlights the importance of human talent in the review and verification of information, as well as the need to adapt to technological change to improve accuracy and efficiency in strategic decision-making.

In addition, it emphasizes the need for a holistic and multidisciplinary vision in intelligence analysis, incorporating various cultural models to reduce biases.

Keywords

Prospective, Analysis, AI, Hallucinations, Biases.

1 Introducción

En este artículo se va a descender a territorios táctico-operativos en el mundo de la IA aplicada a los procesos de análisis de inteligencia orientada a la toma de decisión estratégica, abandonando la perenne tendencia hacia la descripción de niveles estratégicos que no permiten acercarse a este nuevo reto tecnológico de forma holística y con un objetivo de aplicabilidad práctica en sectores diversos entre los que, por supuesto, se encuentra el sector de la Defensa, ocupando, además, un lugar cada vez más central, en un entorno geopolítico complejo, cambiante y con la necesidad de herramientas que permitan su rápida adaptación al escenario.

Las estructuras sociales, políticas, económicas, de nuestras sociedades son cada vez más complejas. Cada avance tecnológico ha introducido, en un modelo de capas superpuestas, una nueva capa de complejidad. La superestructura generada ha supuesto, a nuestro juicio, una barrera en la comprensión de un sistema que, además, requiere de una atención continua, cuya interconexión provoca efectos desconocidos y, a menudo, indeseado entre las diversas capas y en el que, más grave aún, se ha perdido una parte importante de la comprensión del funcionamiento de esta superestructura por imposibilidad intelectual del ser humano para el manejo de este nivel de complejidad, tanto a nivel individual como colectiva.

La eclosión de la inteligencia artificial (no solo la generativa) ha abierto un conjunto de posibilidades, a menudo inaccesibles hasta hace bien poco, a los equipos de análisis de información de fuentes abiertas que elaboran los informes que habrán de ayudar a la toma de decisión en los niveles de decisión estratégica, es decir, a interpretar esa realidad compleja de una forma adecuada para que el decisor pueda ejercer su principal misión.

Las limitaciones existentes, hasta hace bien poco, tanto de índole temporal como de acceso al talento especializado disponible en las fases de detección de activos de información de interés y, más aún, en las fases de análisis y diseminación de información eran cada vez más evidentes para cualquier unidad de análisis de inteligencia de fuente abierta. La enorme dinamicidad y complejidad del mundo actual determinaban, sin duda, una limitación estructural a la cantidad y calidad de los análisis que debían de servir de base para la decisión estratégica.

No menos importante resultaba la progresiva barrera que los sistemas de diseminación automatizada introducían por, a menudo, inundación de información supuestamente relevante (y probablemente lo es) que provocaba un progresivo «desenganche» del decisor del acceso a la información elaborada.

Este artículo describe la experiencia práctica que se ha estado desarrollando desde el Centro de Análisis y Prospectiva de la Guardia Civil para

configurar un ecosistema de detección, selección, análisis y diseminación de información de interés para la Dirección Estratégica, en materia de Seguridad Interior, prácticamente, en tiempo real, con intervención humana mínima y orientada esta, en específico, a la validación de los contenidos en las fases de selección y verificación final de contenido que, se considera, será la principal tarea de futuro de muchas profesiones, entre ellas, la de analista.

Se ha intentado, además, generar un modelo de acceso y diseminación de la información generada que permita segmentar al receptor de la información, limitando (que no eliminando) la decisión de acceso sobre los activos de información recibida a través de las herramientas tecnológicas habituales en este modelo y que, en demasiadas ocasiones, provocaban un colapso por inundación.

2 El Centro de Análisis y Prospectiva de la Guardia Civil (CAP)

Hace ahora 31 años, en un acuerdo innovador entre el mundo de la Academia y la Guardia Civil, se procedió a la creación del Centro de Análisis y Prospectiva de la Guardia Civil (García López, 2010: 45-60). Un hecho sin precedentes, en la historia de nuestro país, el que fuese una Fuerza de Seguridad del Estado la que detectase la necesidad de anticiparse a las amenazas emergentes haciendo uso de la prospectiva y, desde un posicionamiento proactivo, intentase desarrollar el diseño de futuros (probables, plausibles o posibles) a partir de un conocimiento exhaustivo del presente, apoyándose en las herramientas tecnológicas y conceptuales disponibles en cada instante.

Desde aquel momento de génesis hasta el momento actual, el Centro ha pasado por varios modelos de Dirección Estratégica, más o menos orientados a la generación de productos de corte científico-técnico, siguiendo modelos clásicos de detección de información de interés, clasificación, análisis, generación de base documental y diseminación de esta, por los circuitos definidos interna y externamente, por parte de la Institución.

La eclosión de Internet y el acceso global a fuentes de interés para la elaboración de Inteligencia de fuentes abiertas generó la necesidad de dotarse de un conjunto de herramientas tecnológicas que configurasen un ecosistema de tratamiento de la información que permitiese, fundamentalmente, adaptarse a los tiempos, cada vez más inmediatos, en los que es preciso contar con información relevante para su tratamiento y conversión en conocimiento interno y orientado, en el caso del CAP a la toma de decisión estratégica.

De forma paralela, el CAP ha sido centro de detección (y algunas veces de posterior reclutamiento vía oposición) de talentos especiales. Configurado

como un elemento de conexión con la educación superior de nuestro país, sus programas de prácticas, considerados de un nivel de excelencia por las universidades colaboradoras y por el estudiantado que ha pasado por esa experiencia, ha permitido incorporar visiones, experiencias y capacidades desarrolladas por las nuevas cohortes de ciudadanía de nivel universitario.

La incorporación temporal de talento joven, con ideas exógenas a la Institución, brillante, a menudo con experiencia internacional, se ha configurado como un excelente marco de trabajo y de generación de capacidades de análisis que, entre otras externalidades positivas generadas, nos permiten orientar el futuro de las personas que acaban sus prácticas hacia nichos de inteligencia que no se limitan al Estado, sino que se amplían hacia nuestros sectores productivos que, hace tiempo ya, hacen un uso intensivo de estas capacidades en sus procesos de Inteligencia Competitiva e Inteligencia Económica.

Algunos de aquellos y aquellas primeras personas que realizaron parte de sus prácticas profesionales en el CAP son, por tanto, parte de las unidades de Inteligencia que se han ido desplegando, sobre todo, en el nicho de las grandes estructuras corporativas nacionales.

Por último, el CAP tiene encomendada la misión de generar «cultura de la seguridad». Orientada su actividad a mejorar la resiliencia social a través de la interacción con la ciudadanía, utilizando diversos canales, tanto analógicos como digitales, y adaptando los contenidos para impactar sobre grupos poblacionales concretos, a lo largo de los últimos cinco años, se ha participado en actividades con universidades, generado documento y creado y mantenido canales de interacción con la Academia, el sector privado, otras Instituciones y la propia ciudadanía, incorporando tecnologías tales como metaversos, metahumanos o Inteligencia Artificial para la interacción directa con los grupos específicamente seleccionados como de interés (Soliman, 2024).

Conocida la misión del CAP y descritas las herramientas de que dispone para llevarla a cabo, nos introducimos en el proceso de configuración del ecosistema que en la actualidad se está desplegando para mejorar la calidad y los tiempos de respuesta de generación de productos de Inteligencia adaptados a las necesidades del decisor estratégico.

3 Escenario previo: idioma, detección, validación y tiempo

La misión actual de una unidad dedicada al análisis de fuentes abiertas es un auténtico infierno. Detectar, valorar, analizar y diseminar la infinita cantidad de información generada a cada instante no está al alcance de las capacidades humanas, con independencia del número o la calidad de los recursos humanos dedicados a esta misión.

Hace no tanto, las capacidades a desarrollar por parte de los analistas en la primera fase del proceso de detección de información relevante o de interés para la toma de decisión eran, fundamentalmente, la de conocer los repositorios de fuentes de interés (un puñado de revistas científicas, unas cuantas bibliotecas seleccionadas, algún informe de fuente más o menos validada y conocida...).

Este tipo de capacidad se transformó, con el tiempo y con el apoyo de tecnología básica de etiquetado y clasificación de la información y, con suerte, el uso de algún gestor documental con capacidad de indexación de contenidos (se habla de hace no mucho más de dos años el límite temporal en que todas capacidades del analista se podían considerar las más valiosas para el análisis de documento de fuente abierta), en un proceso más o menos automatizado de clasificación y recuperación de documentos de interés por parte de la persona o grupo interesado en algún aspecto relacionado con la Seguridad Interior de nuestro país.

Básicamente, se generaban productos de inteligencia desde fuentes acotadas, consideradas, por su inserción en determinados índices, como de validez absoluta y sin necesidad de análisis en cuanto a su calidad. Esta metodología, de validez contrastada, no impedía, en todo caso la aparición de sesgos o de información incompleta dado que se perdía el acceso a otras corrientes de pensamiento desestimadas por la propia Academia.

Los resultados, como decimos, a menudo probablemente sesgados (sí, ahora se habla de sesgos en la IA, pero no se piensa en los sesgos inducidos por equipos de análisis pequeños, con capacidades pluridisciplinares muy limitadas y con bajo acceso a expertos y expertas de conocimientos no directamente conexos con el asunto de interés que se estuviera analizando (Mosqueira-Rey, 2023). Eso por no hablar de las limitaciones de enfoque inducidas por las limitaciones de acceso a otras áreas geopolíticas y culturales por problemas de idioma), se podrían considerar como óptimos para los recursos disponibles en ese momento, pero claramente insuficientes para entender y, menos aún operar, sobre la complejidad e inmediatez en los procesos de toma de decisión que requiere el mundo actual.

En 2013, a través de un proyecto de investigación del IUISI (Instituto Universitario de Investigación de Seguridad Interior, lamentablemente desaparecido), se detecta este inicial problema en el acceso temprano a información de interés, dentro y fuera de las corrientes de pensamiento principales y se procedió a estudiar el viaje de ida que se había producido desde el mundo de la Inteligencia Estratégica al de la Inteligencia Competitiva y la Económica y que había permitido el desarrollo de nuevas metodología, así como la aplicación de herramientas tecnológicas avanzadas por parte de corporaciones con capacidades económicas comparables a las de los Estados.

De ese modo y con el objetivo de planificar un viaje de vuelta hacia los modelos de Inteligencia Estratégica, de ámbito estatal, de las metodologías y herramientas que las grandes corporaciones habían desarrollado para la generación y uso de su propia Inteligencia, con objetivos sectoriales y eminentemente económicos, incorporamos a nuestro propio modelo de conocimiento los procesos de Vigilancia Tecnológica[1].

Durante el desarrollo de ese proceso de investigación, no nos centramos tanto en la generación de conocimiento documental ni, menos aún, académico, sino que se trabaja en el diseño y despliegue de un ecosistema tecnológico de adquisición, validación y análisis de información de interés a partir de la definición y evolución de un sistema de fuentes orientado a la detección temprana de amenazas emergentes relacionadas con tecnologías de doble uso (en realidad, se podría decir que todas aunque, en aquel momento nos centramos en drónica y biotecnología instrumental desarrollada por grupos de *biohacking*)

Se descubre la existencia de una plataforma tecnológica de *software* libre, desarrollada con el apoyo de las administraciones públicas que permitía automatizar la adquisición de fuentes de interés desde Internet, almacenar una parte de la información de forma local, validar su interés de forma sencilla por parte de los equipos de análisis, ampliarla gracias un trabajo posterior de análisis en profundidad y diseminarla, de forma automatizada, haciendo uso de sistemas de boletinado mediante suscripción por parte de los receptores interesados en un determinado área de conocimiento.

La plataforma HONTZA[2] estaba diseñada para la ejecución de un ciclo completo de Inteligencia Competitiva que abarcaba desde el diseño inicial de las estrategias de la organización y de detección de fuentes relevantes para la misma, hasta la diseminación final automatizada de la información, haciendo uso de boletinado mediante suscripción, pasando por los procesos de transformación de la información en Inteligencia, con la actividad de los equipos de analistas desarrollándose en un ecosistema de red social interna y que incluía la coordinación y gestión de redes de expertos externos a la organización, así como un sistema de propuestas y gestión de proyectos asociados a una determinada detección de interés durante el proceso de vigilancia tecnológica.

[1] La Vigilancia Tecnológica es un proceso sistemático que permite a las organizaciones detectar, seleccionar, analizar y diseminar información relevante sobre avances tecnológicos y científicos. Este proceso es fundamental para anticiparse a las amenazas emergentes y tomar decisiones estratégicas informadas.

[2] La plataforma HONTZA permite a los equipos de trabajo colaborar de manera eficiente, automatizando procesos de vigilancia tecnológica y facilitando la gestión de información relevante. Entre sus características destacan la capacidad de importar canales de información, generar documentos colaborativos, y analizar la evolución de las noticias. La idea de HONTZA surgió para ofrecer una alternativa a los *software* de vigilancia tecnológica de código cerrado, que suelen ser costosos y limitan la personalización y colaboración entre usuarios. El proyecto fue impulsado por asociaciones empresariales del País Vasco y financiado por la Sociedad para la Transformación Competitiva del Gobierno Vasco (SPRI).

Con un equipo de investigación formado por al teniente coronel Arturo Crespo Arranz, al teniente coronel Santiago Alonso Pradillo y la investigadora y experta en Servicios de Inteligencia María Cuiñas Insúa, se opta por el desarrollo de un ecosistema orientado a la formación de analistas de inteligencia y explotación intensiva de la información de fuente abierta de interés, apoyándonos en esta plataforma.

Esa es la base de un moderno ecosistema de generación de Inteligencia: ser capaces de detectar y adquirir, de forma automatizada y en tiempo real, información de interés para la elaboración de conocimiento e inteligencia sobre asuntos de interés estratégico (o táctico) de la organización.

Se hablaba de 2013-2014 y, por supuesto, durante los siguientes diez años, las herramientas orientadas a este tipo de procesos mejoraron en todo lo referente a las capacidades de acceso, detección, indexación y multimodalidad. Ya no se trabajaba solo con elementos textuales, sino que la tecnología permitió el acceso a conocimiento multimodal de todo tipo: información desestructurada, audio, vídeo, etc. (AENOR, 2018).

Es a partir de finales de 2023 cuando entramos en un nuevo escenario: se empiezan a liberar servicios de inteligencia artificial generativa que, al principio sobre base documental textual, pero, poco a poco, con capacidades de multimodalidad, empieza a hacer posible la automatización de varios de los procesos de análisis provocando la evolución del modelo preexistente de forma radical (Storey, 2025).

¿Qué problemas se encontraban en el modelo anterior? Básicamente, se pueden citar cuatro: el tiempo, la enorme cantidad de fuentes disponibles, el idioma y el talento pluridisciplinar al que se puede acceder por parte de cualquier organización. Y el primero, el del tiempo, además, fuertemente mediatizado por todos los demás.

El idioma siempre ha sido un cuello de botella de cualquier organismo que genere informes para un decisor estratégico. En el caso de la elaboración de Inteligencia, además, la no incorporación en el análisis de diversos enfoques pluridisciplinares, multiidioma y multiculturales, induce un conjunto de sesgos que impiden disponer del conocimiento adecuado para el manejo de situaciones de complejidad creciente. Más aún en una sociedad fuertemente globalizada e interdependiente en el que el impacto de diferentes modelos culturales en los procesos de toma de decisión puede llegar a tener que dar por completo la vuelta al resultado de un determinado análisis. Un ejemplo práctico de esta aseveración se puede encontrarlo en el Intelligence Practitioner's HANDBOOK (New Zealand Institute of Intelligence Professionals, 2024), en el que se introducen elementos de la cultura mahorí en los procesos de análisis de inteligencia que aparecen en este interesante libro[3].

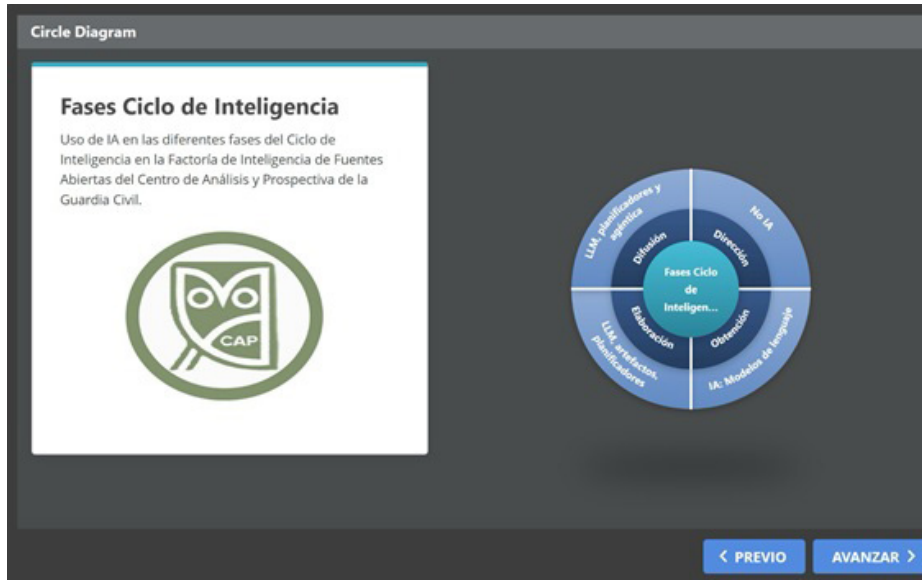
[3] Para una acceso analítico al contenido de este se puede utilizar esta URL: https://www.ciberinteligencia.eu/new-zealand-intelligence-principles-and-practice/ que, además,

A menudo, esta disfunción limita fuertemente la posibilidad de realizar recomendaciones acertadas al decisor. Intentar no caer en este error significa, en un modelo clásico, pasar por farragosos procesos de traducción e interpretación cultural, usando capacidades humanas, muchas veces indisponibles, que, gracias a herramientas de traducción automática han permitido mitigar, en parte, esta primera barrera.

Pero es el momento en que la IA generativa hace su aparición cuando se produce la apertura del foco de acceso de un equipo de Inteligencia hacia un modelo que podría denominarse como 360.

Desaparecen, por ensalmo, las barreras idiomáticas y se reducen, drásticamente, las temporales, a la hora de analizar múltiples fuentes, en diferentes idiomas, en un nuevo proceso dialogado con las fuentes documentales a las que diferentes expertos, en diferentes materias, pueden acceder de forma sencilla y usando lenguaje natural para su «diálogo» con ese conjunto de fuentes.

Es este el momento en el que se empieza a trabajar en la introducción de las herramientas de IA que se van desarrollando en las diferentes fases del Ciclo de Inteligencia clásico. A continuación, se presenta un gráfico que intenta exponer esta implementación. Para un acceso directo al gráfico interactivo se puede usar la URL: https://ciberinteligencia.eu/interacciones/ciclo/.



constituye un ejemplo práctico del modelo de análisis que se está desplegando en el CAP, incluyendo los productos generados para decisor estratégico.

Más adelante, se tratará el problema del talento disponible y de las nuevas capacidades que han de desarrollarse para su progresiva adaptación al nuevo escenario tecnológico porque se trata de un problema de difícil solución inmediata y que requiere modificaciones sustanciales en asuntos relacionados con formación especializada, cultura o rotaciones acotadas.

Nuestro Centro ha ido estudiando y probando durante los dos últimos años, los servicios de inteligencia artificial que se han considerado de interés para mejorar la eficiencia de nuestra misión, con el objetivo de, en la medida de lo posible, transformar el proceso de Ciclo de Inteligencia en un modelo lo más automatizado e industrializado posible, siempre orientado a ofrecer al decisor estratégico la inteligencia que necesita, en el momento preciso, para que sea incorporada en sus procesos de toma de decisión y, por supuesto, preservando el necesario espacio de intervención humana en el último paso de validación de contenidos.

Entre los servicios que se han utilizado, se pueden incluir los siguientes:

— NotebookLM, de Google. Ampliamente utilizado en el mundo académico, permite generar materiales de interés para los procesos de análisis tales como

- Documentos generados desde fuentes documentales desestructuradas de difícil análisis por métodos tradicionales:

  fi Fuentes de audio y vídeo: ya no es necesario un operador humano visualizando/escuchando durante horas una o varias fuentes. Se realiza una transcripción automática y la generación de los productos básicos de este sistema:

  a) Documento resumen.

  b) Preguntas frecuentes.

  c) Fichero resumen de audio en formato podcast.

- Los materiales generados sirven como punto de partida para el «diálogo» con el sistema de fuentes, de tal manera que, una vez adquirido el conocimiento necesario sobre el asunto de interés, el analista, a través de este proceso de «diálogo» con la base documental, es capaz de orientar de manera aedcuada el *prompting* a través de una adecuada contextualización y orientación hacia un público objetivo específico.

- El producto final es una base documental textual, de no más de tres páginas, que delimita el problema e informa al decisor de las cuestiones de interés que deberían ser integradas en el proceso de decisión.

— Google AI Studio. Esta plataforma incorpora los nuevos modelos de razonamiento profundo de esta empresa. Sus capacidades de planificación, razonamiento y búsqueda de información, señalando las fuentes y permitiendo al analista definir cambios en los procesos de planificación de la investigación convierten a esta herramienta en invaluable para un equipo de analistas. La posibilidad de generación de productos de inteligencia tanto documentales clásicos como en otros formatos, más accesibles y comprensibles, incluso, interactivos son, a nuestro juicio un anticipo ya muy avanzado, de un conjunto de agentes de IA que van a desplazar al ser humano del centro de los procesos de análisis[4].

— Copilot de Microsoft. Sus capacidades de integración con procesos a través de la inclusión de agentes y, por supuesto, con herramientas ofimáticas estándar han sido, sin duda, de enorme valor en la integración y confección de productos de interés para el análisis de Inteligencia. Alto impacto en los procesos formativos. Generar los materiales para la realización de una actividad de formación desplegable en una plataforma de teleformación se ha convertido en una actividad de horas y no de meses. Se ha conseguido generar dos cursos de teleformación interna para analistas, en materia de análisis de inteligencia de fuente abierta y en materia de diseño de futuros en menos de una semana. Partiendo de un esquema generado desde un modelo de pensamiento profundo, el uso de Copilot para la generación de presentaciones y otros productos de contenido formativo, para ser desplegados, en formato SCORM, en la plataforma de teleformación corporativa ha resultado una experiencia altamente eficiente. Cualquier conocimiento se encuentra accesible. Cualquier conocimiento puede ser rápidamente transformado en una acción formativa estructurada.

— Deepseek. Se ha incorporado este modelo para disponer de respuestas generadas a partir de otros conjuntos de datos provenientes de otras áreas geopolíticas. Poder comparar los enfoques, calidad de la respuesta y espectro ideológico del modelo ha permitido entender un contexto complejo, así como detectar ciertas amenazas emergentes relacionas con sesgos y determinación de entidades. Este modelo es computacionalmente utilizable con recursos limitados, de tal manera que es posible aislar contenedores de información que haya de ser protegida y no expuesta a sistemas en la nube sobre los

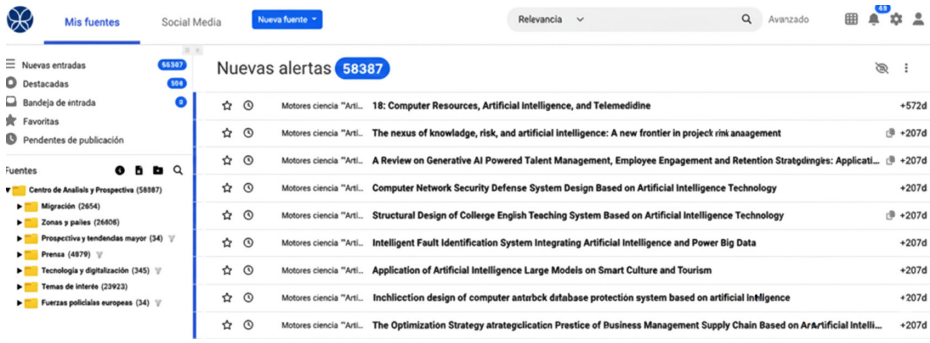
[4] Para ver una «prueba de vida» de esta controvertida aseveración se puede acceder a este ejemplo de análisis, en bruto, que trae razón de la noticia: https://edition.cnn.com/2025/06/03/business/trump-tariffs-china-pharmaceuticals-intl-hnk. A partir de esta amenaza detectada por un medio global, se procede a usar el modelo Gemini 2.5 Pro y su utilidad de generación de informe en profundidad para obtener el siguiente resultado: https://www.ciberinteligencia.eu/informe-impacto-amoxicilina/.

que se pueda perder el control. Su código abierto permite la realización de actividades de *fine tunning* que adapte el campo semántico a las necesidades de la organización, minimizando la posibilidad de que se produzcan las indeseadas alucinaciones.

— Qwen3. Este modelo se caracteriza por su poderosa multicanalidad y sus capacidades de generación de productos diversos incluyendo audio, vídeo, imágenes, artefactos o código, entre otras funcionalidades. El análisis de información desestructurada multimedia ha sido nuestro principal uso al determinar que su calidad era superior a la de los otros modelos.

— Manus. Esto no es un modelo de lenguaje sino un sistema multiagéntico con capacidad de interacción con el sistema operativo. Esto es: puede no solo generar un plan, sino, además, ejecutarlo en forma de tareas complejas. Nos ha interesado, sobre todo, el concepto. La capacidad agéntica de ejecución de tareas complejas constituye, a nuestro juicio, un punto de inflexión. Más aún en entornos que requieran modos de funcionamiento de detección, análisis y respuesta en, prácticamente, tiempo real. Por ejemplo, los de teatro de operaciones. Se trata de un modelo que se define como aún experimental pero que está evolucionando de forma rápida.

La fase temprana de detección de contenidos de interés ya utiliza servicios de IA para facilitar la generación de un sistema de fuentes coherente y orientado a los objetivos descritos por el analista. Esta actividad constituía, históricamente, una de las principales fuentes de error y de discusión por parte del equipo de analistas. En la actualidad, se transforma en un proceso semiguiado por un agente planificador al que, a través del lenguaje natural, informas de cuáles son tus necesidades de información para, a partir de ese nivel, ir profundizando en la selección de las fuentes de interés. El analista pasa a ser un validador de las decisiones del planificador y, para ello, ha de armarse de herramientas culturales que le permitan tomar ese tipo de decisiones.



La fase de análisis a través del «diálogo» con las fuentes objetivo contextualizando los objetivos y el público objetivo al que irá dirigido el análisis, haciendo uso de varias herramientas de inteligencia artificial para, en una última fase, analizar el resultado de los productos obtenidos como nuevas fuentes de información sobre las que, en caso de ser necesario volver a trabajar, ya de manera directa, por parte de los equipos de analistas humanos. (Bosso y Ruberto, 2025).

El analista profesional realizará una primera crítica radical a este modelo apoyándose, a buen seguro, en argumentos conexos con la experiencia profesional y la necesidad de precisión en la respuesta. Argumentará, del mismo modo, sobre la posibilidad de error que toda tecnología introduce en los procesos que se consideran críticos y fuertemente intelectualizados en los que, a menudo, la experiencia profesional es la que permite disponer de ese «momento de inspiración» que parece caracterizar al ser humano y colocarle en un nivel aún superior al de la tecnología.

Sobre consecuencias nefastas de esos «momentos de inspiración humana» a lo largo de la historia, así como su falibilidad se podría mantener un interesante debate que trasciende los objetivos de este documento, ello sin entrar en los «intereses» que pueden mediatizar las recomendaciones de un grupo de análisis.

No obstante, se puede señalar que la falibilidad de la inspiración humana, muy conectada con nuestros sesgos (Kahneman, 2012), es un elemento fundamental a la hora de configurar los equipos de análisis, así como a la hora de desarrollar sus nuevas capacidades. Veamos qué nos dice al respecto Gemini (IA, 2025):

— «**Sesgos cognitivos**: La inspiración, a menudo, surge de intuiciones y corazonadas, que pueden estar influenciadas por sesgos cognitivos. Estos sesgos, como el sesgo de confirmación (buscar información

que confirme nuestras creencias preexistentes) o el efecto halo (dejar que una sola característica positiva influya en nuestra percepción general), pueden distorsionar nuestra evaluación de la situación y llevarnos a tomar decisiones basadas en información incompleta o engañosa.

— **Falta de objetividad**: La inspiración puede ser subjetiva y emocional, lo que puede dificultar la objetividad en el análisis. Cuando nos dejamos llevar por la pasión o el entusiasmo, podemos pasar por alto detalles importantes o ignorar riesgos potenciales.

— **Exceso de confianza**: La inspiración puede generar un exceso de confianza en nuestras ideas y juicios. Cuando estamos convencidos de que tenemos la razón, podemos ser menos propensos a escuchar a los demás o a considerar diferentes perspectivas. Este exceso de confianza puede llevarnos a tomar decisiones arriesgadas o imprudentes».

No podemos, en todo caso, sino señalar nuestro acuerdo parcial con ese tipo de críticas, por parte de los profesionales de la Inteligencia, a la hora de hacer uso de las herramientas descritas, desde el plano estrictamente intelectual clásico. No obstante, el enorme cambio de escenario que impone la inteligencia artificial aplicada al análisis de inteligencia induce la necesidad de posicionarnos de manera crítica (constructiva) frente a las consideraciones de un modelo de trabajo «clásico».

Estos serían los argumentos que se consideran esenciales para defender nuestro posicionamiento a favor del uso de la IA en las fases del ciclo de inteligencia:

— ¿Acaso los seres humanos no cometemos errores de percepción evaluación respuesta al realizar análisis? Creo que es indiscutible nuestro sesgo individual y colectivo a la hora de evaluar situaciones de interés. Los sesgos individuales (educacionales, ideológicos, de género) impactan sobre nuestros análisis. Pero también lo hacen los de grupo a través de liderazgos y relaciones de poder en los equipos.

— ¿La comprensión de la complejidad actual de cualquier sistema humano se encuentra al alcance de una persona (o de un equipo), con limitaciones en el acceso a todo el conocimiento necesario para realizar una evaluación correcta de una amenaza compleja? No se puede a aspirar a entender estructuras tan complejas como las que configuran las realidades actuales. No disponemos de capacidades intelectuales ni individuales ni colectivas para lograrlo. La IA ofrece una oportunidad de simplificación para la comprensión de la complejidad.

— ¿El tiempo necesario para la comprensión y evaluación de una amenaza en el mundo actual se adapta a los tiempos de análisis de un equipo humano y, sobre todo, a la necesidad temporal de respuesta que requiere el decisor estratégico? Sin duda, no. Ya se ha adaptado gran parte de los procesos de toma de decisión actuales a la realidad algorítmica. Y se va a continuar por ese sendero porque no hay una posibilidad alternativa. No se va a parar en el camino de la complejidad y el uso de la tecnología para intentar tomar decisiones, en tiempo real, sobre esa complejidad.

Consideramos los autores que la respuesta a las tres preguntas planteadas es negativa y por ello hemos operado de forma diferente desde nuestro Centro de Análisis y Prospectiva.

Por los motivos señalados, las capacidades humanas, limitadas en cantidad y tiempo, son usadas solo en dos de las fases de elaboración del producto de inteligencia:

— Detección, validación y mantenimiento del sistema de adquisición automatizada de fuentes.

— En la fase de validación del producto obtenido, justo antes de ser diseminado.

Hemos entrenado a nuestros analistas para realizar comprobaciones de estructura argumental y verificación de fuentes con el fin de detectar, de forma temprana, lo que conocemos como «alucinaciones» de la inteligencia artificial, por cierto, nada que no sufra cualquier analista, a lo largo de su trayectoria profesional, en múltiples ocasiones.

No se puede dejar de señalar, en todo caso, que el riesgo se ha detectado más alto en función de ciertos parámetros relacionados con el uso de Inteligencias Artificiales generativas de propósito general como pueden ser:

— Todo lo relacionado con entidades de diversa tipología (personas, lugares, tiempos)

— Información actualizada sobre un determinado asunto de nicho.

Siendo lo antedicho cierto, nos hemos encontrado durante la última fase de desarrollo de nuestra Factoría de Inteligencia, en el segundo semestre de 2024 y primer trimestre de 2025, con un inesperado aliado: la competencia geopolítica (o geoeconómica).

Hemos sido testigos, desde finales de 2025 y, sobre todo, a lo largo de lo que llevamos de 2025, de la competición global por ser referentes en materia de inteligencia artificial. Hasta hace no muchas fechas, al menos en servicios de inteligencia artificial generativa, nadie tenía ninguna duda de que era EE. UU. la ganadora… Hasta que China se ha posicionado. Y

sus modelos (dos, con capacidades de razonamiento profundo, hoy en día, DeepSeek y Qwen) ofrecen respuestas con una orientación diferente cuando se les plantea una cuestión de interés para la decisión estratégica (Khan, 2024).

Nuestros equipos de análisis tienen como misión operar con diferentes tipos de IA con el fin de disponer de una visión más holística sobre cualquier problema que se someta a su análisis, así como de disponer de un sistema paralelo de verificación de la información que levante alertas sobre la existencia de una determinada alucinación.

El uso en paralelo de varios servicios de IA generativa, según nuestra experiencia, mejora y enriquece el contenido de los análisis y, sobre todo, permite disponer de una visión muchas veces radicalmente contrapuesta a la que nuestros equipos de analistas manejan por modelo cultural y geopolítico.

Esta última reflexión nos conecta con el talento. Su disponibilidad. Su calidad. Su pluridisciplinaridad.

4 El problema del talento

El CAP, configurado en la actualidad como una unidad civil dentro de la Guardia Civil, tiene como una de sus misiones principales la relación con las universidades.

Nuestro programa de prácticas está considerado dentro de un nivel de excelencia por las universidades y las especialidades formativas con las que trabajamos habitualmente.

Históricamente, la gran mayoría de nuestro alumnado en prácticas procedía de los grados de Traducción e Interpretación, Relaciones Internacionales, Derecho, Criminología o Comunicación. Hace ahora cuatro años, se detectó la necesidad de nutrir nuestros programas con capacidades de Ciencias Exactas, Ciencias Químicas, Ciencias Físicas, Ingenierías y especialidades conexas que nos permitiesen desarrollar capacidades propias relacionadas con las tecnologías más avanzadas que, en ese momento, comenzaban a eclosionar en el mercado.

La formación que se ofrece a este alumnado es el de analista de inteligencia de nivel básico y, durante su estancia, se les proponen trabajos y problemas que nos ayuden en nuestro proceso de mejora continua de capacidades.

En el nuevo escenario de desarrollo de sus competencias se apuesta por incidir en su capacidad crítica y el desarrollo de habilidades culturales de índole transversal, con frecuentes encuentros para el debate que sean generadores de una necesaria «inteligencia colectiva» orientada a objetivo (Rey, 2022). Estas sesiones son registradas y transcritas para, haciendo uso de sistemas

de inteligencia artificial, incorporar el conocimiento generado a las ontologías semánticas propias del ecosistema desarrollado.

Configurar equipos estables y pluridisciplinares de análisis de Inteligencia de Fuentes Abiertas requiere capacidades de acceso a talento y organizativas comparables a las que despliegan las unidades de Inteligencia de grandes Corporaciones, en nuestro caso, con el problema añadido de la altísima rotación y de la necesidad de un control exhaustivo de la información de nuestros equipos en prácticas.

El proceso de entrenamiento del equipo comienza por la superación de dos cursos en línea que permiten, por un lado, conocer el entorno y el contexto en el que se van a desarrollar las labores de análisis: la Guardia Civil. Una Institución de Seguridad Pública. Ello tiene una importancia estratégica dado que el estudiantado, proveniente, fundamentalmente, de un entorno «urbanita», tiene un conocimiento limitado no ya de la seguridad del Estado y de la seguridad ciudadana, sino de la propia Guardia Civil, a la que conecta de forma inmediata con sus competencias de tráfico, desconociendo todo de sus misiones y capacidades reales.

Este hecho induce la necesidad previa de una capacitación en el conocimiento de las antedichas misiones y del «modelo semántico» adecuado para que los equipos puedan comunicarse entre ellos y con el decisor estratégico a través de sus informes.

El entrenamiento se dirige a configurar un modelo de «cultura general compartida» en las dos áreas de conocimiento y competencia para el CAP: el análisis de inteligencia y el diseño de escenarios de futuro. Dos herramientas complementarias y fundamentales para configurar una estructura de apoyo a la toma de decisión orientada a las necesidades de un entorno VUCA como el actual.

Una vez superada esta formación inicial en la que, como reiteramos, se ha construido el campo semántico adecuado, se procede a aplicar las herramientas disponibles a través de ejemplos específicos, a través de los cuales se entrenan las capacidades de generación del *prompting* adecuado para definir un contexto, unos objetivos y una determinación de fuentes y planificación de investigación adecuadas al objetivo marcado.

De forma recursiva y haciendo uso constante de metodología DELPHI para la mejora del producto final, ya sea a partir de la optimización en la fase de generación como en la fase final de aprobación del producto que pase a la fase de diseminación.

La experiencia, una vez generadas las estructuras de conocimiento y flujos de información, puede calificarse como óptima, toda vez que todas estas cohortes de estudiantado se caracterizan por un conocimiento y uso de las capacidades tecnológicas que se puden calificar de sobresaliente.

Veamos una representación gráfica del proceso que se puede seguir, de forma interactiva, a partir de la URL: https://ciberinteligencia.eu/interacciones/analistas/.

Por todo lo antedicho, se cierra el círculo y, siendo nuestra misión entrenar a este estudiantado en capacidades básicas de análisis y de diseño de futuros, se dedica su talento a la revisión final de los productos generados de manera casi automática por las herramientas de inteligencia artificial que ponemos a su disposición para la generación de informes para decisor estratégico. Además, sus propias aportaciones, como se ha reseñado, pasan a ser parte del conocimiento compartido tanto dentro de cada cohorte como para cohortes posteriores lo que, al final, constituye una de las mejores externalidades positivas conseguidas: La persistencia del conocimiento, independientemente de las personas. Todo el conocimiento generado pasa, de forma automática, a formar parte de la ontología de conocimiento del CAP, de tal manera que podrá ser utilizada, en una fase posterior, para la realización de un tuneado fino recursivo del modelo, de tal forma que se minimice la posibilidad de que se produzcan «alucinaciones» en el proceso de análisis.

Se comprueba, por tanto, que la diversidad (que no solo las capacidades pluridisciplinarias) adquiere todo su sentido en el caso que nos ocupa. Edad, sexo, ideología, conocimiento diverso..., sin duda, enriquecen la calidad del producto del análisis y, por ende, la capacidad de detección de posibles alucinaciones en el producto generado por la IA.

5 Alucinaciones y otras cuestiones: una aproximación práctica

Las IA generalistas, aunque avanzan rápido en materia de pensamiento profundo, aún tienen problemas graves para el manejo de cierta información relacionada con entidades específicas. La mayoría de nosotros hemos hecho la prueba de preguntarle a la IA qué sabe de nosotros mismos y hemos sido conscientes del desastroso resultado que ha presentado, aunque, es necesario reconocerlo, la precisión avanza a una velocidad incontestable.

Imaginemos un resultado parecido al valorar una entidad persona, física o jurídica, una geolocalización o un vehículo, por poner ejemplo de interés para la Seguridad Interior. Esas «alucinaciones» harían inviable el uso de procesos de automatización en investigación policial o, peor aún en un escenario de teatro de operaciones de cualquier tipo.

Los modelos de lenguaje entrenados con objetivos generales tienen, entre otras, esta fundamental, podría denominarse, tara. Eso las transformaría en herramientas prácticamente inútiles para la generación de Inteligencia por la imprecisión o, aún peor, por la evidente tendencia a contestar inventándose las respuestas.

Afortunadamente, además de la mejora exponencial de sus capacidades y precisión que ya se ha enunciado con anterioridad, existen posibles soluciones, hasta el momento parciales y sujetas a revisión, para la mitigación de este problema.

¿Cómo se podría mejorar la calidad y actualización de los datos que han de nutrir las respuestas de los modelos de lenguaje para que resulten confiables?

La generación de modelos específicos, de agentes especializados, de ontologías semánticas adaptadas o de grafos de conocimiento, permiten mejorar la precisión de las respuestas de la IA generativa, así como mitigar las posibles alucinaciones de esta, de forma sectorial.

Vamos a entrar en el detalle en este conjunto de tecnologías, a nuestro juicio, justo estos son los elementos fundamentales para poder hacer un uso intensivo y preciso de los sistemas de inteligencia artificial generativa en los procesos de generación de Inteligencia, en el caso del CAP, a partir de fuentes abiertas.

El documento Ontology Learning for Hybrid Threats (Bosso y Ruberto, 2025), en el que se recomienda el uso de la herramienta HYBOLT que se describe como:

> «una herramienta para el aprendizaje de ontologías aplicada al análisis de amenazas híbridas. Se propone usar modelos de lenguaje extenso (LLM) y grafos de conocimiento (KG) para extraer información fiable de fuentes abiertas, mitigando problemas como las alucinaciones de los LLM. La metodología se

centra en la extracción de tripletas sujeto-acción-objeto para construir un KG, simplificando la información para mejorar la precisión. Se evalúa el rendimiento de HYBOLT en tareas como la extracción de ubicaciones y cantidades de individuos afectados, mostrando una alta precisión y resistencia a las alucinaciones».

Este documento ofrece, a nuestro juicio, las líneas maestras básicas a explorar para conseguir los resultados deseados.

Tras «dialogar» con un sistema de fuentes relacionadas con conocimiento sobre ontologías semánticas y otras estrategias asociadas, aplicadas al análisis de inteligencia, se ha obtenido el conocimiento suficiente para intentar desarrollar un conjunto de pautas con el objetivo de generar un ecosistema consistente de mitigación de riesgos asociados a posibles alucinaciones de la IA generativa durante el proceso de generación de informes de Inteligencia dentro de nuestro Centro de Análisis y Prospectiva, orientados a la Seguridad Interior.

Con el fin de mejorar la precisión de una IA generativa en un sector específico a partir de servicios de IA generativa generalistas, se ha considerado implementar las siguientes estrategias:

— **Utilizar bases de conocimiento formales (Knowledge Graphs – KG) para corregir las limitaciones de los Modelos de Lenguaje Grandes (LLM)** (Dieter Fensel, 2020). Los LLM pueden sufrir de alucinaciones, sesgos y falta de conocimiento, en especial, en campos específicos como el análisis de amenazas híbridas. Las bases de conocimiento, como los grafos de conocimiento (KG), proporcionan información estructurada y verificada para mejorar la calidad de las respuestas de los LLM. Estas bases de conocimiento se nutrirían de fuentes abiertas consolidadas y, de manera recurrente, con productos propios validados y correctamente etiquetados. Se entraría, por tanto, en un proceso de mejora continua de la calidad de la información manejada y utilizada para generar nuevo conocimiento.

— **Implementar un sistema que transforme texto no estructurado en datos estructurados**. Este sistema incluye una herramienta de aprendizaje de ontologías, diseñada para inferir un KG específico del dominio Seguridad Interior a partir del texto y poblarlo con datos de alta calidad. En la actualidad, desde el CAP se está evaluando el servicio Protegé[5], de la Universidad de Stanford, para la generación de una ontología semántica específica de Seguridad Interior. Se ha iniciado la generación a partir de subdominios específicos dado que la tarea de generar una ontología semántica de Seguridad Interior requeriría recursos y equipos, ahora mismo, inalcanzables por nuestro equipo.

[5] Véase: https://protege.stanford.edu/

— **Aprovechar las capacidades básicas de los LLM**. En lugar de depender de conocimientos específicos del campo o de razonamiento lógico complejo, se pueden usar las capacidades básicas de los LLM, como el reconocimiento de patrones gramaticales (sujeto, acción, objeto), para extraer información y crear KG. Esto minimiza los sesgos y alucinaciones, ya que solo se requieren habilidades lingüísticas básicas. Apoyarse en las propias capacidades de los LLM para la generación de los KG constituye la herramienta básica para asegurar la eficiencia del proceso. La generación de KG es un proceso complejo y costoso que minora los recursos necesarios para llevarlo a efecto, haciendo uso de las propias herramientas de Inteligencia Artificia generativa disponibles[6].

— **Atomizar entidades para crear grafos de conocimiento más simples e informativos**. Este proceso implica simplificar los nombres de las entidades y agregar información adicional como atributos, lo cual hace que los grafos sean más legibles y fáciles de analizar. Etiquetar correctamente las entidades y hacer un diseño coherente de sus atributos constituye un elemento fundamental a la hora de tener éxito en la implementación del ecosistema. Para llevar a cabo esta acción se precisa de la incorporación de talento específico. Se ha procedido a ampliar las ofertas de incorporación de personal en prácticas a las áreas de conocimiento necesarias para trabajar en el sentido expuesto.

Pongamos un ejemplo para entender mejor el concepto.

Imaginemos una noticia de fuente abierta de interés para una investigación.

«El empresario Juan Pérez, CEO de la empresa tecnológica Neuronix, se reunió en Madrid con representantes del Ministerio de Ciencia para discutir una posible colaboración en inteligencia artificial».

Se procedería a ejecutar un proceso de extracción de entidades, atomización de estas y generación de los grafos de conocimiento simples y representativos de la siguiente forma:

Paso 1: extracción de entidades (sin atomizar)

En un inicio, se extraerán las entidades detectadas de la siguiente forma:

— Juan Pérez.
— Neuronix.
— Ministerio de Ciencia.

[6] Se puede acceder a un ejemplo visualmente muy atractivo en la sede del Tribunal Constitucional. Dominio Derecho Constitucional desde la URL: https://hj.tribunalconstitucional.es/es/Descriptor/Index?vista=1.

— Madrid.

— Inteligencia artificial.

Pero esto puede generar un grafo poco claro si las relaciones entre entidades no están bien definidas.

Paso 2: atomización de entidades

Atomizar significa dividir entidades complejas en componentes más simples y específicos. Así, se pueden representar las relaciones entre las mismas de forma mucho más clara.

Entidades atomizadas:

- Persona: Juan Pérez.
- Rol: CEO.
- Organización: Neuronix.
- Ubicación: Madrid.
- Institución gubernamental: Ministerio de Ciencia.
- Tema: Inteligencia artificial.
- Evento: Reunión.
- Relación: Colaboración potencial.

Paso 3: construcción del grafo de conocimiento

Con las entidades atomizadas, se construirá el grafo a partir de estas relaciones entre las mismas:

- Juan Pérez → ocupa el rol de → CEO.
- CEO → de → Neuronix.
- Juan Pérez → participó en → reunión.
- Reunión → ubicación → Madrid.
- Reunión → con → Ministerio de Ciencia.
- Reunión → tema → Inteligencia artificial.
- Ministerio de Ciencia → interesado en → colaboración.
- Neuronix → interesado en → colaboración.

De esta forma, se estructuraría el conocimiento de tal forma que se podría alimentar nuestra ontología de forma mucho más segura y firme, con conocimiento estructurado que minimizaría la posibilidad de error por parte del LLM.

— **Utilizar un enfoque de *human-in-the-loop***. Aunque se puede automatizar parte del proceso de aprendizaje de ontologías, es importante que un experto revise y ajuste la salida generada por la IA. Nuestro circuito de validación actual debería poder implementar la revisión por pares del producto final. De momento, esta revisión se asigna a un único analista que comprueba coherencia del documento sin entrar en elementos de precisión salvo detección de alucinación lo que induce un conjunto indeseable de riesgos. Valoramos el riesgo residual subyacente como adecuado, en función del tiempo.

— **Construir ontologías de manera semiautomática**. Se pueden usar un LLM para generar preguntas de competencia para el desarrollo de ontologías y convertir oraciones de lenguaje natural en axiomas OWL (W3C, 2025), reduciendo el esfuerzo asociado con la creación manual. El apoyo del propio LLM en esta tarea es fundamental para la obtención de resultados y, sobre todo, el mantenimiento de la precisión del sistema. El ya referenciado Protegé constituye una valiosa herramienta para acometer este proceso de automatización.

— **Implementar estrategias de validación de conocimiento**. Se pueden comparar las respuestas del LLM con la información de fondo de los grafos de conocimiento, verificando la coherencia y la veracidad de la salida. También se pueden utilizar grafos de conocimiento como entrada en procesos de inferencia de múltiples pasos, limitando aún más el riesgo de alucinación. Esta actividad la se integrará en el proceso de auditoría de la calidad de las respuestas. En un proceso de mejora continua. Probablemente, podrá ser automatizada en el futuro. En este momento, en el CAP se está estudiando la posibilidad de dedicar parte de los recursos disponibles a entrenar estas capacidades con el fin de validar, de forma más ajustada, la calidad de los análisis obtenidos.

— **Usar un modelo de lenguaje más pequeño, con menos parámetros**. Modelos más pequeños, pueden ejecutarse de forma local sin necesidad de recursos computacionales externos, ahorrando energía y permitiendo la posibilidad de usar la complejidad del modelo para futuras necesidades. Esta acción ha de complementarse con bases de conocimiento específicas, con alta calidad de sus datos, que, de alguna manera, permitan «sectorizar» el modelo. Se estudia la posibilidad de creación de agentes específicos que minimicen los tiempos de respuesta, orientados a tareas específicas relacionadas con determinados procesos de toma de decisión o de obtención de información acotada sobre un determinado asunto o entidad.

— **Utilizar la estructura gramatical del texto para la extracción de conocimiento**. El sistema puede identificar y extraer elementos

como sujeto, acción y objeto utilizando una estrategia de *few-shot prompting*[7].

— **Descomponer los nombres de las entidades en componentes más pequeños**. El sistema puede usar LLM para dividir los nombres de las entidades en nombre principal y atributos, lo que permite la creación de entidades simplificadas y enriquecidas, más manejables para su incorporación en otros procesos más complejos. En el CAP, hemos hecho pruebas de extracción y atomización de entidades en determinados documentos para, a partir de los mismos, generar KG sobre los que trabajar en la mejora de la eficiencia y precisión de la respuesta. Aún en proceso de refinado, los resultados son muy prometedores.

— **Asegurar la consistencia de las entidades**. El sistema puede comparar las entidades atomizadas con las originales para garantizar que la misma entidad no sea convertida en diferentes entidades con nombres similares. La consistencia ha de asegurarse para que la precisión no se resienta.

— **Implementar diferentes estrategias para construir una base de conocimiento coherente**. Esto puede ser por medio de estrategias de alta o baja resolución en la validación de entidades de texto con entidades de una base de conocimiento existente. En nuestro sectorial específico, de Seguridad Interior, esta acción es fundamental para mitigar el riesgo de alucinaciones. La coherencia de la base de conocimiento y una ontología semántica precisa son las herramientas fundamentales de mitigación de alucinaciones.

— **Mejorar la calidad de las instrucciones que se dan al LLM en los *prompts***. Se pueden comparar los diferentes grafos de conocimiento generados por diferentes «prompts» para determinar cuál es el más prometedor. Forma parte de las capacidades que han de desarrollar los y las nuevas analistas: ser capaces de contextualizar desde diferentes ángulos una determinada necesidad y, por ende, ser capaces de expresar esa contextualización en «prompts» que generen respuestas de calidad diversa para poder escoger la más adecuada para el escenario propuesto. Entrenar al equipo de analistas para desarrollar estas capacidades específicas y, más aún, que el conocimiento adquirido en esta materia goce de persistencia constituye el «core de negocio» de estos nuevos equipos de analistas. No registrar el ecosistema de *prompts* de manera adecuada ha sido un error que

[7] Se trata de una técnica de aprendizaje automático que permite a los modelos de lenguaje aprender a realizar una tarea nueva con solo unos pocos ejemplos. En lugar de entrenar el modelo en un conjunto de datos masivo, se le proporcionan algunos ejemplos de la tarea y se espera que generalice a partir de ellos para realizar la tarea en nuevas entradas.

se ha cometido durante el desarrollo de las nuevas metodologías automatizadas de análisis.

— **Implementar el método de *Retrieval Augmented Generation* (*RAG*)**. Se puede usar una base de datos vectorial para realizar el seguimiento de los grafos de conocimiento importantes cargados por el usuario (memoria declarativa) o las interacciones previas usuario-LLM (memoria episódica). La implementación de un RAG es un proyecto complejo y dependiente de acciones previas que, aunque estudiada, pasaría a formar parte de una evolución de nuestras capacidades actuales. Fundamentalmente orientada al mantenimiento proactivo del dominio semántico.

Todo lo antedicho puede representarse gráficamente de la siguiente forma:

Pueden acceder al contenido del gráfico interactivo desde: https://ciberinteligencia.eu/interacciones/mitigacion/.

6 Conclusiones

El análisis de inteligencia de fuentes abiertas dispone de una herramienta, la inteligencia artificial generativa, que ha abierto un nuevo escenario en este sector.

Las capacidades multiidioma, la multimodalidad y el multimodelo LLM constituyen una oportunidad para los equipos de análisis de inteligencia en

su objetivo de detección temprana y acceso a información de fuente abierta de interés para la decisión estratégica pudiendo realizar un tratamiento desde diversos modelos culturales proporcionados por los entrenamientos de los LLM, con lo que es posible disminuir los posibles sesgos y, gracias a ello, mejorar la precisión de los análisis automatizados.

El problema de las alucinaciones, sobre todo, las asociadas a entidades específicas, constituye un riesgo de confiabilidad de los análisis. En este artículo, se han glosado posibles metodologías y acciones orientadas a la mitigación del antedicho problema. Algunas de las mismas ya están siendo estudiadas para implementación en nuestra factoría de inteligencia de fuente abierta, de tal forma que se substituya parte del trabajo manual de los equipos por herramientas y procesos automatizados que, además, mejoren de forma recursiva la calidad de los análisis.

El continuo desarrollo de nuevas capacidades de tipo agéntico, planificación y ejecución automatizada de procesos de investigación de fuente abierta, por parte de los nuevos modelos de razonamiento profundo sorprenden a diario por su precisión y calidad de los productos generados que, sin duda, pasan a ser base de trabajo para el inicio de la acción de validación final de contenidos por parte del analista humano mejorando, exponencialmente, la eficiencia del proceso y los tiempos de respuesta.

El conocimiento generado, además, es incorporado al corpus de conocimiento especializado de la Institución, lo que permite el desarrollo de una ontología semántica especifica con la que trabajar, de forma recursiva, en el reentrenamiento de modelos adaptados a las necesidades de la Institución. Reduciendo, al tiempo, la posibilidad de errores o alucinaciones durante los procesos de análisis.

Al aplicar estas técnicas, es posible construir sistemas de IA generativa más precisos, confiables y adaptados a dominios específicos, lo que mejora la calidad de la información extraída y reduce la posibilidad de errores o alucinaciones.

Parte de estas técnicas y metodologías de mejora recursiva de los modelos ya están en estudio para ser aplicadas en el proceso de evolución de las capacidades de análisis del CAP. Requerirán del desarrollo de proyectos específicos asociados a una visión estratégica que ha de determinar cuáles son los objetivos y misiones que habrá de llevar a cabo nuestra unidad especializada en análisis de inteligencia de fuentes abiertas para que el desarrollo y despliegue sea capaz de cumplir con la misión encomendada.

Por supuesto, la asignación de recursos económicos y la captación del talento para una explotación intensiva y eficiente de estas herramientas constituye, ahora mismo, el principal de los objetivos del CAP en el corto y medio plazos.

Estamos aprendiendo, a veces, a través del error y, desde luego, gracias al mismo. No hay que temer al error. Estamos en un proceso de exploración metodológica en el que la recompensa promete ser de muy alto nivel. El proceso de mejora en la precisión de los análisis haciendo uso de herramientas de inteligencia artificial está en evolución y sometido a la posibilidad de fracasos parciales pero los resultados que estamos obteniendo, sin duda, nos anticipan la disponibilidad de un conjunto de conocimientos y herramientas que harán que manejar la complejidad no sea un sueño inalcanzable.

No nos resistamos al cambio porque, precisamente, ese cambio es el que nos abre alguna oportunidad de éxito en el futuro.

Bibliografía

AENOR. (2018). UNE 166006:2018. Gestión de la I+D+i: Sistema de vigilancia e inteligencia competitiva. Obtenido de https://en.tienda.aenor.com/norma-une-166006-2018-n0059973

Dieter Fensel, U. Ş. (2020). Knowledge Graphs: Methodology, Tools and Selected Use Cases. Springer.

Francesco BOSSO, Stefano RUBERTO. (2025). EU Science Hub. Comisión Europea. Obtenido de https://publications.jrc.ec.europa.eu/repository/bitstream/JRC140863/JRC140863_01.pdf

Guldenmund, F. W. (2000). The nature of safety culture: A review of theory and research. Safety Science, 215-257.

IA, G. (2025). Fuentes de error en la inspiración humana.

Kahneman, D. (2012). Pensar rápido, pensar despacio. Debate.

Khan, M. A. (2024). Impact of Artificial Intelligence on the Global Economy and Technology Advancements. Artificial General Intelligence (AGI) Security, 147–180.

Mosqueira-Rey, E. H.-P.-R.-B.-L. (2023). Human-in-the-loop machine learning: A state of the art. Artificial Intelligence Review 56, 3005–3054.

Rey, A. A. (2022). El libro de la Inteligencia colectiva. Almuzara.

Soliman, M. M. (2024). Artificial intelligence powered Metaverse: Analysis, challenges and future perspectives. Artificial Intelligence Review, 57, Art. 36.

Storey, V. C. (2025). Generative Artificial Intelligence: Evolving Technology, Growing Societal Impact, and Opportunities for Information Systems Research. Information Systems Frontiers.

W3C. (2025). Estándar OWL. Obtenido de W3C: https://www.w3.org/2007/09/OWL-Overview-es.html

ECySAP y la conciencia situacional en operaciones de guerra multidominio

Antonio Legaz
Juan Tejero
José Francisco Suárez Mulero

Resumen

El artículo analiza el papel de ECySAP (Enhanced Cyber Situational Awareness Platform) como plataforma integral para la generación de conciencia situacional cibernética (CySA) en el contexto de operaciones militares multidominio. A partir de una evolución conceptual desde el «coup d'œil» de Clausewitz hasta el modelo de Endsley adaptado al ciberespacio, se expone cómo ECySAP permite percibir, comprender y proyectar amenazas en entornos complejos, facilitando la toma de decisiones, la planificación operativa y la gestión de riesgos. Se detalla su arquitectura funcional, su potencial integración con inteligencia artificial y su papel como habilitador de la guerra mosaico, donde la interoperabilidad y la sincronización entre dominios son clave. A través de un caso de uso hipotético basado en la anexión de Crimea, se ilustra cómo ECySAP podría haber contribuido a mitigar riesgos, detectar campañas de desinformación y proteger infraestructuras críticas, alineándose con doctrinas OTAN y marcos normativos europeos.

Palabras clave

Conciencia situacional, Guerra multidominio, Guerra mosaico, Ciberdefensa, Inteligencia artificial.

ECySAP and situational awareness in multi-domain warfare operations

Abstract

The article analyzes the role of ECySAP (Enhanced Cyber Situational Awareness Platform) as an integral platform for cyber situational awareness generation (CySA) in the context of multi-domain military operations. Based on a conceptual evolution from the "coup d'œil" of Clausewitz to the Endsley model adapted to cyberspace, it is exposed how ECySAP allows to perceive, understand and project threats in complex environments, facilitating decision making, operational planning and risk management. It details its functional architecture, its potential integration with artificial intelligence and its role as enabler of mosaic

warfare, where interoperability and cross-domain synchronization are key. Through a hypothetical use case based on the annexation of Crimea, it illustrates how ECySAP could have contributed to mitigating risks, detecting disinformation campaigns and protecting critical infrastructure by aligning with NATO doctrines and European regulatory frameworks.

Keywords

Situational Awareness, Multidomain Operations, Network-Centric Warfare, Cyberdefence, Artificial Intelligence.

1 Fundamentos de la Conciencia Situacional Cibernética (CySA)

1.1 Del Coup d'Oeil a la Conciencia Situacional Cibernética: transformación del paradigma militar

El concepto de «coup d'œil», definido por Carl von Clausewitz, hace referencia a la capacidad de un líder para percibir de manera intuitiva y rápida la verdad en una situación compleja. Clausewitz describía esta acción como un ejercicio basado en el instinto y la sensación de la verdad, sin apoyo en datos cuantificables o en análisis extensivos. En el contexto de los campos de batalla tradicionales, caracterizados por una estructura lineal y una relativa claridad en las operaciones, la intuición combinada con el discernimiento y la previsión permitía a los comandantes tomar decisiones oportunas y efectivas. Sin embargo, la naturaleza del conflicto ha evolucionado de manera drástica con la irrupción del dominio cibernético, el cual ha redefinido los métodos y desafíos de la toma de decisiones.

El actual entorno cibernético se caracteriza por su complejidad, dinamicidad y alto grado de incertidumbre. A diferencia de los conflictos tradicionales, este dominio se ve marcado por la interconexión global, la rapidez de los acontecimientos y la multiplicidad de actores involucrados, lo que limita la efectividad de una toma de decisiones basada exclusivamente en la intuición individual. La toma de decisiones en el ciberespacio se enfrenta a una «niebla de guerra» más densa que nunca, donde las amenazas evolucionan rápido y los adversarios utilizan tácticas cada vez más sofisticadas. En este contexto, la Conciencia Situacional Cibernética (Cyber Situational Awareness, CySA) surge como una necesidad imperativa para comprender y actuar de manera eficaz en este escenario.

1.2 Evolución histórica de la conciencia situacional: de Sun Tzu al entorno digital

El concepto de conciencia situacional ha adquirido una relevancia fundamental en múltiples disciplinas, en especial, en el ámbito militar. Aunque el término es relativamente reciente, la esencia de esta capacidad cognitiva, es decir, la percepción, comprensión y proyección del entorno para una toma de decisiones efectiva, ha sido reconocida y aplicada en la estrategia y táctica militar desde tiempos antiguos.

Desde la antigüedad, los líderes militares han reconocido la importancia de una percepción clara del entorno para la planificación y ejecución de operaciones. En *El arte de la guerra*, escrito por Sun Tzu en el siglo v a. C., se enfatiza la necesidad de conocer tanto al enemigo como a uno mismo como un principio esencial para la victoria. La afirmación «Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cien batallas» ilustra

una concepción temprana de la conciencia situacional, basada en la comprensión del contexto y la anticipación de las acciones del adversario.

En los siglos XVIII y XIX, la literatura militar europea reflejaba esta misma preocupación por la percepción del entorno. En los tratados de estrategia de la época napoleónica, se destacaba la relevancia del reconocimiento del terreno, la observación de las condiciones climáticas y la recopilación de información sobre la disposición enemiga. Durante las campañas de Napoleón Bonaparte, por ejemplo, el uso de exploradores y unidades de reconocimiento permitió a los comandantes adaptar sus estrategias en función de información actualizada, demostrando una comprensión implícita de lo que hoy se denomina conciencia situacional.

Con la Primera Guerra Mundial, el concepto evolucionó en el ámbito aéreo. El término «situational awareness» comenzó a emplearse para describir la capacidad de los pilotos de combate para mantenerse conscientes de su entorno y de los movimientos enemigos, una habilidad crucial para la supervivencia en el combate aéreo. Posteriormente, en conflictos como la guerra de Corea y la guerra de Vietnam, los pilotos de la Fuerza Aérea de los Estados Unidos identificaron esta capacidad como el «factor as» (ace factor), es decir, la aptitud para anticipar y reaccionar de manera eficaz ante maniobras adversarias.

1.3 Marco teórico de la Conciencia Situacional Cibernética: el modelo de Endsley en el Ciberespacio

La Conciencia Situacional (SA) se define como la percepción de elementos en el entorno dentro de un volumen de tiempo y espacio, la comprensión de su significado y la proyección de su estado en un futuro próximo (Endsley, 1988). Este concepto ha experimentado una evolución natural hacia el dominio cibernético. La Conciencia Situacional Cibernética (CySA) surge como respuesta a la necesidad de aplicar estos principios al complejo entorno digital contemporáneo, caracterizado por amenazas difusas y en constante evolución (Franke y Brynielsson, 2014).

La adaptación de este concepto al ámbito cibernético no ha sido trivial. Mientras que en entornos físicos la percepción se realiza, principalmente, a través de los sentidos humanos, en el ciberespacio esta percepción depende, sobre todo, de sistemas técnicos y herramientas de monitorización (Barford *et al*., 2010). Esta transición conceptual ha requerido un replanteamiento de los modelos clásicos para incorporar las particularidades del entorno digital.

El modelo de Endsley, ampliamente reconocido, establece tres niveles jerárquicos para la CySA. El primer nivel, la percepción, implica la recopilación de datos del entorno cibernético mediante sensores, dispositivos de monitorización y sistemas de detección de intrusiones (Endsley y Connors,

2008). Esta fase resulta crucial, pues constituye la base informativa sobre la que se construye toda comprensión posterior del escenario cibernético.

El segundo nivel, la comprensión, conlleva el análisis e interpretación de los datos recopilados para formar una imagen coherente de la situación actual. Este proceso requiere no solo capacidades técnicas, sino también contextualización y correlación de eventos, en apariencia, dispares para identificar patrones significativos (Tadda y Salerno, 2010). La comprensión adecuada permite discriminar entre falsos positivos y amenazas reales, optimizando así la asignación de recursos defensivos.

Finalmente, el tercer nivel, la proyección, representa la capacidad para anticipar la evolución futura del escenario cibernético basándose en la comprensión actual de la situación (Onwubiko, 2016). Esta capacidad predictiva resulta fundamental para la planificación estratégica y la implementación proactiva de medidas defensivas antes de que las amenazas potenciales se materialicen.

La relación de la CySA con el concepto de *ground truth* es intrínseca y complementaria. El *ground truth* representa la realidad objetiva del entorno cibernético, con independencia de las limitaciones perceptivas o interpretativas de los analistas (Jajodia *et al*., 2010). Lograr una conciencia situacional efectiva implica aproximarse lo máximo posible a esta verdad fundamental, reconociendo que la complejidad del ciberespacio impone limitaciones inherentes a esta aspiración (McGuinness y Foy, 2000).

1.4 Contexto operativo contemporáneo: guerra multidominio y enfoque mosaico

Las guerras modernas ya no se tratan solo de tener la mayor potencia de fuego o el mejor blindaje, sino también de tener una superior conciencia situacional, la capacidad de procesar información rápidamente y de tomar decisiones más rápido que el oponente (Pulido, 2021). El concepto del ciclo OODA (Observar, Orientar, Decidir y Actuar) se ha vuelto fundamental en la planificación y ejecución de las operaciones militares (Boyd, 1976). Este ciclo destaca por la importancia de la velocidad y la agilidad en la toma de decisiones para obtener una ventaja en el campo de batalla.

La transición hacia las operaciones multidominio surge de la necesidad de los ejércitos de ser capaces de operar simultáneamente en todos estos dominios, reconociendo que las acciones en uno de ellos pueden tener efectos en cascada en los demás (Fojon, 2020). Las operaciones multidominio no se limitan al conflicto armado, sino que abarcan una visión más holística de la estrategia militar. Esto implica la necesidad de coordinar los esfuerzos en diferentes dimensiones, como lo terrestre, marítimo, aéreo, ciberespacial, aeroespacial y el espectro electromagnético.

Esta necesidad de coordinación y de operar en un entorno complejo ha dado lugar al concepto de guerra mosaico, que se basa en la idea de que las grandes plataformas militares pueden ser divididas en una serie de funciones que pueden ser llevadas a cabo por componentes individuales, pero interconectados (Jordán, 2023). Cada uno de estos componentes equivaldría a una pieza de un mosaico, operando en conjunto para lograr un objetivo común. De esta manera, la guerra mosaico busca superar las limitaciones de los sistemas monolíticos y crear una fuerza de combate más adaptable y flexible.

La guerra mosaico se caracteriza por la desagregación de funciones, donde los sensores, los responsables de la toma de decisiones y los ejecutores de acciones se convierten en entidades separadas que se comunican y colaboran en una red (Pulido, 2021). La importancia de la información y la conectividad en este nuevo paradigma es central, pues todos los «tiradores» deben ser capaces de usar la información de todos los sensores, creando una «red de muerte» o «kill web» (López Díaz, 2020). Esta arquitectura no jerárquica y distribuida permite una mayor capacidad de adaptación y resiliencia.

2 ECySAP: plataforma integral para la Conciencia Situacional Cibernética

ECySAP funciona como una plataforma integrada y modular que facilita el traslado de información sobre incidentes, amenazas, riesgos e impactos en el plano cibernético, a los diferentes efectos y objetivos de las misiones. Esto se alinea con el concepto de un Cyber Common Operational Picture (CyCOP), cuyo objetivo es integrar y contextualizar numerosos flujos de datos y puntos de datos para acelerar la conciencia situacional cibernética (Kim *et al*., 2023: 1).

Esta herramienta integral de apoyo al planeamiento y misión multisectorial permite que la información generada se integre de manera efectiva en los procesos de planificación, optimizando la rapidez y precisión en la toma de decisiones (Indra, 2021). La conciencia situacional (SA), aunque ligada a la cognición humana, es esencial para percibir el entorno (Schaberreiter *et al*., 2022: 149, citado en Kim *et al*., 2023: 2) y ECySAP contribuye de manera significativa a este propósito.

Dado el creciente nivel de interdependencia entre dominios físicos y digitales, las operaciones militares y de seguridad deben adoptar un enfoque holístico para lograr una representación precisa del entorno operativo. ECySAP no solo se enfoca en la identificación y mitigación de riesgos cibernéticos, sino que también facilita el análisis, la identificación y validación de elementos clave en múltiples dominios operativos.

2.1 Arquitectura funcional de ECySAP: de la percepción a la proyección

ECySAP se fundamenta en una arquitectura de múltiples niveles diseñada para optimizar la toma de decisiones en entornos operacionales complejos. La estructura de esta se organiza en dos capas principales (figura 1):

— Capa de Misión o *Mission Layer*: incluye los objetivos y tareas de misión, representando el nivel estratégico y táctico de la operación.

— Capa de Sistemas de Información y Comunicación o *CIS Layer*: contiene los servicios y sistemas CIS, responsables de proporcionar la infraestructura tecnológica necesaria para el desarrollo de la misión.

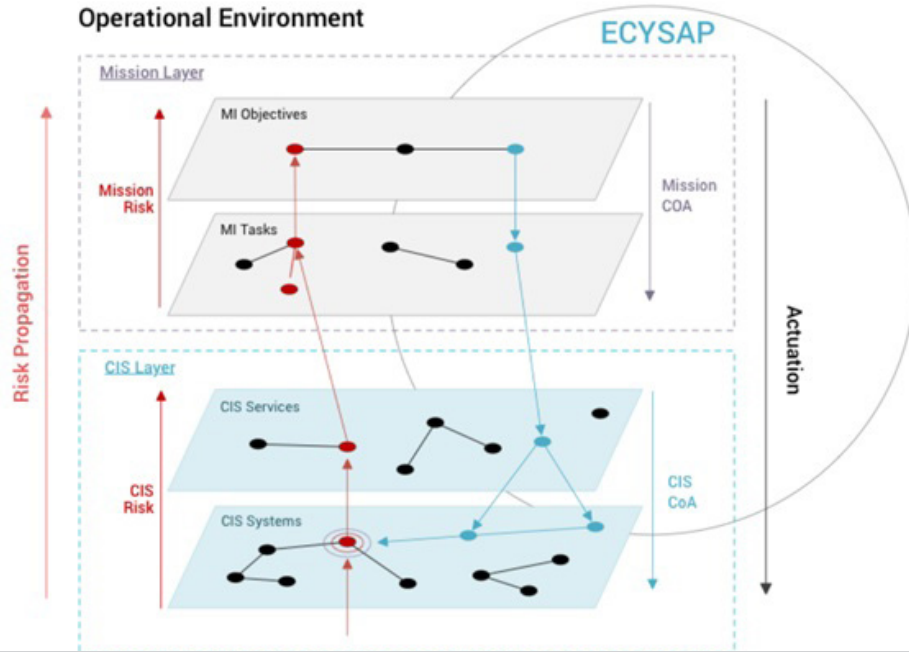


Figura 1. Fuente: ecysap.eu

Uno de los aspectos clave en la arquitectura del ECYSAP es la propagación del riesgo desde los sistemas CIS hasta los objetivos de misión. Los riesgos en la CIS Layer, originados en los CIS Systems y que afectan a los CIS Services, pueden propagarse hacia la Mission Layer, afectando las tareas y objetivos de la misión. Estos fallos o vulnerabilidades en los sistemas de información pueden comprometer servicios críticos, generando impactos adversos en la ejecución de tareas y en la consecución de los objetivos estratégicos.

Para mitigar estos riesgos, se aplican Cursos de Acción (CoA) en la capa de misión y en la capa CIS se recurre a contramedidas. ECySAP puede ayudar en la toma de decisiones para establecer un CoA óptimo, presentando la información de manera detallada tanto en el plano cibernético como en el de misión. De este modo, se facilita la gestión del riesgo y se refuerza la resiliencia operativa ante incidentes cibernéticos.

2.2 Aplicaciones de ECySAP en la planificación operativa y cursos de acción

La información que proporciona ECySAP sobre la materialización de amenazas e incidentes, riesgos e impactos y su repercusión en las misiones es fundamental para la toma de decisiones. Esta información sirve como una vital aportación para comprender la situación en el ciberespacio en términos de impacto (Comunicación Oficial Demostrador, 2025), lo cual es esencial para la planificación de misiones y la definición de Cursos de Acción (CoA), como se describe en el contexto del proceso de planificación operativa de la OTAN (NATO Allied Command Operations, 2010: 4-31).

La planificación operativa implica el análisis de la misión y el desarrollo de COA (NATO Allied Command Operations, 2010: 4-15). Un CyCOP, como el desarrollado por Universitat Politècnica de València, tiene como objetivo generar conciencia situacional cibernética híbrida (CyHSA), fusionando información del dominio cibernético con información georreferenciada de sistemas de comando y control del dominio físico, proporcionando una visión integral para la toma de decisiones (Esteve *et al*., 2016).

ECySAP, al proporcionar información relevante sobre la situación cibernética, puede actuar como una base para la integración con sistemas de soporte a la decisión, permitiendo a los comandantes o responsables de misión desarrollar estrategias y tácticas en misiones de ciberdefensa en un espacio de toma de decisiones basado en una conciencia situacional precisa y adecuada.

Asimismo, esta plataforma desarrolla e implementa herramientas analíticas avanzadas para detectar y evaluar riesgos en el entorno tecnológico, analizando su posible propagación y el impacto sobre los objetivos operacionales. En un futuro, se plantea que el sistema pueda emplear técnicas sofisticadas para el intercambio de información sobre amenazas cibernéticas entre distintos actores, fortaleciendo sus capacidades individuales y colectivas de respuesta a través de la ejecución eficiente de estrategias durante la misión.

2.3 Gestión de riesgos y evaluación de incidentes a través de ECySAP

ECySAP, al proporcionar información clave sobre incidentes, amenazas, riesgos y su impacto en las misiones, facilita y ofrece funcionalidades para

el análisis de riesgos y la evaluación de las consecuencias de los incidentes (Llopis y López, 2024). Este enfoque responde a la necesidad de evaluar el daño de los ataques cibernéticos (Kim *et al*., 2022: 59270-59276, citado en Kim *et al*., 2023) y va más allá de la simple identificación de incidentes, permitiendo una comprensión profunda del contexto operacional en el que se desarrollan las capacidades de los sistemas de información y su impacto en las misiones (NATO Standardization Office, 2024: A-3).

En este sentido, el concepto de conciencia del riesgo situacional cobra relevancia, ya que busca evaluar las amenazas y vulnerabilidades de sistemas sociotécnicos complejos (Chatzimichailidou *et al*., 2015, citado en Kim *et al*., 2023: 6).

Para abordar este análisis de manera estructurada, ECySAP sigue una serie de pasos clave en la evaluación de riesgos y consecuencias:

1. Identificación de activos críticos: se determinan los elementos esenciales, como servidores y firewalls, y su relación con la misión.
2. Evaluación de riesgos y vulnerabilidades: se analizan amenazas mediante métricas cuantitativas, considerando tanto el contexto técnico como el operativo y la misión en curso.
3. Análisis de resiliencia cibernética: ECySAP proporciona los datos en bruto necesarios para que el analista examine la capacidad de los sistemas para resistir ataques y minimizar su impacto.
4. Evaluación del impacto en la misión: se proyectan escenarios para optimizar la toma de decisiones en distintos niveles operacionales.

Este enfoque integral permite a ECySAP proporcionar información relevante en entornos militares, facilitando la planificación de misiones y la definición de cursos de acción (U.S. Army, 2023). Un caso concreto de este proceso sería la identificación de un servidor de correo como un activo crítico para la comunicación en una operación militar. En este escenario, la evaluación no solo contemplaría la vulnerabilidad técnica del servidor ante ataques de denegación de servicio, sino también el impacto que la interrupción de las comunicaciones podría tener en el éxito de la misión (Documento interno, 2024).

2.4 Integración de inteligencia artificial: potenciando las capacidades de ECySAP

La inteligencia artificial (IA) se considera una herramienta clave para mejorar la toma de decisiones, pues permite analizar grandes volúmenes de datos con rapidez, proporcionar soporte dinámico a los decisores y generar propuestas estratégicas (Llopis y López, 2024). En este sentido, la IA facilita la visualización de información al refinar automáticamente las

representaciones en función de los niveles de riesgo, lo que mejora la comprensión de situaciones complejas (Llopis, 2023).

Uno de los principales usos de la IA es la automatización de la detección de *malware* y la gestión de incidentes. Algoritmos de aprendizaje automático, como Ensemble Machine Learning y Self-Adjusting Memory k-Nearest Neighbors, permiten analizar flujos de datos en tiempo real para identificar patrones maliciosos (Llopis, Esteve y Mees, 2023). Estos sistemas pueden detectar comportamientos anómalos que indiquen una infección o un ataque en curso, permitiendo una respuesta rápida y eficiente. Además, la automatización reduce la carga de trabajo de los analistas, liberándolos para tareas más complejas, mientras que los sistemas basados en IA pueden aplicar contramedidas de forma automática, como el bloqueo de direcciones IP maliciosas o el aislamiento de máquinas infectadas.

De igual manera, la IA se emplea para estudiar el comportamiento de los atacantes y elaborar perfiles de ciberataques, identificando las Tácticas, Técnicas y Procedimientos (TTPs) utilizados por grupos de ciberdelincuentes (U.S. Army, 2021). Esta capacidad facilita la anticipación y prevención de posibles amenazas. Además, la IA contribuye a la toma de decisiones en tiempo real al analizar de manera rápida grandes cantidades de datos, ofrece recomendaciones concretas y simula el impacto de diferentes estrategias, lo que permite a los comandantes tomar decisiones mejor fundamentadas.

En el contexto de ECySAP, la plataforma se beneficiará significativamente de la IA, en especial, a través de algoritmos de aprendizaje automático. En la actualidad, ECySAP no cuenta con IA integrada, pero se está desarrollando el proyecto ECySAP EYE para su futura implementación. Esta evolución permitirá a ECySAP mejorar de manera significativa su eficacia, al posibilitar un análisis más exhaustivo de los datos recopilados y transformar información bruta en inteligencia procesable para la toma de decisiones.

2.5 ECySAP en el contexto de la Guerra Mosaico: habilitador de Conciencia Situacional Multidominio

En el contexto de la guerra mosaico, la relación entre la plataforma ECySAP y las redes de efectos es fundamental para comprender la dinámica de las operaciones militares modernas. La guerra mosaico se caracteriza por la desagregación de fuerzas, la adaptabilidad y la creación de múltiples dilemas para el adversario, en lugar de depender de grandes plataformas monolíticas y la confrontación directa (López Díaz, 2020). En este marco, la plataforma ECySAP desempeña un papel crucial al habilitar la conciencia situacional necesaria para coordinar y sincronizar acciones en diferentes dominios, lo que a su vez permite la generación efectiva de redes de efectos (Maestre *et al*., 2022).

La plataforma ECySAP facilita esta visión integral al proporcionar una comprensión profunda del ciberespacio, un dominio que, en la guerra mosaico, tiene un impacto transversal en todos los demás. ECySAP integra información de diversas fuentes, incluyendo sensores físicos y lógicos, para construir una imagen completa de la situación operativa (Maestre *et al*., 2022). Esta capacidad de integración de información es fundamental para la creación de redes de efectos, ya que permite identificar las vulnerabilidades en el sistema del adversario y los puntos críticos que pueden ser explotados para generar el máximo impacto.

En este sentido, ECySAP no solo ofrece información sobre la actividad en el ciberespacio, sino que también permite comprender cómo dicha actividad afecta a otros dominios. Por ejemplo, un ataque cibernético coordinado puede degradar las comunicaciones del enemigo, interrumpir sus sistemas de mando y control, y afectar la precisión de sus armas guiadas, creando así un efecto dominó en otros dominios. Al proporcionar esta visión multidominio, ECySAP se convierte en un habilitador esencial para la planificación y ejecución de redes de efectos que busquen desarticular la capacidad del adversario.

2.6 ECySAP como habilitador de operaciones sincronizadas en entornos multidominio

La efectividad de las operaciones multidominio depende fundamentalmente de la capacidad para sincronizar acciones en diferentes espacios de batalla, generando efectos que se amplifican mutuamente. ECySAP trasciende su rol como mera plataforma de análisis cibernético para convertirse en un elemento vertebrador de la integración entre dominios (Maestre *et al*., 2022). Esta capacidad se materializa a través de diversas funcionalidades que facilitan la transición del paradigma tradicional de operaciones segmentadas hacia un enfoque verdaderamente integrado.

Una de las contribuciones más significativas de ECySAP a las operaciones multidominio es su capacidad para establecer correlaciones entre eventos cibernéticos y sus potenciales manifestaciones en otros dominios. Por ejemplo, la detección de actividades de reconocimiento en redes militares puede correlacionarse con datos de vigilancia electromagnética y movimientos de tropas, proporcionando indicadores tempranos de acciones inminentes en el dominio físico (López-Muñiz, 2023). Esta correlación multidimensional posibilita la identificación de patrones que permanecerían ocultos al analizar cada dominio de manera aislada.

La plataforma incorpora capacidades de análisis predictivo y simulación que permiten a los comandantes y estados mayores explorar escenarios sintéticos y anticipar efectos cruzados entre dominios. Estas funciones se

orientan a evaluar cómo incidentes en el ciberespacio -como ataques contra sistemas de control industrial (SCADA) o la degradación de servicios de posicionamiento satelital (GPS)- pueden impactar sobre la logística militar o la eficacia de sistemas de armas guiadas. Estos ejercicios contribuyen a desarrollar intuición operativa sobre las interdependencias entre dominios, preparando a los decisores para gestionar la complejidad inherente a las operaciones modernas.

Quizá el valor más significativo de ECySAP en el contexto multidominio radica en su contribución a la aceleración del ciclo OODA (Observar, Orientar, Decidir, Actuar). Al proporcionar una visión integrada del entorno operativo que trasciende las divisiones artificiales entre dominios, la plataforma permite a los comandantes identificar oportunidades y amenazas que pasarían desapercibidas bajo enfoques compartimentados tradicionales. Esta aceleración del proceso decisorio constituye una ventaja decisiva en escenarios caracterizados por la alta velocidad de los acontecimientos y la constante evolución de la situación táctica (Pulido, 2021).

3 Marco doctrinal y normativo

3.1 La doctrina en ciberdefensa

La evolución doctrinal de la OTAN en ciberdefensa refleja la transformación del panorama de amenazas global. Desde los primeros ciberataques contra Estonia en 2007, la Alianza ha desarrollado progresivamente un corpus doctrinal robusto, incorporando el ciberespacio como dimensión crítica de la seguridad euroatlántica. La Cumbre de Lisboa (2010) marcó el primer reconocimiento formal de las ciberamenazas en el Concepto Estratégico, pero fue la Cumbre de Varsovia (2016) la que consolidó el *Cyber Security Pledge*, comprometiendo a los aliados a fortalecer sus capacidades nacionales como contribución esencial a la Defensa Colectiva (Warsaw Summit Communiqué, OTAN, 2016).

La evolución continuó en la Cumbre de Bruselas (2018) con el establecimiento del Cyberspace Operations Centre (CyOC) en Mons y en Londres (2019) con la creación del NATO Cyber Security Centre (NCSC). Ambas estructuras operan bajo el NATO Communications and Information Agency (NCIA) y garantizan capacidades defensivas robustas y la protección de redes C3 críticas para el mando y control (Brussels Summit Declaration, OTAN, 2018). La Cumbre de Madrid (2022) profundizó este compromiso, estableciendo el Marco Estratégico Reforzado para la Ciberdefensa, que integra la disuasión, defensa y resiliencia cibernéticas en la postura general de la Alianza (Madrid Summit Declaration, OTAN, 2022).

El documento MC 0665 *NATO Military Concept for Cyberspace Operations* define el enfoque militar aliado para operaciones en el ciberespacio y

estableció tres funciones principales: protección de redes, operaciones defensivas y apoyo a operaciones cinéticas (NATO Military Concept for Cyberspace Operations, OTAN, 2018). Este concepto se desarrolla en la doctrina AJP-3.20, que proporciona directrices detalladas sobre planificación, ejecución y evaluación de operaciones cibernéticas, definiendo procesos para la integración del ciberespacio con operaciones terrestres, marítimas, aéreas y espaciales (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

Los ejercicios *Cyber Coalition* y *Locked Shields* han permitido a la OTAN probar y mejorar sus doctrinas, proporcionando escenarios realistas para validar conceptos operativos. El ejercicio *Crossed Swords* se centra, sobre todo, en técnicas ofensivas dentro del marco legal internacional, permitiendo el desarrollo de capacidades avanzadas para contrarrestar amenazas emergentes (CCDCOE Exercise Reports, OTAN, 2023).

La aplicación del artículo 5 al ámbito cibernético sigue un enfoque de umbral, donde la determinación de un «ataque armado» depende de la evaluación de escala, efectos, intencionalidad y atribución (Strategic Concept, OTAN, 2022). Esta aproximación, respaldada por el Manual de Tallin 2.0, proporciona flexibilidad estratégica mientras establece líneas rojas creíbles frente a adversarios potenciales (Schmitt, 2017).

ECYSAP implementa estos principios doctrinales mediante capacidades de fusión de inteligencia multifuente, análisis avanzado de amenazas y herramientas de respuesta coordinada, alineándose con el concepto OTAN de *Federated Mission Networking* para garantizar interoperabilidad y coherencia operativa en entornos multinacionales.

3.2 Marco normativo

El entramado normativo que sustenta la ciberseguridad europea constituye un ecosistema complejo y multinivel en constante evolución. La Directiva NIS2 (2022/2555) representa su piedra angular, ampliando considerablemente el alcance regulatorio a dieciocho sectores críticos e introduciendo un régimen de supervisión más estricto con sanciones de hasta 10 millones de euros o el 2 % de la facturación global anual. Establece mecanismos de notificación de incidentes en tres fases (24h/ 72h/ 1 mes) y exige medidas técnicas y organizativas proporcionadas al riesgo (La Directiva SRI2, Comisión Europea, 2023).

El Reglamento de Ciberresiliencia (2024/1313) complementa este marco abordando productos conectados, estableciendo requisitos de seguridad desde el diseño y obligaciones para fabricantes durante todo el ciclo de vida del producto. Su enfoque *Security by Design* representa un cambio paradigmático hacia la responsabilidad proactiva (Reglamento de Ciberresiliencia,

UE, 2024). Paralelamente, el Reglamento DORA (2022/2554) establece un régimen específico para el sector financiero, incluyendo pruebas de penetración avanzadas (TLPT) y gestión de riesgos de terceros proveedores críticos (TPRM), reconociendo la interconexión entre estabilidad financiera y ciberseguridad (Parlamento Europeo, 2022).

La Ley de Ciberseguridad (Cybersecurity Act, 2019/881) fortalece el mandato de ENISA y establece el marco europeo de certificación de ciberseguridad, creando esquemas sectoriales como EUCC para productos TIC y EUCS para servicios *cloud* (ENISA Certification Framework, 2023). La Directiva CER (2016/1148) aborda infraestructuras críticas, mientras que el Reglamento eIDAS2 (2023/2084) actualiza el marco de identidad digital, incorporando la *wallet* europea y reforzando los requisitos para servicios de confianza cualificados (eIDAS 2.0, Comisión Europea, 2023).

A nivel nacional, España transpuso la Directiva NIS2 mediante el Real Decreto-ley 3/2024, creando la Oficina Nacional de Ciberseguridad y reforzando las capacidades del CCN-CERT (BOE, 2024). Francia implementó la *Loi de Programmation Militaire* (2019-2025) con disposiciones específicas sobre ciberdefensa y capacidades ofensivas bajo el Commandement de la Cyberdéfense (COMCYBER) (Ministère des Armées, 2022). Alemania adoptó el IT-Sicherheitsgesetz 2.0, otorgando poderes ampliados al BSI para auditar infraestructuras críticas y establecer el *KRITIS-Dachgesetz* para estandarizar la protección sectorial (Germany - Federal Government, 2024). Italia desarrolló el *Perimetro di Sicurezza Nazionale Cibernetica* mediante el Decreto-Legge 105/2019, estableciendo la Agenzia per la Cybersicurezza Nazionale (ACN) como autoridad nacional (Gazzetta Ufficiale, 2021).

Los estándares ISO/IEC 27001:2022 (gestión de seguridad), ISO/IEC 27032:2023 (ciberseguridad), y ISO/IEC 42001:2023 (gobernanza de IA) proporcionan marcos técnicos globalmente reconocidos, mientras que el NIST Cybersecurity Framework 2.0 ofrece un enfoque complementario basado en funciones (identificar, proteger, detectar, responder, recuperar) ampliamente adoptado por organizaciones europeas (ISO/NIST Standards, 2023).

ECYSAP implementa este complejo entramado normativo mediante una arquitectura modular que garantiza el cumplimiento multinivel, incorporando capacidades específicas para la gestión del riesgo regulatorio y la adaptación ágil a requisitos emergentes. Su diseño facilita la interoperabilidad con estructuras nacionales de ciberseguridad y defensa, alineándose con los principios de soberanía digital europea mientras mantiene compatibilidad con estándares OTAN, ejemplificando la aproximación «Brussels-Washington» que caracteriza la ciberseguridad europea moderna (EU Cybersecurity Strategy, 2023).

4 Caso de uso

La anexión de Crimea por parte de Rusia en 2014 representó una operación multidominio compleja, donde las acciones en el ciberespacio jugaron un papel más que importante, como en el caso del ataque al sistema gubernamental ucraniano mediante el uso del arma cibernética «Ouroboros» o también llamada Snake, en marzo del año 2014 (Ross, 2014) o, según declaró la empresa CrowdStrike, el ataque con *malware* en el *software* utilizado en los Obús D-20 de Ucrania, lo que provocó la destrucción de un porcentaje elevado de los mismos (Zaks, 2017). A continuación, vamos a realizar un ejercicio de imaginación hipotético sobre cómo ECySAP podría haber sido utilizada para comprender, gestionar y mitigar los riesgos asociados a esta operación.

4.1 Contexto histórico: guerra mosaico y anexión de Crimea

En febrero de 2014, Rusia ocupó y, posteriormente, anexionó la península de Crimea, territorio de Ucrania. Esta operación constituyó un ejemplo paradigmático de guerra híbrida moderna, combinando operaciones militares convencionales con acciones cibernéticas, guerra de información y operaciones encubiertas. Como señala la evaluación oficial de la OTAN, «la anexión ilegal e ilegítima de Crimea» representó una flagrante violación del derecho internacional y un desafío directo al orden de seguridad europeo (Wales Summit Declaration, OTAN, 2022).

En el caso de Crimea, se observa cómo Rusia implementó una estrategia que combinó elementos discretos, pero coordinados: operaciones cibernéticas contra infraestructuras críticas, campañas de desinformación en medios tradicionales y redes sociales, despliegue de tropas sin insignias «hombres de verde» y acciones diplomáticas para legitimar la anexión. Esta combinación de elementos heterogéneos actuando en concierto ejemplifica los principios de la guerra mosaico, donde la sinergia entre componentes diversos crea efectos que superan la suma de sus partes individuales.

Según el Centro de Estudios Estratégicos e Internacionales (CSIS), la anexión de Crimea marcó el inicio de una nueva era en la conducción de operaciones cibernéticas como parte integral de campañas militares más amplias, estableciendo un patrón que se ha replicado y refinado en conflictos posteriores (CSIS, 2023). La Agencia de Ciberseguridad de Canadá ha documentado cómo, desde 2014, Ucrania ha tenido que mejorar significativamente sus capacidades de ciberdefensa en respuesta a las persistentes amenazas rusas (Cyber Centre Canada, 2022).

En este contexto, una plataforma como ECySAP resultaría especialmente valiosa, ya que proporcionaría la capacidad de integrar información proveniente de múltiples fuentes y dominios, generando una conciencia

situacional unificada que permita contrarrestar las estrategias de guerra mosaico. Al igual que el concepto de guerra mosaico enfatiza la flexibilidad y adaptabilidad de las operaciones militares, ECySAP está diseñada para adaptarse rápido a un panorama de amenazas constantes, proporcionando las herramientas necesarias para mantener la ventaja operativa en escenarios complejos.

4.2 Capas de Análisis de ECySAP en el contexto Crimea-Rusia

En este contexto, desde la perspectiva de ECySAP, el análisis comenzaría con una evaluación de las capas de misión y de sistemas de información y comunicación (CIS). Entre otros objetivos rusos, uno estratégico era asegurar el control de Crimea, protegiendo sus intereses geopolíticos y militares en la región, lo que incluía asegurar la base naval de Sebastopol y proyectar influencia en el mar Negro. Las tareas operativas incluían el despliegue de fuerzas, la realización del referéndum y la integración de Crimea en la Federación Rusa. Por otro lado, los servicios CIS críticos incluían telecomunicaciones, sistemas de información gubernamentales ucranianos, infraestructura de energía y redes de medios, cada uno sujeto a riesgos de ataques cibernéticos dirigidos a interrumpir las comunicaciones, difundir desinformación e influir en la opinión pública.

En el análisis de riesgos y evaluación de incidentes, ECySAP se centraría en la identificación de activos críticos, como servidores gubernamentales ucranianos en Crimea, la infraestructura de telecomunicaciones que conecta Crimea con Ucrania continental y los sistemas de control de la infraestructura energética en la península. Continuaría con una evaluación de riesgos y vulnerabilidades para analizar vulnerabilidades explotables y posibles campañas de desinformación. Un análisis de resiliencia cibernética evaluaría la capacidad de los sistemas ucranianos para resistir ataques y mantener la integridad de la información. Por último, se evaluaría el impacto en la misión proyectando vistas sobre cómo los ataques cibernéticos podrían afectar a una misión específica, la capacidad de Ucrania para responder a la intervención rusa y mantener el control sobre Crimea, así como el riesgo del impacto de la desinformación en la opinión pública y la legitimidad del referéndum.

Si bien, de momento, ECySAP no cuenta con IA integrada, se está desarrollando ECySAP EYE, con lo que, con una posible futura integración de IA, podría mejorar su eficacia en este escenario. Algoritmos de aprendizaje automático podrían analizar el tráfico de red en tiempo real para detectar patrones maliciosos asociados con la actividad rusa. Sistemas basados en IA podrían aplicar contramedidas automatizadas, como el bloqueo de direcciones IP maliciosas o el aislamiento de sistemas comprometidos. Además, la IA podría estudiar el comportamiento de los atacantes rusos y elaborar perfiles de ciberataques, identificando las Tácticas, Técnicas y

Procedimientos (TTP) utilizados, lo que facilitaría la anticipación y prevención de dichas posibles amenazas.

En el contexto de la guerra mosaico, ECySAP podría haber facilitado la coordinación y sincronización de acciones en diferentes dominios, permitiendo la generación efectiva de redes de efectos. Esto implicaría una conciencia situacional multidominio, integrando información de diversas fuentes para construir una imagen completa de la situación operativa. En cuanto a las operaciones sincronizadas, ECySAP establecería correlaciones entre eventos cibernéticos y sus potenciales manifestaciones en otros dominios, como la detección de actividades de reconocimiento en redes militares ucranianas que se correlacionen con movimientos de tropas rusas. La plataforma facilitaría la modelización de *kill chains* multidominio, donde acciones iniciales en el ciberespacio, como la inhabilitación de sistemas de defensa aérea mediante ataques a su infraestructura de red, facilitarían operaciones subsiguientes en el dominio físico como incursiones aéreas.

4.3 Protección frente a la desinformación

En el escenario real de 2014, Rusia desplegó una masiva campaña de desinformación que sentó las bases para su intervención militar. Los medios estatales rusos como RT y Sputnik difundieron narrativas falsas sobre supuestas amenazas a la población ruso-parlante de Crimea, mientras que operaciones encubiertas en redes sociales amplificaban estos mensajes. La doctrina OTAN reconoce la desinformación como un componente integral de las amenazas híbridas, definiéndola como «la difusión intencional de información falsa destinada a engañar y manipular» (NATO's approach to counter information threats, OTAN, 2025).

Si ECySAP hubiera estado operativo en 2014 habría proporcionado capacidades fundamentales para contrarrestar esta campaña de desinformación. La plataforma habría monitorizado en tiempo real los flujos de información, identificando patrones anómalos y narrativas falsas mediante análisis de *big data* y procesamiento de lenguaje natural avanzado. Esto se alinea con el requisito establecido en la Directiva NIS2 de «desarrollar capacidades de detección temprana de amenazas» (Unión Europea, 2022a).

ECySAP habría analizado la difusión de noticias falsas en medios sociales, detectando la creación repentina de miles de cuentas automatizadas (*bots*) antes de la intervención militar, un indicador temprano de una operación coordinada. La plataforma habría correlacionado estas actividades de desinformación con movimientos de tropas rusas, estableciendo patrones que indicaban una operación inminente, proporcionando así lo que la doctrina AJP-3.20 denomina «capacidad de proyección situacional» (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

Adicionalmente, ECySAP habría proporcionado evidencia verificable a autoridades ucranianas y organizaciones internacionales sobre la campaña coordinada rusa, facilitando la atribución de las acciones, un aspecto crítico según la doctrina OTAN para determinar respuestas apropiadas. La plataforma también habría generado contenidos contrastados para contrarrestar la desinformación, contribuyendo a lo que la Política de Ciberdefensa de la UE denomina «resiliencia cognitiva» frente a campañas de manipulación (Comisión Europea, 2022).

4.4 Protección de infraestructura crítica

Durante la crisis de Crimea, Ucrania experimentó numerosos ciberataques contra su infraestructura crítica, incluyendo ataques de denegación de servicio (DDoS) contra sitios web gubernamentales, interrupciones en comunicaciones de telefonía móvil, bloqueo de comunicaciones entre unidades militares y disrupciones en servicios esenciales. La protección de infraestructuras críticas constituye un pilar fundamental tanto de la doctrina OTAN como del marco regulatorio europeo, con la Directiva NIS2 designando dieciocho sectores críticos que requieren medidas reforzadas de ciberseguridad.

La implementación de ECySAP habría proporcionado capacidades significativas para la protección de estas infraestructuras. La plataforma habría detectado temprano los intentos de infiltración en redes críticas ucranianas mediante análisis de tráfico de red y detección de anomalías, cumpliendo con el requisito establecido en el artículo 21 de la Directiva NIS2 de implementar «medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos para la seguridad de las redes y sistemas de información» (Unión Europea, 2022a).

ECySAP habría identificado vulnerabilidades en sistemas SCADA de infraestructura energética, anticipado ataques a redes de telecomunicaciones basándose en patrones observados y monitoreado continuamente redes eléctricas, suministro de agua y sistemas de transporte para detectar anomalías. Esto se alinea con lo que la doctrina AJP-3.20 denomina «protección de infraestructuras de información críticas» (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

Asimismo, de acuerdo con el concepto de «Common Operational Picture» (COP) establecido en la doctrina OTAN MC 0665, que destaca la importancia de una visión compartida del entorno operativo para lograr una acción eficaz, el sistema habría ofrecido a las autoridades una visión unificada del estado de las infraestructuras críticas. Esto habría facilitado la toma de decisiones coordinadas y la priorización eficiente de los recursos defensivos (NATO Military Concept for Cyberspace Operations, OTAN, 2018).

Ante incidentes confirmados, ECYSAP habría alertado automáticamente sobre sistemas comprometidos para que los analistas los aísleran con la mayor celeridad posible y así evitar la propagación de ataques. Además, se podrían haber establecido canales de comunicación alternativos entre instalaciones críticas ante la interrupción de los primarios, implementando así los principios de «segmentación de redes» y «redundancia de sistemas críticos» recomendados por la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023).

4.5 Protección de activos físicos militares

En el escenario de Crimea, los denominados «hombres de verde», soldados rusos sin insignias, tomaron control de instalaciones militares estratégicas, mientras se producía un bloqueo naval de la flota ucraniana, interferencia con sistemas de comunicación militar y deshabilitación de radares y sistemas de defensa aérea. La doctrina OTAN AJP-3.20 reconoce y subraya la creciente interconexión entre los dominios cibernético y físico, afirmando que «las operaciones en el ciberespacio pueden tener efectos cinéticos» (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

ECySAP habría proporcionado capacidades para la protección de activos militares en este escenario. La plataforma habría alertado sobre interferencias electromagnéticas en sistemas de navegación y comunicación militar mediante análisis del espectro electromagnético y correlación con actividades cibernéticas. Habría detectado patrones anómalos de comunicaciones en las cercanías de bases militares ucranianas, proporcionando alertas tempranas de actividades hostiles inminentes.

Un aspecto en particular relevante habría sido la capacidad de ECySAP para identificar la suplantación de señales GPS utilizadas para confundir a unidades ucranianas, una técnica de guerra electrónica empleada por Rusia durante el conflicto. La doctrina OTAN MC 0665 identifica la guerra electrónica como un componente crítico de las operaciones híbridas modernas, estrechamente vinculado a las capacidades cibernéticas (NATO Military Concept for Cyberspace Operations, OTAN, 2018).

La plataforma habría correlacionado eventos cibernéticos con actividades físicas sospechosas alrededor de activos militares, proporcionando un análisis multidominio «Multi-Domain Operations» (Allied Joint Doctrine, OTAN, 2021) que habría facilitado la comprensión holística de la situación.

Además, ECySAP habría proporcionado información necesaria al comandante para valorar rutas seguras para la evacuación o refuerzo de instalaciones críticas, mantenido comunicaciones seguras entre el mando central ucraniano y las unidades desplegadas en Crimea y permitido la operación remota de sistemas defensivos aun después de la ocupación física

de instalaciones. Estas capacidades implementan el principio de «resiliencia operativa» establecido en la Directiva NIS2, que requiere «medidas para asegurar la continuidad de servicios críticos incluso bajo condiciones adversas» (Unión Europea, 2022a).

4.6 Conclusiones caso de uso

El uso hipotético de ECySAP en la anexión de Crimea demuestra cómo una plataforma integral de conciencia situacional cibernética podría ser utilizada para comprender, gestionar y mitigar los riesgos asociados a operaciones multidominio complejas. ECySAP, en este caso, podría haber proporcionado una información valiosa para la toma de decisiones y la planificación de respuestas.

Adicionalmente, aunque se destaca y se recuerda que este planteamiento es meramente un enfoque hipotético basado en las capacidades potenciales de ECySAP, la experiencia de Crimea podría evidenciar cinco características fundamentales de los conflictos contemporáneos que ECySAP sería capaz de abordar:

- La línea entre paz y guerra se difumina en escenarios de conflicto híbrido, creando lo que la doctrina OTAN denomina «zona gris» donde se desarrollan actividades hostiles sin llegar a un conflicto armado declarado (Allied Joint Doctrine, OTAN, 2021). ECySAP proporcionaría herramientas necesarias para detectar y responder a amenazas en este espectro ambiguo.
- En un ambiente bélico, los ataques comienzan en el ciberespacio antes de manifestarse físicamente, siguiendo lo que el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) denomina «modelo de operaciones cibernéticas preparatorias» (CCDCOE, 2023). ECySAP permitiría la detección temprana de estas actividades preparatorias, facilitando respuestas preventivas.
- El sistema ECySAP proporcionaría capacidades para detectar y contrarrestar campañas de desinformación. Esta última prepara el terreno para operaciones militares convencionales, como parte de lo que la doctrina OTAN MC 0665 identifica como «operaciones de información» destinadas a «influir en las percepciones, actitudes y comportamientos» (NATO Military Concept for Cyberspace Operations, OTAN, 2018).
- La Directiva NIS2 reconoce que la integridad de infraestructuras críticas se convierte en objetivo prioritario, y es importante establecer medidas reforzadas para su protección (Unión Europea, 2022a). ECySAP podría proporcionar un marco integrado para la protección de esta tipología de infraestructuras.

5 Conclusiones

En un entorno internacional caracterizado por la competición estratégica y el protagonismo creciente de las operaciones en el ciberespacio, el desarrollo de capacidades avanzadas de Conciencia Situacional Cibernética constituye ya no una ventaja opcional sino un requisito indispensable para la seguridad nacional. Las organizaciones militares y de seguridad que no logren adaptarse a este nuevo paradigma se encontrarán en desventaja significativa frente a adversarios tecnológicamente avanzados.

El futuro desarrollo de la CySA deberá afrontar distintos desafíos, especialmente, en lo relativo a la integración de fuentes heterogéneas de datos, la traducción de indicadores técnicos en implicaciones operativas y la evaluación objetiva de su impacto real. La colaboración entre el ámbito académico, la industria y las organizaciones de defensa resultará crucial para superar estas limitaciones y maximizar el potencial de herramientas como ECySAP.

En última instancia, el valor estratégico de la Conciencia Situacional Cibernética radica en su capacidad para reducir la incertidumbre y acelerar el ciclo OODA en entornos complejos y dinámicos. En un mundo donde la superioridad informativa constituye un factor determinante del éxito operativo, la inversión en estas capacidades representa una prioridad ineludible para cualquier nación que aspire a garantizar su seguridad en el complejo escenario geopolítico del siglo XXI.

Bibliografía

Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2023). *Recomendaciones para la segmentación de redes y sistemas críticos*. Heraklion, ENISA.

Alianza Atlántica. (2022). *Marco estratégico para la ciberdefensa en el ámbito de la OTAN*. Bruselas, OTAN.

Barford, P., Dacier, M., Dietterich, T., Fredrikson, M., Giffin, J., Jajodia, S., y Ou, X. (2010). Cyber Situational Awareness: Issues and Research. *Advances in Information Security*. 46, pp. 3-13.

Boyd, J. (1976). *Destruction and Creation*. U.S. Army Command and General Staff College.

Centro de Estudios Estratégicos e Internacionales (CSIS). (2023). *Cyber Operations during the Russo-Ukrainian War*. Washington, CSIS.

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE). (2023). *Estrategias de operaciones cibernéticas en conflictos modernos*. Tallin, CCDCOE.

Chatzimichailidou, M. M., Protopapas, A., & Dokas, I. M. (2015). Seven issues on distributed situation awareness measurement in complex socio-technical systems. In F. Boulanger, D. Krob, G. Morel, & J.-C. Roussel (Eds.), Complex systems design & management (pp. 89–101). Springer. https://doi.org/10.1007/978-3-319-11617-4_8

Comisión Europea. (2022). *Política de Ciberdefensa de la UE*. COM (2022) 49 final. Bruselas, Comisión Europea.

Comisión Europea. (2023). *La Directiva SRI2: asegurar las redes y los sistemas de información*. Bruselas: Comisión Europea.

Comunicación Oficial Demostrador. (2025). Informe ECySAP: Evaluación de impacto cibernético en operaciones. Documento interno de proyecto.

Cyber Centre Canada. (2022). *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine*. Ottawa, Communications Security Establishment.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. *Proceedings of the Human Factors Society Annual Meeting*. 32(2), pp. 97-101.

Endsley, M. R., y Connors, E. (2008). Situation awareness: State of the art. *2008 IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*. Pittsburgh, pp. 1-4.

Esteve, M., Pérez, I., Palau, C., Carvajal, F., Hingant, J., Fresneda, M. A., & Sierra, J. P. (2016). Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness Improvement. North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO), Technical Report STO-MP-IST-148.

Fojon, E. (2020). Nuevos paradigmas militares en la era de la Competición Estratégica: el caso de las operaciones anfibias y la guerra mosaico. Real Instituto Elcano, ARI 13/2020.

Franke, U. y Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*. 46, pp. 18-31.

Gazzetta Ufficiale. (2021). Decreto-legge 14 giugno 2021, n. 82, convertido en Legge 4 agosto 2021, n. 109: creación de la Agenzia per la Cybersicurezza Nazionale (ACN). https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG; https://www.gazzettaufficiale.it/eli/id/2021/08/04/21A04841/sg

Germany – Federal Government. (2024). Draft KRITIS-Dachgesetz (Ley marco de infraestructura crítica) – Comunicado y documentación.

(Resumen oficial del proceso legislativo 2024). https://www.bmi.bund.de

Indra. (2021). ECySAP: Enhanced Cyber Situational Awareness Platform. *Technical White Paper*.

Indra, Unidad de Ciberdefensa. (2024). *Documento interno*. (Documento no publicado).

Jajodia, S., Liu, P., Swarup, V., & Wang, C. (2010). Cyber situational awareness: Issues and research. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Cyber Situational Awareness: Issues and Research* (pp. iii-iv). (Advances in Information Security; Vol. 46). https://doi.org/10.1007/978-1-4419-0140-8

Jordán, J. (2023). Guerra mosaico: qué es y a qué desafíos se enfrenta. Revista de Aeronáutica y Astronáutica, (920), 160-167.

Kim, J., Jeong, S., Kim, J., & Lee, J. (2022). Study on cyberattack damage assessment framework. IEEE Access, 10, 59270–59276. https://doi.org/10.1109/ACCESS.2022.3179977

Kim, K., Youn, J., Yoon, S., Kang, J., Kim, K., & Shin, D. (2023). Study on Cyber Common Operational Picture framework for cyber situational awareness. Applied Sciences, 13(4), 2331. https://doi.org/10.3390/app13042331

Llopis Sánchez, S. (2023). Decision support elements and enabling techniques to achieve a cyber defence situational awareness capability (Doctoral dissertation, Universitat Politècnica de València).

Llopis Sanchez, S., & Lopes Antunes, D. (2024). Operation assessment in cyberspace: Understanding the effects of cyber deception. Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-8). Association for Computing Machinery. https://doi.org/10.1145/3664476.3672355

Llopis, S., Hingant, J., Pérez, I., Esteve, M., Carvajal, F., Mees, W., & Debatty, T. (2018). A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. In 2018 International Conference on Military Communications and Information Systems (ICMCIS) (pp. 1-7). IEEE.

López Díaz, J. A. (2020). Guerra Mosaico vs Confrontación de Sistemas. Cuaderno de Pensamiento Naval, Número 28, 49-68.

Maestre Vidal, J., Sotelo Monge, M. A., Rodríguez López, F. A., Mateos Calle, M., Estevez Tapiador, J. M., Villagrá González, V., Tornero Sánchez, D., Gómez Henche, R., & Aragonés Lozano, M. (2022). Plataforma Europea para adquisición de Consciencia de Situación

del Ciberespacio. En Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2022) (Vol. 11, pp. xx–xx). Red de Excelencia Nacional de Investigación en Ciberseguridad. https://2022.jnic.es/Actas_JNIC_2022_v11.pdf

McGuinness, B., & Foy, L. (2000). A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS). In Human performance, situation awareness and automation conference; user-centered design for the new millennium (pp. 286-291). SA Technologies.

Ministère des Armées. (2022). Commandement de la cyberdéfense (COMCYBER) – misión y organización (página oficial). https://www.defense.gouv.fr/comcyber

Ministerio para la Transformación Digital y de la Función Pública. (2024, 30 de abril). Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G (BOE núm. 106, pp. 49754–49801). Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-2024-8715

NATO. (2018). NATO Military Concept for Cyberspace Operations (MCCO). https://www.nato.int/cps/en/natohq/

NATO. (2021). AJP-3.20 Allied Joint Doctrine for Cyberspace Operations (Edition A, Version 1). (Edición abierta reproducida) https://iwar.org.uk/wp-content/uploads/2021/06/AJP-3.20-EDA-V1-E.pdf

NATO Allied Command Operations. (2010). Comprehensive Operations Planning Directive (COPD). Norfolk: ACO.

NATO Standardization Office. (2020). *AJP-3.20: Allied Joint Doctrine for Cyberspace Operations* (Edition A, Version 1). North Atlantic Treaty Organization. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

NATO Standardization Office. (2024, abril). AJP-6 (Edition B, Version 1) – Allied Joint Doctrine for Communication and Information Systems. NATO. https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf

North Atlantic Treaty Organization. (2016, July 9). Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

North Atlantic Treaty Organization. (2019, July 11). Brussels Summit Declaration. https://www.nato.int/cps/fr/natohq/official_texts_156624.htm

North Atlantic Treaty Organization. (2022, June 29). Madrid Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_196951.htm

Onwubiko, C. (2016). Understanding cyber situation awareness. International Journal on Cyber Situational Awareness, 1(1), 11–30. https://doi.org/10.22619/IJCSA.2016.100101

OTAN. (2016-2025). *Cyber defence, doctrinas y conceptos militares en ciberseguridad*. Varsovia, Bruselas y Gales, OTAN.

Pulido, G. (2021). Guerra multidominio y mosaico: El nuevo pensamiento militar estadounidense. Los libros de la Catarata.

Real Instituto Elcano. (2020). *Nuevos paradigmas militares en la era de la Competición Estratégica: el caso de las operaciones anfibias y la guerra mosaico*. Madrid, Real Instituto Elcano.

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo. (2024, 23 de octubre). Reglamento sobre requisitos horizontales de ciberseguridad para productos con elementos digitales (Cyber Resilience Act). Diario Oficial de la Unión Europea, L 2847, 20 de noviembre de 2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Ross, A. (2014) Russia's cyber weapons hit Ukraine: How to declare war without declaring war. *The Christian Science Monitor*. [Consulta: 2025]. Disponible en: https://www.csmonitor.com/Commentary/Global-Viewpoint/2014/0312/Russia-s-cyber-weapons-hit-Ukraine-How-to-declare-war-without-declaring-war

Schaberreiter, T., Röning, J., Quirchmayr, G., et al. (2022). A cybersecurity situational awareness and information-sharing solution for local public administrations: The CS-AWARE project. En Challenges in Cybersecurity and Privacy – the European Research Landscape. CRC Press. https://doi.org/10.1201/9781003337492-8

Schmitt, M. N. (ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press.

Tadda, G. P., & Salerno, J. S. (2010). Overview of cyber situation awareness. En S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), Cyber Situational Awareness: Issues and Research (Advances in Information Security, Vol. 46). Springer. https://doi.org/10.1007/978-1-4419-0140-8_2

Unión Europea. (2022a). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE)

n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). *Diario Oficial de la Unión Europea*. 27 de diciembre, L333.

Unión Europea. (2022b). Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012. (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011. *Diario Oficial de la Unión Europea*. 27 de diciembre, L333.

U.S. Army (2023). ATP 3-12.3, Electromagnetic Warfare Techniques. https://irp.fas.org/doddir/army/atp3-12-3.pdf

U.S. Department of the Army. (2021). *Field Manual 3-12: Cyberspace and electronic warfare operations (FM 3-12)*. Headquarters, Department of the Army. https://irp.fas.org/doddir/army/fm3-12.pdf

Zaks, D. (2017). Ukraine's military denies Russian hack attack. *RFI*. [Consulta: 2025]. Disponible en: https://www.rfi.fr/en/contenu/20170106-ukraines-military-denies-russian-hack-attack

La innovación tecnológica en el área de la inteligencia de ciberamenazas y por extensión de la ciberdefensa

Juan Adolfo Montero

Resumen

La ciberseguridad tradicional se enfoca en proteger sistemas de amenazas genéricas, siendo insuficiente frente a actores estatales avanzados con intenciones militares específicas. Para abordar este desafío, surge la ciberdefensa, que integra la inteligencia de ciberamenazas para planificar y conducir operaciones defensivas adaptadas a amenazas concretas.

La ciberdefensa se basa en tres pilares:

- La Misión: garantiza que los sistemas críticos estén protegidos para el éxito operativo.
- La Amenaza: evalúa adversarios, tácticas y herramientas empleadas.
- El Ciberespacio: identifica vulnerabilidades, rutas de ataque y zonas estratégicas para establecer defensas efectivas.

Para mejorar la eficacia defensiva, se han desarrollado tecnologías avanzadas como PICO, una plataforma que integra inteligencia de ciberamenazas y la Gestión de Incidentes y ECySAP, que evolucionará desde un Sistema de Cyber Situational Awarenes hacia un sistema de mando y control de ciberoperaciones.

Además, ambos proyectos (junto a alguno más también en desarrollo) se integrarán en el programa SCOMCE, el cual aplicará tecnologías como Datalakes, inteligencia artificial y simulación para detectar patrones, predecir ataques y automatizar respuestas.

El éxito de la Ciberdefensa dependerá no solo de estas herramientas, sino también de personal altamente capacitado y de una industria tecnológica nacional que garantice independencia estratégica en la protección del ciberespacio militar.

Palabras clave

Ciberdefensa, Ciberespacio, PICO, ECYSAP, SCOMCE.

Technological innovation in the area of cyber threat intelligence and, by extension, cyber defense

Abstract

Traditional Cybersecurity focuses on protecting systems from generic threats, which is insufficient against advanced state actors with specific military intentions. To address this challenge, Cyber Defense has emerged, integrating Cyber Threat Intelligence to plan and conduct defensive operations tailored to specific threats.

Cyber Defense is based on three pillars:

The Mission: Ensures Critical Systems to be protected to guarantee operational success.

The Threat: Assesses adversaries, tactics, techniques, procedures and tools employed.

The Cyberspace: Identifies vulnerabilities, attack routes, and strategic zones to establish effective defenses.

To enhance defensive effectiveness and capabilities MCCE have acquired advanced technologies such as the PICO Platform, that integrates Threat Intelligence and Incident Management capabilities, and will acquire a CYSA capability based on ECYSAP project, which will evolve from a Cyber Situational Awareness System to a Cyber Defense Command and Control System.

Both projects, together with some others already developed for MCCE, will be integrated in the Spanish SCOMCE program. The SCOMCE program will apply technologies like Datalakes, Artificial Intelligence, and Simulation to detect patterns, predict attacks, and automate responses.

The success of Cyber Defense will depend not only on these tools but also on highly trained personnel and a national technology industry that ensures strategic independence in the defence of military Cyberspace.

Keywords

Cyberdefence, Cyberspace, PICO, ECYSAP, SCOMCE.

1 Introducción: la inteligencia de ciberamenazas como base de la transición de la ciberseguridad a la ciberdefensa

Durante años, la ciberseguridad ha sido el eje central del desarrollo tecnológico en materia de protección del ciberespacio[1]. La investigación, desarrollo e innovación (I+D+i) han estado orientados a generar productos destinados, principalmente, al ámbito civil, con el objetivo de hacer frente a amenazas generales y no dirigidas. Este enfoque, lógico dentro de contextos empresariales o institucionales, se centra en la protección básica de sistemas[2] y servicios frente a riesgos comunes en el ciberespacio. (Seguritecnia, 2023)

Sin embargo, al analizar estos mismos productos desde una óptica militar, se revela una carencia importante: no contemplan aspectos tácticos, operacionales ni estratégicos propios de las operaciones militares. Tampoco están diseñados para enfrentarse a amenazas específicas y sofisticadas que afectan directamente a la Defensa Nacional ni responden a las prioridades operativas derivadas de las misiones en curso.

Durante mucho tiempo, las Fuerzas Armadas adoptaron herramientas comerciales de ciberseguridad, aplicándolas en contextos militares con un enfoque similar al civil. No obstante, la realidad del ciberespacio como nuevo dominio de las operaciones ha demostrado que este enfoque resulta insuficiente. Se hace indispensable integrar un modelo más amplio: la ciberdefensa, que complemente la ciberseguridad con un análisis orientado a las necesidades específicas del entorno militar.

En este contexto de ciberespacio de interés militar, los sistemas de ciberseguridad convencionales no son un obstáculo real frente a actores estatales con grandes capacidades y recursos (tecnológicos, económicos y humanos) y con objetivos estratégicos (geopolíticos y militares) claros. Estos adversarios pueden emplear herramientas especializadas para evadir fácilmente los mecanismos tradicionales de protección (ciberseguridad). (Real Instituto Elcano, s. f.)

---

[1] En este artículo nos referiremos como ciberespacio (o a veces, como «sistemas» en general), a cualquier sistema CIS, plataformas o sistema de combate, o sistema de armas que entre sus componentes se encuentra elementos de ***software*** dentro del mismo, así como infraestructuras y servicios civiles dependientes de tecnología IT/OT y que sean soporte de las capacidades militares o de los poderes del Estado y sean, por tanto, críticos para la Defensa y Seguridad Nacional.

[2] Bajo el término «Sistema» nos referiremos en este artículo a cualquier Sistema CIS, plataformas/sistema de combate o sistema de armas que, entre sus componentes, se encuentran elementos de ***software*** dentro del mismo, así como infraestructuras y servicios civiles dependientes de tecnología IT/OT y que sean soporte de las capacidades militares o de los poderes del Estado y sean, por tanto, críticos para la Defensa y Seguridad Nacional.

1.1 ¿Por qué la ciberseguridad tradicional ya no es suficiente? (Rodríguez, 2023)

— Porque los adversarios emplean tecnologías avanzadas capaces de eludir los sistemas convencionales de ciberseguridad.

— Porque las soluciones comerciales están diseñadas y configuradas[3] para identificar amenazas comunes y no están optimizadas para detectar ni neutralizar amenazas específicas dirigidas a las Fuerzas Armadas.

Por esta razón, la ciberdefensa basada en Inteligencia de Ciberamenazas se posiciona como un elemento clave. Este enfoque permite:

— Obtener conciencia situacional del ciberespacio (CySA).

— Apoyar la toma de decisiones tácticas y operacionales y el planeamiento defensivo del ciberespacio con una perspectiva militar.

— Reconfigurar sistemas de ciberseguridad y ciberdefensa para responder de forma concreta a las amenazas específicas[4] que afectan directamente a la misión o a los intereses estratégicos.

Este tipo de inteligencia requiere una Plataforma de Inteligencia de Ciberamenazas (TIP[5]) especializada, capaz de adaptarse a las características únicas del entorno de las operaciones en el ciberespacio de interés militar.

La creciente actividad de servicios secretos, unidades militares de operaciones en el ciberespacio o grupos intermediarios (*proxies*) subvencionados y apoyados por estados y naciones hostiles llevó a que, en 2016, durante la Cumbre de Varsovia, la OTAN reconociera el ciberespacio como un nuevo dominio o ámbito de las operaciones militares. Esta declaración supuso un giro conceptual: de una ciberseguridad reactiva y genérica (necesaria, pero insuficiente), hacia una ciberdefensa basada en la planificación y la inteligencia de ciberamenazas. (NATO, 2016)

---

[3] Los sistemas de ciberseguridad están diseñados y configurados con reglas de detección para detectar los modus operandi más habituales y comunes a la generalidad de las amenazas, pero no está especializada, ni prioriza la capacidad de detección/reacción frente a actores de la ciberamenazas específica a la que las FAS deben de hacer frente. La ciberseguridad comercial se basa en detectar indicadores técnicos de compromiso (IOC) o comportamientos anómalos, pero no ofrece una defensa táctica o estratégica ante adversarios con intenciones claras y persistentes contra intereses nacionales o de la Defensa y Seguridad Nacional.

[4] En función de la misión, de la coyuntura geopolítica, de la región o área de operaciones, etc.

[5] TIP son las siglas que se corresponden con: «Threat Intelligence Platform»

1.2 Diferencias clave entre ciberseguridad y ciberdefensa

La ciberdefensa no es solo una evolución de la ciberseguridad, sino un enfoque distinto que incorpora tres factores críticos:

1. La misión. ¿Qué funciones, capacidades, sistemas o servicio debemos proteger?
2. La amenaza específica. ¿Quién nos ataca o puede atacar?, ¿cómo y con qué intenciones?
3. Las debilidades del sistema. ¿Dónde somos vulnerables? ¿Dónde nos pueden atacar e impactarnos operativamente?

Desde esta óptica, el análisis de amenazas se convierte en un factor determinante. La ciberdefensa implica la planificación y conducción de una defensa predictiva y proactiva dirigida por inteligencia de ciberamenazas.

1.3 Analogía militar: ciberseguridad como defensa básica

Se puede comparar la «ciberseguridad tradicional» con los elementos básicos de «protección inmediata»[6] de una posición de infantería: alambradas, campos de minas, posiciones fijas. Son necesarios, sí, pero no suficientes para detener a un enemigo determinado, bien armado y con objetivos concretos. Estos mecanismos actúan como una protección inmediata, pero sin una visión táctica o estratégica.

La ciberdefensa, en cambio, se basa en inteligencia de ciberamenazas, planeamiento y adaptación, con el propósito de proteger el entorno del ciberespacio de interés militar en función de la misión militar, anticipando y neutralizando los movimientos del adversario.

2 La «Operacionalización» del ciberespacio

El concepto de «Operacionalización» del ciberespacio representa un cambio profundo en la forma de entender las operaciones en el ciberespacio. Hasta hace poco, las acciones en el ciberespacio se abordaban desde un enfoque puramente técnico. Sin embargo, este dominio ha comenzado a integrarse plenamente en el planeamiento y ejecución de las operaciones militares, aplicando principios tácticos y operacionales similares a los de otros ámbitos tradicionales de las operaciones militares (tierra, mar, aire, espacio). (Junta Interamericana de Defensa, 2023).

Este nuevo enfoque implica que las acciones defensivas en el ciberespacio ya no se basan únicamente en proteger sistemas de forma generalizada,

[6] Sin finalidad táctica, con la sola finalidad de dar cierta protección a los combatientes.

sino que ahora deben considerarse y analizarse en detalle tres factores clave:

— La amenaza concreta a enfrentar.
— La misión que se debe cumplir.
— Las vulnerabilidades del ciberespacio de interés militar a defender.

Gracias a esta evolución, comienzan a desarrollarse herramientas y tecnologías diseñadas específicamente con una mentalidad militar operativa, superando las limitaciones de los enfoques meramente técnicos. La atención ya no se centra en amenazas genéricas, sino en actores concretos, cuyas capacidades, motivaciones e intenciones se analizan a la luz de su contexto geopolítico, su área de influencia y sus objetivos estratégicos.

Esta transformación ha dado lugar a un tipo de inteligencia de ciberamenazas mucho más especializada, capaz de integrar en su análisis aspectos como:

— La región donde se desarrollan las operaciones.
— Las intenciones de los actores hostiles.
— Los intereses militares y políticos que motivan posibles ataques.

En consecuencia, la operacionalizacion del ciberespacio no solo cambia el enfoque, sino que también incorpora el análisis de la ciberamenaza como un componente esencial para diseñar y ejecutar una defensa eficaz. Esta inclusión convierte a la ciberdefensa en un ámbito de operaciones que ya no puede limitarse a prevenir o reaccionar ante incidentes, sino que debe anticiparse a ellos, basándose en una comprensión profunda del adversario, del entorno operativo y del ciberespacio militar sobre el que las operaciones descansan.

3 La ciberdefensa: un enfoque integral y dirigido por la Inteligencia de Ciberamenazas

Uno de los mayores desafíos en el ciberespacio es la clara ventaja con la que cuenta el atacante. Este puede decidir qué atacar, cuándo y cómo, utilizando técnicas, herramientas y *malware* a su antojo, y con el tiempo del mundo necesario para planificar y ejecutar su ofensiva. Por el contrario, el defensor debe proteger todo el sistema en su conjunto, sin saber con exactitud por dónde se producirá el ataque ni cuándo ni cómo.

3.1 Ventajas y desventajas del atacante y del defensor

El atacante solo necesita explotar una vulnerabilidad. El defensor, en cambio, debe asegurar todas. Esta asimetría define el carácter de la defensa del ciberespacio de interés militar: reactiva en su forma más básica, pero

con el potencial de ser proactiva y predictiva si se apoya en inteligencia especializada de ciberamenazas.

Aun así, el defensor dispone de ciertos recursos a su favor:

- Conocimiento del entorno a proteger (ciberterreno).
- Acceso a inteligencia de ciberamenazas, con un análisis histórico del comportamiento enemigo.
- Capacidad de modificar el ciberespacio de interés militar, aplicando configuraciones defensivas, reorganizaciones y contramedidas adaptadas.

3.2 Ciberdefensa: de la reacción a la anticipación

Frente a amenazas avanzadas como los APT[7] (Amenazas Persistentes Avanzadas), la ciberdefensa debe buscar anticipación, planificación, y actitud proactiva. Esto se logra mediante un enfoque que parta del análisis detallado de tres factores fundamentales:

3.2.1 La Amenaza

Implica identificar y comprender a los adversarios potenciales[8]:

— Sus capacidades y recursos.
— Sus motivaciones, intenciones y objetivos.
— Sus tácticas, técnicas y procedimientos (TTPs, *modus operandi*).
— Herramientas, *malware*, vulnerabilidades que explotan, etc.

Este conocimiento permite planificar operaciones defensivas dirigidas por inteligencia específica de ciberamenazas *(Intel-Driven Defensive Cyber Operations*).

3.2.2 La Misión

La defensa no puede ser genérica. Debe enfocarse en proteger los sistemas y servicios críticos para el éxito de la operación militar. Este enfoque se enmarca en el concepto de Mission Assurance. Para ello se analiza:

— ¿Qué partes del ciberespacio[9] son esenciales o críticas para la misión?

[7] APT son siglas que se corresponden con: «Advanced Persistent Threat». Es decir, actores de la amenaza con grandes recursos humanos, económicos, tecnológicos y procedimentales. Normalmente subvencionados y apoyados por Estados y con intereses geopolíticos, estratégico-políticos, y militares.

[8] Por lo general, APT compuestos por unidades militares de operaciones en el ciberespacio estatales o servicios secretos y grupos criminales (Proxies) apoyadas y subvencionadas por estados hostiles.

[9] Elementos o servicios críticos del ciberespacio que debemos, prioritariamente, defender para alcanzar el objetivo de Mission Assurance.

— ¿Qué sistemas, si son atacados, pueden, potencialmente, impactar más negativamente en la misión?
— ¿Cuál sería el impacto potencial si fueran atacados?
— ¿Qué servicios y activos son prioritarios entonces que defendamos?

El análisis de nuestro «Centro de Gravedad» operacional, de las capacidades críticas, de las dependencias de esas capacidades respecto a zonas del ciberespacio de interés militar, y de las vulnerabilidades que presentan estas zonas[10], ayuda a identificar los objetivos potenciales del adversario y las áreas prioritarias a defender.

3.2.3 El ciberespacio a defender[11]

Una vez definidos los activos y servicios clave[12], se debe analizar:

— Sus vulnerabilidades[13] técnicas y tácticas.
— Las posibles avenidas de aproximación del adversario[14]: rutas que podría utilizar para infiltrarse, avanzar y alcanzar sus objetivos.
— Las zonas vulnerables o menos protegidas del ciberespacio a defender.

Aquí, la inteligencia avanzada de la ciberamenaza es la clave para pasar de una defensa reactiva a una preventiva y planificada.

3.3 Aplicación de inteligencia táctica, operacional y estratégica

Para planificar y ejecutar la defensa, se requiere aplicar inteligencia de ciberamenazas en todos los niveles:

— Táctica: analiza vulnerabilidades defensivas, servicios críticos, posibles rutas de acceso del enemigo, intenciones y capacidades. Permite definir el plan defensivo de nivel táctico.
— Operacional: estudia las acciones y efectos que el adversario puede buscar para alcanzar sus objetivos más amplios (operacionales y estratégicos).

---

[10] Estas zonas del ciberespacio estarán formadas por servicios, sistemas, plataformas, etc.
[11] Esto incluye activos digitales, como bases de datos, aplicaciones críticas y sistemas operativos, así como infraestructura clave e información y datos críticos para la misión.
[12] Zonas prioritarias del ciberespacio a defender por interés militar.
[13] Tales como configuraciones inseguras, software desactualizado, interconexiones y puntos de vulnerabilidades del ciberespacio a defender que puedan ser explotados por el adversario en su ataque.
[14] Haciendo un símil al ámbito terrestre, se trataría Identificar los potenciales valles y vaguadas en el ciberespacio que podrían ser potencialmente empleado por el adversario como avenidas de aproximación, avance o ataque a sus objetivos. Estos valles o vaguadas en el ciberespacio estarían formados por las rutas formadas por los dispositivos y servicios más vulnerables y configurados de manera más insegura.

Estratégica: identifica actores clave[15] de la ciberamenaza, sus relaciones, capacidades estructurales, recursos tecnológicos y de formación y vínculos con gobiernos hostiles. Permitirá un planeamiento defensivo de nivel estratégico enfocado a atacar[16] las raíces de las capacidades ofensivas del adversario en el ciberespacio.

3.4 El modelo IPB aplicado al ciberespacio (Cyber-IPB)

Este enfoque, tomado del ámbito terrestre, se adapta a la ciberdefensa aplicando elementos y conceptos tácticos terrestres al ciberespacio.

El Cy-IPB es el resultado de un análisis cruzado (correlación) de los datos y la información disponible sobre: la misión, la amenaza y el ciberespacio, proporcionada a los cibercombatientes de forma estructurada y fácilmente visible y comprensible, de manera que apoye el asesoramiento y la toma de decisiones en las operaciones en el ciberespacio. (Winterfeld, 2002).

Este enfoque incluye la realización de un análisis detallado del entorno, similar al proceso de Planeamiento basado en Inteligencia (*Intelligence Preparation of the Battlefield*, IPB) (U.S. Department of the Army, 2009). Algunos de los conceptos claves traducidos al ámbito de las operaciones en el ciberespacio son:

- Bases de Partida: serán puntos de entrada del atacante (tales como, correos electrónicos, puertos USB, interconexiones entre sistemas y servicios, etc.).
- Objetivos: serán servicios o activos críticos que el adversario puede tener intención de atacar o alcanzar (tales como, servidores de bases de datos, Servidores de aplicaciones críticas, servidores de servicios CORE, servicios COI[17] y servicios básicos, etc.).
- Avenidas de Aproximación[18]: serán las rutas más vulnerables dentro del ciberespacio a defender[19] que puede ser empleados por un atacante en su avance hacia sus objetivos.

[15] En función de la coyuntura geopolítica, de la misiones y operaciones, etc.
[16] Atacar sus recursos humanos, tecnológicos, formativos, económicos, etc.
[17] COI son las siglas que se corresponde con: «Community of Interest». Son servicios funcionales como INTEL-FS, JTS, etc. (anteriormente se denominaban Servicios FAS o Funtional Area Services).
[18] El número de «Avenidas de Aproximación» potenciales puede ser numerosos, por lo que es necesario realizar un análisis y descartar aquellas cuyas vulnerabilidades no sean, teóricamente, explotables por las TTP de los actores de la ciberamenaza definido para cada caso. Además, estas rutas deberán priorizarse desde un punto de vista de planeamiento de la defensa y bloqueo de dichas rutas.
[19] Se entiende por «Ciberespacio a defender», al conjunto de sistemas IT y OT que soportan las capacidades militares y por tanto las operaciones militares.

— Zonas Ocultas o Semi-Ocultas: serán zonas del ciberespacio a defender donde los adversarios pueden operar sin ser detectados por los sistemas tradicionales de ciberseguridad. Pueden ser:

  - Zonas Ocultas: serán zonas del ciberespacio a defender no monitorizada por mecanismos de ciberseguridad de detección.
  - Zonas Semi-Ocultas: serán zonas del ciberespacio a defender que, aunque monitorizados por mecanismos de detección, estos dispositivos no disponen de las reglas de detección o la configuración adecuada para detectar las TTP[20] empleadas por los actores de la ciberamenazas específicos a la que nos enfrentamos.

— Zonas a Cubierto: serán zonas del ciberespacio a defender sin mecanismos de ciberdefensa y ciberseguridad implementados que nos permitan reaccionar directamente sobre el atacante o modificar la configuración[21] del ciberespacio.

— Terreno Clave Ciber (CKT[22]): serán puntos del ciberespacio a defender (normalmente donde convergen rutas críticas y vulnerables, como interconexiones de sistemas, servidores esenciales, satélites o cables submarinos), cuyo control, defensa y monitorización proporciona una ventaja defensiva.

  El Terreno Clave (CKT) son aquellas zonas del ciberespacio que, si son defendidos de forma adecuada, dificultarán enormemente el progreso o avance del adversario por nuestro ciberespacio y el éxito de los ataques del adversario sobre sus objetivos en el ciberespacio. (Multinational Capability Development Campaign, 2017).

Este análisis ayuda a planificar una defensa proactiva y dinámica, anticipando los movimientos del adversario y cerrando brechas antes de que puedan ser explotadas.

3.4.1 Cyber-IPB: objetivos y beneficios

El Cyber-IPB permite:

— Identificar quién podría atacarnos, qué podría atacar, por qué y cómo.

[20] TTP son las siglas que se corresponden con: «Tactics, Techniques, and Procedures». (Tácticas, Técnicas y Procedimientos).
[21] Por ejemplo, modificando la configuración de seguridad de los dispositivos o las reglas de acceso, etc.
[22] CKT son las siglas que se corresponden con: «Cyber Key Terrain». Terreno Clave en el Ciberespacio. Equivalente al concepto de «Terreno Clave» en el ámbito terrestre pero trasladado al ámbito del ciberespacio.

— Detectar rutas de ataque y zonas críticas explotables por el adversario:
  - Rutas vulnerables dentro del ciberespacio.
  - Vulnerabilidades explotables en el ciberespacio.
  - Configuraciones inseguras explotables.
— Evaluar impactos potenciales y riesgos (técnicos, tácticos y operacionales).
— Diseñar planes defensivos, de prevención, contención, reacción y recuperación más eficaces y eficientes.

Todo esto con el fin de:

— Anticiparse al adversario.
— Asignar mejor los escasos recursos existentes:
  - Priorizar recursos
  - Priorizar actividades defensivas
  - Priorizar zonas del ciberespacio donde ejercer los esfuerzos principales en el ciberespacio.
— Reducir el impacto operativo de un posible ciberataque.

3.5 Planes de ciberdefensa (Corletti Estrada, 2017)

Con base en este análisis Cyber-IPB, se elaborará un Plan de Ciberdefensa específico, cuyo objetivo es:

— Reducir los riesgos en el ciberespacio.
— Reducir los potenciales impactos.
— Responder a los ciberataques.
— Garantizar la continuidad operativa.
— Asegurar el cumplimiento de la misión.

Se diseñarán y ejecutarán planes de ciberdefensa en todos y cada uno de los niveles de la guerra: técnico, táctico, operacional y estratégico. Cada uno de los planes de estos niveles hará frente a la ciberdefensa desde perspectivas diferentes:

— Nivel Técnico: gestión técnica de los riesgos y de los potenciales impactos.
— Nivel Táctico: dirección de la ciberdefensa de forma táctica, como una defensa del ciberespacio como un todo.

— Nivel Operacional: apoyo a la gestión de los riesgo e impactos de ciberataques en las operaciones militares.

— Nivel Estratégico: gestión estratégica de recursos de ciberdefensa (humano, formativos y tecnológicos), ataque estratégico a las fuentes de las capacidades ofensivas del adversario

Este plan incluye los siguientes componentes:

3.5.1 Plan de Detección Avanzada

Tiene como propósito establecer mecanismos que permitan identificar comportamientos maliciosos en redes y sistemas, usando inteligencia sobre ciberamenazas.

Se centra en:

— Desplegar sensores de seguridad en áreas clave del ciberespacio (Cy-NAIs[23]), en especial, en puntos estratégicos[24] por donde podría avanzar un adversario.

— Configurar estos sensores con reglas que permitan detectar tácticas, técnicas, herramientas y *malware* habitualmente usados por los actores de amenazas definidos, según inteligencia de ciberamenazas táctica y técnica.

3.5.2 Plan de Obstáculos

Busca dificultar el avance del adversario dentro del sistema a través de:

— Mecanismos de seguridad que monitorean, filtran y restringen el tráfico de datos en puntos clave del ciberespacio, impidiendo el libre movimiento del adversario.

— Planes predefinidos para desactivar servicios[25] vulnerables que podrían ser aprovechados como vía de acceso, penetración y progresión de un ciberataque.

Este plan se basa en un análisis detallado de las posibles rutas de ataque (Avenidas de Aproximación), considerando las debilidades (vulnerabilidades) del sistema y las capacidades (TTPs y tecnología) del enemigo.

---

[23] CyNAI son las siglas que se corresponden con: «Cyber Name Areas of Interest».
[24] Generalmente, puntos de confluencia de varias avenidas de aproximación del adversario.
[25] Sería el equivalente a la realización de destrucción de puentes en un avance adversario en al ámbito terrestre, para retrasarlos o canalizarlos.

3.5.3 Plan de Mitigación de Efectos

Diseñado para minimizar los daños (efectos/impactos) en caso de un ciberataque exitoso por parte del adversario:

— A nivel táctico, se establecerán sistemas redundantes y configuraciones de alta disponibilidad que mantengan los servicios activos pese a las agresiones.

— A nivel operacional, se implementarán planes de contingencia con recursos alternativos, tanto militares como civiles, que aseguren la continuidad de las operaciones, incluso fuera del ámbito digital[26].

3.5.4 Plan de Reacción

Contempla respuestas específicas frente a distintos tipos de ciberataques anticipados (Cy-OCOAs[27]), incluyendo:

— Planes de despliegue de Unidades de Reacción Rápida (RRT[28]).

— Planes detallados de gestión de incidentes a nivel técnico y táctico.

3.5.5 Plan de Recuperación

Asegura la restauración rápida de servicios y sistemas críticos mediante:

— En el ámbito IT y OT, el uso de tecnologías como la virtualización o hiperconvergencia[29], que permiten reconstruir servicios en minutos.

— En cuanto a datos, sistemas de recuperación de datos (DRP[30]) con tiempos (RTO[31]) y puntos de recuperación (RPO[32]) definidos según la criticidad[33] del servicio para la operación militar.

---

[26] Por ejemplo, tener previsto transporte de combustible mediante trenes de cisternas de combustible, en caso de que un determinado oleoducto sea atacado.

[27] Cy-OCOA son las siglas que se corresponden con: «Cyber Opposite Course of Action». Líneas de acción potenciales de las operaciones en el Ciberespacio del adversario.

[28] RRT son las siglas que se corresponden con: «Rapid Reaction Team». Equipo de Reacción Rápida ante incidentes de Ciberseguridad o Ciberataque.

[29] Se trata de sistemas avanzado que, en vez de tener servidores, almacenamiento (como SAN o NAS) y redes separados; la infraestructura hiperconvergente (HCI) combina todo eso en nodos modulares (como cajas que tienen de todo un poco), lo que facilita la escalabilidad y el manejo del entorno.

[30] DRP son las siglas que se corresponden con: «Data Recovery Plans».

[31] RTO son las siglas que se corresponden con: «Recovery Time Objective», es decir, el tiempo máximo en el que se debe poder recuperar los datos y que el servicio o sistema pueda acceder a los datos.

[32] RPO son las siglas que se corresponden con: «Recovery Point Objective», es decir, el tiempo máximo de datos que se puede perder, que corresponde al tiempo que transcurre entre que se realizan dos *backups* de datos consecutivos.

[33] Impacto potencial en las operaciones en caso de ataque al mismo.

4 Desafíos Tecnológicos en Ciberdefensa

El panorama actual del ciberespacio está marcado por una evolución acelerada de las amenazas. Ataques como los *zero-day*[34], el *malware* polimórfico[35] o el ransomware dirigido, avanzan a una velocidad que supera la capacidad de respuesta de las herramientas de ciberseguridad tradicionales. (Internet Security Auditors, 2025).

Los mecanismos convencionales, basados en firmas o indicadores técnicos de compromiso (IOC), han quedado obsoletos frente a adversarios altamente cualificados, sofisticados y, en muchos casos, respaldados por estados hostiles.

4.1 Necesidad de soluciones nacionales y estratégicas

Ante este contexto, se vuelve esencial contar con sistemas de ciberdefensa diseñados específicamente para este entorno de alta exigencia y estén adaptadas a las necesidades específicas de nuestras Fuerzas Armadas.

Además, por su carácter estratégico[36], es fundamental que estas soluciones:

— Sean desarrolladas a nivel nacional, garantizando la independencia tecnológica.

— No dependan de tecnologías o empresas extranjeras que puedan comprometer la seguridad o deshabilitar las capacidades defensivas remotamente (*Kill-Switch*[37]).

---

[34] Un «zero day» (o «día cero») es una vulnerabilidad de seguridad en software que es descubierta por atacantes antes de que el desarrollador del software sepa que existe. Como el fabricante no ha tenido tiempo de corregirla (porque no sabía de ella), no hay parches ni defensas oficiales disponibles, lo que la hace especialmente peligrosa. Su nombre proviene del hecho que el proveedor del ***software*** tiene «cero días» para arreglarla desde que se descubre públicamente o se empieza a explotarse por potenciales adversarios u actores maliciosos.

[35] Capaz de cambiar su forma para evadir la detección.

[36] La ciberdefensa es un ámbito tan transversal a todas las capacidades militares, lo cual le proporciona un carácter estratégico y requiere, por tanto, de una independencia estratégica, no se puede depender de tecnología no nacional. La ciberdefensa de nuestras capacidades militares no puede depender de una industria bajo control de un tercer país, que pueda desactivar estas capacidades de ciberdefensa a su antojo, o que pueda acceder a información sobre las debilidades de nuestro ciberespacio.

[37] Un *Kill-switch* (o interruptor de apagado de emergencia) es un mecanismo diseñado para detener de manera automática un sistema, proceso o dispositivo en caso de emergencia o cuando se detecta una amenaza. Un *Kill-switch* puede apagar remotamente una ***app*** o dispositivo si es robado o comprometido o a voluntad. Por ejemplo, algunos ***smartphones*** permiten borrar todos los datos si se pierden.

La industria nacional de ciberdefensa se convierte así en un pilar clave para garantizar una defensa autónoma y eficaz del ciberespacio militar. Sin una base tecnológica soberana, la ciberdefensa se convierte en un castillo con cimientos prestados: estable, mientras el proveedor de las herramientas de ciberdefensa lo permita. Fortalecer la industria nacional no es una opción, es una necesidad estratégica. (Arteaga y Alonso, 2023)

4.2 Necesidad de desarrollos y adquisiciones ágiles

El ciberespacio es un entorno dinámico, donde atacantes y defensores compiten en una carrera tecnológica continua. Por ello, las herramientas de ciberdefensa deben:

— Mantenerse a la par o por delante del ritmo tecnológico de los atacantes.

— Superar los tiempos lentos de adquisición y desarrollo típicos en entornos tradicionales.

— Tener ciclos de evolución y despliegue muy rápidos[38].

4.3 Lagunas Tecnológicas

A pesar de los avances, siguen existiendo lagunas tecnológicas importantes, especialmente en tres áreas críticas:

1. Inteligencia de ciberamenazas.
2. Conciencia situacional.
3. Mando y Control de operaciones defensivas.

4.3.1 Conciencia Situacional (CySA[39])

Uno de los principales retos es contar con una visión clara, completa, precisa y en tiempo real de lo que acontece en el ciberespacio. Sin esta Conciencia Situacional, resulta difícil:

— Gestionar riesgos en el ciberespacio.

— Priorizar activos a defender y acciones a ejecutar.

— Entender el contexto de un ciberataque.

— Evaluar su impacto potencial y efectos operativos.

— Tomar decisiones informadas bajo presión.

[38] Es decir, ciclos de vida de las herramientas y software específico de ciberdefensa muy ágil.
[39] CySA son las siglas que se corresponde con: «Cyber Situational Awareness».

Esto implica monitorizar enormes volúmenes de datos en tiempo real, provenientes de múltiples fuentes, y transformarlos en información útil. Para lograrlo, se necesita:

— Integración de datos desde diversos sistemas y fuentes.

— Un repositorio único, flexible y escalable (*datalake*).

— Herramientas avanzadas de procesado y análisis en tiempo casi real.

— Interfaces que presenten la información de forma personalizable[40] a las necesidades de cada combatiente en el ciberespacio en cada rol y nivel de mando.

4.3.2 Modelado de la ciberamenaza

Frente a amenazas genéricas, el entorno actual requiere una inteligencia especializada y orientada a actores concretos. El modelado de amenazas se ha convertido en un elemento central en los sistemas modernos de Inteligencia de ciberamenazas y esencial para una táctica y estrategia avanzada de ciberdefensa.

El modelado de la ciberamenaza consiste en:

— Recopilar, almacenar, analizar y representar toda la información disponible sobre cada actor de la amenaza.

— Construir perfiles estructurados (atributos y parámetros) que incluyan: tácticas, herramientas, objetivos frecuentes, infraestructura, relaciones geopolíticas, capacidades técnicas, etc.

— Establecer una especie de «ficha policial digital» de cada actor, con sus huellas, modus operandi (TTP), relaciones, patrones y comportamientos.

— Buscar relaciones y patrones entre los datos de la ciberamenaza.

— Representar gráficamente el modelado de la amenaza de forma entendible por los analistas de Inteligencia de ciberamenazas.

El modelado de la ciberamenaza se aplica a:

— Planeamiento: predicción y anticipación a los comportamientos de los actores de la ciberamenazas para reducir riesgos y definir planes de contingencia.

— Conducción de operaciones (Gestión de Incidentes):

[40] Mediante filtrado y selección del formato de representación más adecuado en cada momento y para cada finalidad.

- Compara[41] características[42] (modelado) del incidente con las del actor.
- Establece atribuciones probables.
- Dirige la investigación.
- Propone tácticas y contramedidas adaptadas.

El modelado de la amenaza permitirá:

— Realizar atribuciones técnicas y tácticas sobre la posible autoría de los incidentes, asignando probabilidades basadas en la coincidencia entre los patrones del incidente y los comportamientos conocidos de distintos actores de ciberamenazas.

— Orientar la investigación del incidente utilizando inteligencia de ciberamenazas, definiendo líneas de investigación en función de los modos de operación (*modus operandi*) de las posibles atribuciones (autores potenciales) identificados en el paso anterior.

— Anticipar los próximos movimientos del atacante, basándose en su perfil y comportamiento histórico.

— Definir las tácticas y técnicas más adecuadas para responder al incidente, incluyendo acciones de detección, contención, mitigación, reacción y recuperación, con el objetivo de recuperar el control del sistema y expulsar al adversario.

La dificultad técnica radica en desarrollar sistemas capaces de combinar grandes volúmenes de datos con técnicas de inteligencia artificial (IA) (como el *Machine Learning* (ML) o *Deep Learning* (DL), para identificar patrones y relaciones útiles que permiten guiar la ciberdefensa (*Intel Driven Defensive Cyber Operations*).

En el ámbito de las operaciones en el ciberespacio[43], una forma tecnológicamente avanzada es representar a los atacantes a través del modelado vectorial. Esta técnica utiliza bases de datos vectoriales en las que cada actor de amenaza se representa como un punto en un espacio multidimensional[44]. Cada una de esas dimensiones corresponde a una característica o

[41] Esta comparación se realiza de forma matemática (automatizada), mediante comparación vectorial de los vectores (en una base de datos vectorial) que representan cada uno de los incidentes y de los actores, en las que, por ejemplo, cada actor es representado por un vector multidimensional y en el que cada dimensión de ese espacio vectorial es un parámetro o atributo de estos.

[42] Haciendo un símil, es como comparar la ficha de investigación policial (modelado) de un incidente o robo (con sus evidencias e indicios) con fichas policiales (modelado) de los delincuentes.

[43] Especialmente, en cuanto a gestión de incidentes y análisis de inteligencia.

[44] Con múltiples dimensiones, cada una de ellas representando un parámetro o característica del objeto a modelar.

comportamiento del atacante y el conjunto de estos datos forma un vector que lo describe.

Este enfoque no solo sirve para modelar actores maliciosos, sino que también se puede aplicar a otros elementos del ciberespacio, como incidentes de seguridad o ciberataques.

Si representamos un ciberataque como un vector en ese mismo espacio multidimensional, puede compararse con los vectores de los distintos actores de amenaza.

Una comparación entre el vector del ataque y el del posible autor (actor de amenaza) permite obtener un «vector diferencia». Este «vector diferencia» revela qué características del atacante aún no se han manifestado en el potencial ciberataque en curso, lo que ofrece dos ventajas clave:

— Guía de investigación: orienta sobre las evidencias, comportamientos o detalles que deberían buscarse en el análisis del ciberataque.

— Predicción de acciones futuras: ayuda a anticipar los siguientes movimientos del atacante, basándonos en lo que normalmente haría, pero aún no ha hecho.

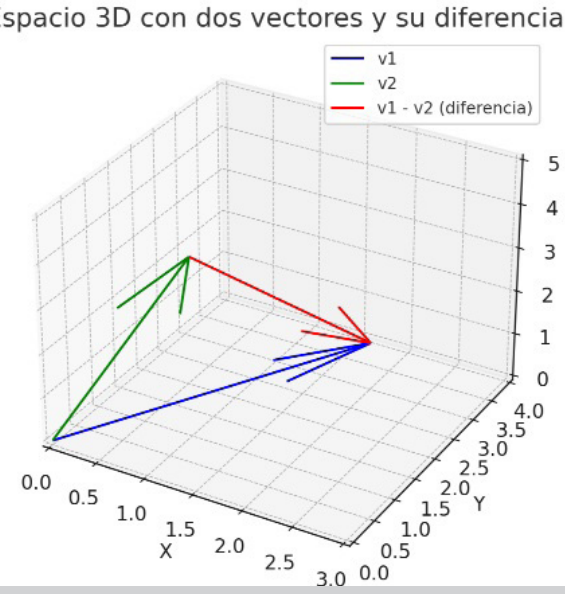


Figura 1. Modelado en tres dimensiones. Representación de vectorial de dos objetos modelados vectorialmente en un cubo tridimensional (de solo tres parámetros) y la representación del vector diferencia de la comparación de los dos modelos. Las proyecciones de ese vector diferencia en los ejes de dicho cubo, nos mostrará los parámetros en los que ambos modelos no concuerda, y el valor de esa diferencia. En un modelado real, el cubo no sería tridimensional, sino n-dimensional. [Imagen obtenida de Chagpt]

Además, al comparar el vector de un ataque con los vectores de múltiples actores conocidos, se puede realizar un análisis probabilístico de atribución. Cuanto más cercano sea un vector a otro (menor distancia entre ellos), mayor será la probabilidad de que el actor correspondiente sea el responsable del ataque.

Este tipo de técnicas ofrece un enorme potencial no solo en ciberdefensa, sino también en otras áreas donde es necesario analizar y anticipar comportamientos complejos.

5 Iniciativas tecnológicas impulsadas por el MCCE

El incremento constante de amenazas en el ciberespacio ha obligado a desarrollar soluciones tecnológicas específicas para la ciberdefensa militar. Sin embargo, la oferta comercial en este ámbito aún es escasa, debido a la naturaleza reciente del enfoque militar en este dominio.

Por ello, el Mando Conjunto del Ciberespacio (MCCE) ha promovido una serie de proyectos que buscan cubrir estas carencias tecnológicas mediante herramientas tecnología y conceptualmente avanzadas, diseñadas para:

- Integrar Inteligencia de Ciberamenazas.
- Proporcionar capacidades de Mando y Control.
- Mejorar la Conciencia Situacional.
- Asegurar la Respuesta Defensiva operativa.

A continuación, se presentan las principales iniciativas.

5.1 Plataforma PICO

La plataforma PICO (Plataforma de Inteligencia para la Conducción de Operaciones en el Ciberespacio) ha representado uno de los primeros pasos de adquisición y evolución de capacidades específicas de ciberdefensa militar dentro del MCCE.

Se basa en el desarrollo previo del producto CIAT[45] de la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica) y ha sido adaptada para fines militares por dicha compañía para cumplir con los requisitos operativos definidos y requeridos por el MCCE.

5.1.1 ¿Qué ofrece PICO?

PICO combina dos capacidades en una única solución:

- Gestión de inteligencia de ciberamenazas.
- Gestión de incidentes de ciberseguridad.

[45] CIAT son las siglas que se corresponde con: «Plataforma Global de Ciber Inteligencia Avanzada de Telefónica».

Esta integración permite:

— Modelar incidentes y actores de amenazas.
— Correlacionar evidencias entre ambos modelos (incidentes y amenazas).
— Gestionar ciberataques dirigidos por inteligencia de ciberamenazas.
— Priorización, automatización y control de tareas de respuesta a ciberataques o incidentes de seguridad.

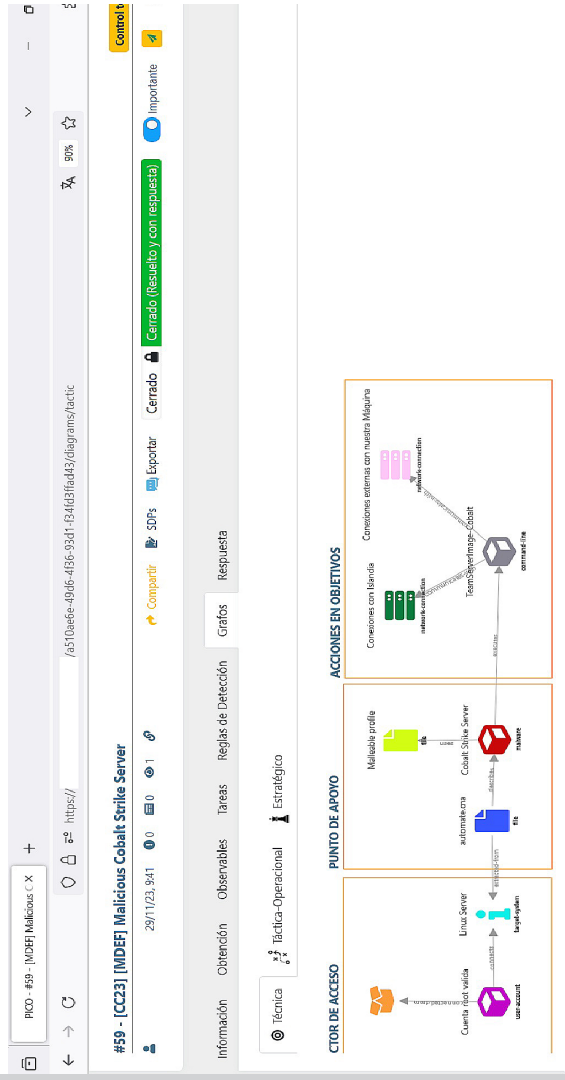


Figura 2. Modelado Técnico de un Ciberataque. Esta imagen muestra un caso de modelado de un Ciberataque realizado mediante la Plataforma PICO. En el que se representa los pasos, evidencias y artefactos empleados por un atacante en la ejecución de su ataque. [Imagen cedida por la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica)]

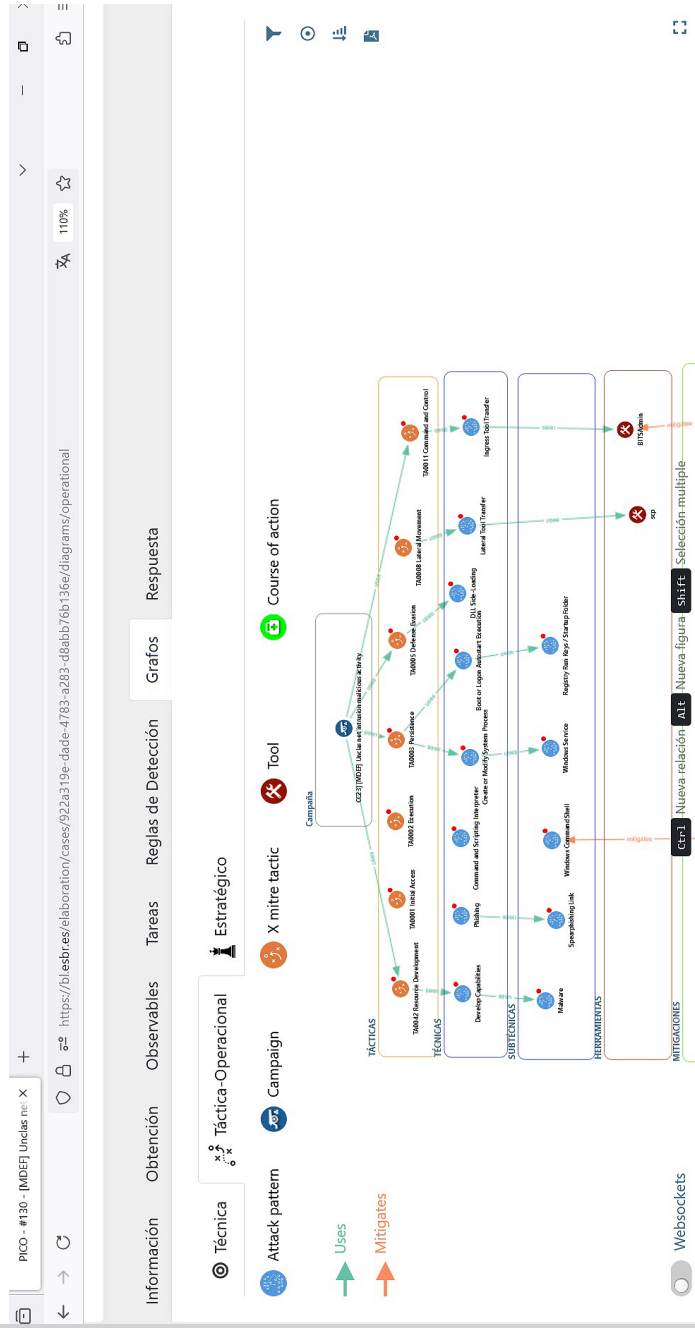


Figura 3. Modelado Táctico de un Ciberataque. Esta imagen muestra un caso de modelado Táctico de un ciberataque, realizado mediante la Plataforma PICO. En el que se representa las tácticas, técnicas, procedimientos, herramientas malware empleados, así como las COAs defensivas empleadas por el Ciberdefensor. [Imagen cedida por la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica)]

Además, PICO emplea el *framework* de las matrices de MITRE ATT&CK[46] para modelar (mapear) las tácticas, técnicas y procedimientos empleadas por los atacantes, lo que permite realizar atribuciones más precisas y planes de defensa proactivas.

La plataforma PICO está diseñada para facilitar una gestión integral, coordinada y eficiente de las operaciones defensivas y de inteligencia, a nivel técnico (e incipientemente a nivel táctico), en el ámbito del ciberespacio. Estas son sus principales capacidades:

— Unificación de herramientas: permite operar desde una única plataforma, eliminando, en gran medida, la necesidad de usar múltiples sistemas a la vez. Esto ofrece un cuadro de mando centralizado que simplifica la gestión y mejora la eficiencia.

— Gestión centralizada de la información de inteligencia de ciberamenazas: reúne todos los datos disponibles tanto del entorno propio como de posibles amenazas en un repositorio único[47], lo que facilita la correlación de información y mejora la conciencia situacional para apoyar una toma de decisiones más efectiva.

— Automatización: optimiza tareas repetitivas relacionadas con la gestión de incidentes y el análisis de inteligencia y permite a los operadores centrarse en labores de mayor valor estratégico. Permite también definir *workflows* de tareas, con asignación y control de tareas.

— Vigilancia y monitorización integrales: integra diversas herramientas de detección en una sola plataforma, lo que permite una vigilancia continua del ciberespacio, así como una visualización técnica/táctica unificada. Todas las alertas se muestran en una única interfaz, priorizadas según el nivel de amenaza identificado por la inteligencia de ciberamenazas y la misión.

— Sincronización entre inteligencia y operaciones: asegura que la gestión de incidentes esté guiada por inteligencia (Intel Driven), lo que permite responder de forma más eficaz ante ciberataques y anticipar posibles movimientos del adversario.

— Correlación de datos: la plataforma analiza de forma automatizada grandes volúmenes de información para detectar patrones y

[46] Para hacer un símil, las matrices de Mitre Att&ck son a Ciberdefensa lo que la tabla periódica de elementos es a la química. Es decir, las matrices de Mitre Att&ck es una especie de tabla periódica ordenada de todas las tácticas, técnicas y procedimientos existentes o al menos identificadas.

[47] Se trata de una base de datos relacional. No incorpora aún un ***datalake*** y, por tanto, no presenta las ventajas de este tipo de tecnologías.

relaciones entre incidentes, lo que ayuda a identificar conexiones entre ataques en apariencia aislados.

— Gestión y respuesta efectiva a incidentes: permite registrar, clasificar y priorizar incidentes según su impacto potencial, asignar recursos de manera eficiente, y coordinar respuestas con rapidez, al estilo de los sistemas SOAR[48].

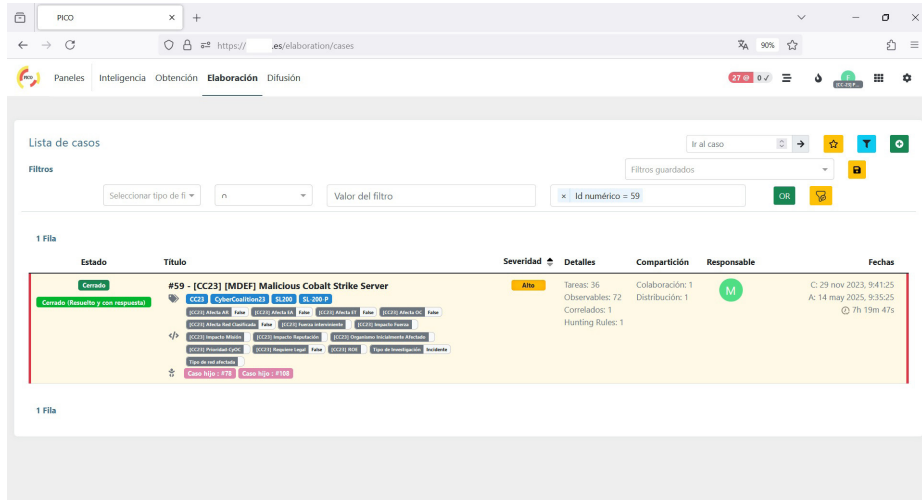


Figura 4. Visualización de la Vista de Gestión de Incidentes de la Plataforma PICO. [Imagen cedida por la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica)]

— Apoyo a la toma de decisiones: genera información procesada y relevante para que los equipos de ciberdefensa puedan actuar con rapidez y precisión, incluso bajo presión.

— Reducción de riesgos: contribuye a mitigar los efectos de los incidentes y a prevenir futuras amenazas, de modo que asignan y coordinan las tareas defensivas de forma estructurada y eficaz.

Al tomar como punto de partida esta versión de PICO inicial, desde el MCCE se planea apoyar de forma activa la evolución de este producto hasta convertirse en un módulo táctico/técnico del Sistema de Inteligencia y del Sistema de Mando y Control dentro del futuro SCOMCE[49].

[48] SOAR son las siglas que se corresponde a «Security Orchestration, Automación and Response». Se trata de un dispositivo de gestión de incidentes de seguridad con capacidad de respuesta automatizada y de *workflow*.
[49] SCOMCE son las siglas que se corresponden con: «Sistema de Combate en el Ciberespacio».

5.2 ECYSAP / ECYSAP EYE

El proyecto ECYSAP (European Cyber Situational Awareness Platform) nace de una iniciativa europea impulsada y subvencionada por la UE, con el objetivo de desarrollar una plataforma de Conciencia Situacional (en su versión v 1.0) y de Mando y Control de operaciones de ciberdefensa (en su versión v 2.0).

5.2.1 ECYSAP[50] v1.0

Figura 5. Visualización del logo del proyecto ECYSAP. [Imagen cedida por la empresa INDRA]

Se trata de una herramienta centrada en proporcionar Cyber Situational Awareness (CySA).

- Desarrollado con apoyos de fondos europeos.
- Coordinado por INDRA, con participación de España, Italia, Francia y Estonia.
- El MCCE (Mando Conjunto del Ciberespacio) ha apoyado este proyecto desde el punto de vista técnico y operativo, por delegación de la DGAM, desde sus inicios.
- La OTAN ha mostrado su interés en esta herramienta y a nivel de la UE se ha presentado en la reunión Anual de Cybercommanders de la UE de este año. Las FAS españolas cuentan con disponer de una versión de ECySAP adaptada a las necesidades de nuestras FAS como producto operativo y funcionando antes de final de año (2025) en las instalaciones del MCCE.

ECySAP dispone de cuatro niveles de visualización, correspondientes a los niveles de la guerra: técnico, táctico, operacional y estratégico.

Cada nivel de la guerra, a su vez integra cuatro vistas especializadas:

- Vista Misión: enfocada a satisfacer las necesidades del personal del área de operaciones y planes.
- Vista Amenaza: enfocada a satisfacer las necesidades del personal del área de inteligencia.
- Vista Ciberespacio enfocada a satisfacer las necesidades del personal del área CIS/CYBER.

[50] ECySAP son las siglas que se corresponden con: «European Cyber Situational Awareness Project».

— Vista CYBER: enfocada a satisfacer las necesidades del comandante CYBER o comandante de las operaciones.

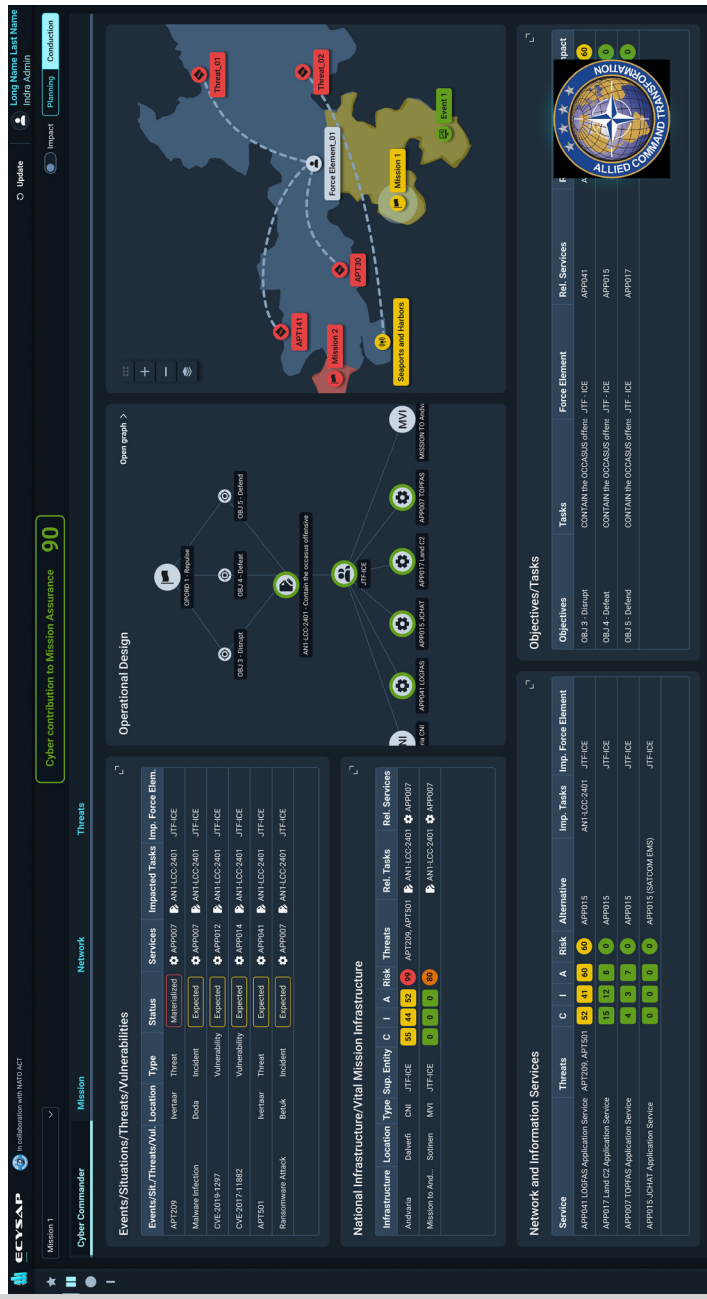


Figura 6. Visualización de la Plataforma ECYSAP.(Vista de nivel Operacional) para el Oficial de Enlace o Jefe del Grupo de trabajo Ciberoperaciones (CyOWG) en un nivel de Mando Conjunto. [Imagen cedida por la empresa INDRA y NATO ACT CYBER]

Figura 7. Visualización de la Plataforma ECYSAP (Vista de nivel Táctico) para el Oficial de Inteligencia de Ciberamenazas dentro del Estado Mayor de un Mando de Operaciones en el Ciberespacio. En el que puede visualizar y editar las TTPs de un Actor de la Ciberamenaza concreto. [Imagen cedida por la empresa INDRA y NATO ACT CYBER]

5.2.2 ECYSAP v2.0 (ECYSAP EYE)

Versión evolutiva del sistema ECYSAP v 1.0, cuyo objetivo es convertirse en un Sistema Integral de Mando y Control de operaciones en el ciberespacio, incorporando:

— Conciencia Situacional (CySA).
— Planificación y Conducción de operaciones y misiones en el ciberespacio (Guiadas por inteligencia de ciberamenazas).
— *Wargaming* y simulación[51].
— Flujo de trabajo colaborativo.
— *Targeting*.

Este proyecto, también es subvencionado por la UE y será desarrollado por un consorcio de ocho países europeos[52], liderado de nuevo por INDRA y está previsto su finalización para 2028, en nivel de madurez tecnológica TRL 6-7[53].

El MCCE (Mando Conjunto del Ciberespacio) también apoyará este proyecto desde el punto de vista técnico y operativo, por delegación de la DGAM.

5.3 SCOMCE: sistema de Combate en el Ciberespacio

Como parte de su esfuerzo por reforzar su capacidad de combate en el ciberespacio, el MCCE está desarrollando el Sistema de Combate en el Ciberespacio (SCOMCE).

El sistema SCOMCE es el proyecto[54] más ambicioso del MCCE. Se plantea como un «Sistema de Sistemas» que integre capacidades completas para operar y combatir en el ciberespacio, con la inclusión los siguientes sistemas:

— Sistema de Mando y Control:
  • Proporciona la capacidad de dirección y supervisión de las operaciones en el ciberespacio en tiempo real.

[51] Con base en «Modelados» de los diferentes actores de la ciberamenaza. Estos modelados se emplearán para las simulaciones de los ataques de los actores de la ciberamenaza en módulos de ***wargaming*** de nivel técnico (simulaciones LIVE) y nivel táctico (simulaciones de carácter TTX).
[52] Francia, Austria, Italia, Estonia, Polonia, Rumania, Grecia y España.
[53] TRL siglas que se corresponden con: «Tecnology Readiness Levels» (Nivel de madurez tecnológica). TRL 6 – Tecnología demostrada en un entorno relevante (entorno relevante a nivel industrial en el caso de tecnologías habilitadoras clave). TRL 7 – Demostración del prototipo del sistema en un entorno operativo.
[54] En realidad, se tratará de un programa compuesto por casi una veintena de proyectos.

— Sistema de Inteligencia:

  - Proporciona la capacidad de inteligencia de ciberamenazas en todos los niveles de la guerra (técnico, táctico, operacional y estratégico).

— Sistema Ofensivo:

  - Proporciona la capacidad de ejecutar operaciones activas en el ciberespacio adversario y permite acciones de disuasión, neutralización, etc.

— Sistema Defensivo:

  - Proporciona las capacidades de ciberdefensa del ciberespacio propio mediante medidas avanzadas de detección, contención, mitigación y recuperación ante ciberataques.

— Sistema Transversal:

  - Proporciona capacidades transversales a todos los sistemas anteriores: servicios compartidos y soporte a los demás sistemas.

La inclusión de un Sistema de Inteligencia propio dentro del SCOMCE demuestra la importancia creciente de la inteligencia de ciberamenazas como eje central de toda operación defensiva u ofensiva en el ciberespacio, al igual que ocurre en otros ámbitos de operaciones militares.

Este sistema está siendo diseñado para dar servicio en todos los niveles de mando y niveles de la guerra, desde el nivel técnico hasta el estratégico.

6 Requisitos tecnológicos avanzados para el SCOMCE

El Sistema de Combate en el Ciberespacio requiere integrar las tecnologías más avanzadas disponibles para cumplir con los desafíos operativos y estratégicos del dominio o ambiente de operaciones en el ciberespacio.

Se requiere que sea capaz de:

— Centralizar toda la información relevante del ciberespacio.

— Correlar, relacionar y analizar toda la información y datos disponibles de forma estructurada y predictiva.

— Apoyar la toma de decisiones en tiempo real.

Existe cuatro tecnologías que son, sobre todo, críticas para alcanzar las capacidades que requiere el Sistema de Inteligencia del SCOMCE.

6.1 Tecnología de datalake

Los *datalakes* representan una evolución tecnológica respecto a las bases de datos tradicionales, ya sean relacionales o no relacionales, y aportan un valor significativamente superior.

Un datalake[55] es un repositorio único[56] que permite ingestar, almacenar y preprocesar grandes volúmenes de datos de múltiples fuentes y formatos, de forma estructurada o no estructurada.

Entre sus principales ventajas destacan:

— Almacenamiento flexible y versátil: pueden manejar datos en múltiples formatos y niveles de estructura e incluyen:

  • Estructurados (como los almacenados en bases de datos relacionales).

  • Semiestructurados (por ejemplo, archivos JSON o XML).

  • No estructurados (textos, imágenes, capturas de red).

  • Poco estructurados (como datos de sensores o comunicaciones interceptadas).

  Además, permiten guardar la misma información y de forma coherente en diferentes formatos simultáneamente (relacional, gráfico, vectorial, etc.), lo que facilita su consulta por parte de Sistemas de Inteligencia, Mando y Control, u otros sistemas que requieran distintos tipos de análisis.

— Integración de múltiples fuentes: unifican información que, por norma, estaría dispersa en sistemas independientes o «silos de datos». Esta centralización favorece la correlación entre datos de diferentes orígenes y herramientas, lo que ayuda a identificar patrones complejos o relaciones que pasarían desapercibidas en sistemas fragmentados.

---

[55] Un ***datalake*** es un repositorio centralizado que permite almacenar datos en su formato nativo, sin restricciones de estructura o tamaño. En el caso del SCOMCE, este ***datalake*** integrará (a diferencia de las bases de datos tradicionales) todo tipo de información y datos en bruto e incluirá una capa de ***software*** de procesado de datos específico para curar (fusionar, deduplicar, integrar, depurar, enriquecer, relacionar) los datos y la información según las necesidades analíticas del módulo ***software*** posterior del SCOMCE que consuma los datos del ***datalake***.

[56] Actúa como el «repositorio único de la verdad», almacena toda la información y datos (objetos, con sus parámetros/atributos y relaciones semánticas) correspondientes a las operaciones en el ciberespacio. La existencia de silos de información almacenados en distintos sistemas, herramientas y soluciones técnicas dificulta una visión única y clara de la situación en el ciberespacio y la correlación de datos: el descubrimiento de relaciones, patrones y tendencias.

— Preprocesamiento inteligente: antes de almacenar los datos, los *datalakes* pueden realizar tareas como eliminación de duplicados, corrección de inconsistencias y normalización, lo que mejora la calidad y coherencia de la información disponible.

— Escalabilidad: se adaptan fácil al crecimiento del volumen de datos sin necesidad de rediseñar la estructura y permiten almacenar grandes históricos, que son clave para análisis retrospectivos o anticipar tendencias futuras.

— Acceso centralizado: al concentrar toda la información en una única plataforma, se simplifica su gestión y acceso para los equipos de ciberdefensa y mejora la eficiencia operativa y la toma de decisiones.

Este *datalake* se convertirá en el repositorio desde el que los diferentes sistemas del SCOMCE consumirán los datos y la información y en el cual almacenaron los productos generados por los mismos.

6.1.1 Fuentes de información y datos a integrar

El *datalake* debe reunir información detallada y completa que abarque tres grandes áreas clave para la defensa en el ciberespacio:

— La misión: debe incluir misiones, planes, órdenes e informes operativos de todos los niveles de mando y niveles de la guerra. Esto permite analizar cómo dependen las operaciones de ciertas capacidades o servicios del ciberespacio y así identificar los riesgos asociados a posibles ataques que podrían afectar su ejecución.

— La amenaza (organizada por niveles):

- Estratégico: datos sobre actores potenciales, sus alianzas, doctrinas, capacidades, fuentes de financiación, métodos de formación y desarrollo de ciberarmas.
- Operacional: información sobre posibles intenciones, objetivos habituales, efectos que buscan generar y los integrantes que conforman estos grupos o entidades.
- Táctico: conjunto de tácticas, técnicas y procedimientos (TTP) empleados, vectores de entrada, infraestructuras utilizadas, tecnologías, herramientas, *malware* y ciberarmas disponibles.
- Técnico: detalles más específicos sobre las herramientas y *malware* utilizados, vulnerabilidades explotadas y los Indicadores de Compromiso (IOC) que pueden emplearse para detectar sus actividades.

— Información del ciberespacio propio: debe reflejar el estado de los activos y servicios, así como incluir vulnerabilidades, flujos de datos entre ellos, configuraciones de seguridad incorrectas o ausentes, relaciones entre componentes y la ubicación/configuración de los mecanismos de ciberseguridad y ciberdefensa.

La integración total de estos datos permite elaborar una visión única y compartida del ámbito de las operaciones en el ciberespacio (RCyP[57]).

6.1.2 Estructura del *datalake*

Un *datalake* de este tipo está, normalmente, estructurado en las siguientes áreas o zonas:

— Área Bronce: almacena los datos en bruto tal y como llegan.

— Área Plata: organiza los datos según una ontología específica del ciberespacio (relaciones entre activos, amenazas, misiones, etc.).

— Área Oro: almacena datos preprocesados listos para ser utilizados por sistemas de análisis e inteligencia artificial.

6.1.3 Desafío en la implementación de un *datalake*

El verdadero reto para implementar un *datalake* no es tanto tecnológico —hoy en día integrar diferentes fuentes de datos no representa una gran dificultad técnica—, sino más bien cultural y organizativo.

Para que este sistema sea de verdad eficaz, es fundamental que se integren datos provenientes de múltiples ámbitos:

— Los sistemas que gestionan el ciberespacio operativo, controlados por proveedores de servicios IT y OT.

— Los sistemas de Mando y Control (incluido los de planeamiento) en todos los niveles de la guerra y niveles de mando.

— Los sistemas de inteligencia sobre ciberamenazas militares, en los que se incluye, idealmente, información compartida desde organismos civiles, entidades privadas y administraciones públicas.

Sin embargo, esta integración, a menudo, se ve obstaculizada por una falta de comprensión del valor estratégico de la ciberdefensa y de la importancia de centralizar toda la información en una única plataforma que apoye tanto la inteligencia como la toma de decisiones en operaciones del ciberespacio.

[57] RCyP son las siglas que se corresponden con: «Recognized Cyber Picture».

6.2 Ontología

A diferencia de otros tipos de repositorios, un *datalake* requiere del desarrollo de un modelado de datos especifico, ya que no solo define los elementos clave (objetos o conceptos) del dominio, sino también sus atributos, relaciones y reglas que describen cómo interactúan entre sí. Este modelado de datos especifico se denomina «ontologías».

Una ontología es una representación formal y estructurada[58] del conocimiento dentro de un dominio específico, que permite modelar el conocimiento de una forma que puede ser entendida por humanos y procesada por máquinas, lo que la hace especialmente útil en áreas como la inteligencia artificial para realizar inferencias, la gestión del conocimiento, los sistemas expertos o la interoperabilidad entre sistemas. (Gruber, 1993).

Aunque no existe una ontología especifica de operaciones en el ciberespacio como ya lo existe en otros ámbitos de operaciones militares, si existe algunos elementos desde los cuales partir:

— Respecto al ciberespacio:

  - El modelo de datos CYBERDEM[59] estandarizado de SISO[60] que tiene como objetivo facilitar el intercambio de información del ciberespacio entre distintos sistemas, en especial, en contextos de simulación, entrenamiento, análisis y operaciones militares o de ciberdefensa (Simulation Interoperability Standards Organization. 2014).
  - El estándar abierto OASIS TOSCA[61] desarrollado por el consorcio OASIS[62] que permite definir, desplegar y gestionar aplicaciones y servicios en entornos de computación en la nube de forma portátil, automatizada e interoperable (Kirvan y Bigelow, 2023).

— Respecto a la Misión:

  - La ontología C2SIM[63] es una estructura conceptual formalizada que sirve para facilitar la interoperabilidad entre sistemas

[58] Define de forma estructurada los elementos clave (objetos), sus características (atributos) y las relaciones entre ellos.
[59] CYBERDEM son las siglas que se corresponden con: «Cyber Data Exchange Model».
[60] SISO son las siglas que se corresponden con: «Simulation Interoperability Standards Organization».
[61] OASIS TOSCA siglas que se corresponden con: «Topology and Orchestration Specification for Cloud Applications».
[62] OASIS son las siglas que se corresponden con: «Organization for the Advancement of Structured Information Standards».
[63] C2SIM son las siglas que se corresponden con: «Command and Control – Simulation Interoperation Ontology».

de mando y control (C2) y sistemas de simulación, sobre todo, en contextos militares o de defensa. La ontología C2SIM es un modelo formal que define los conceptos, relaciones y estructuras necesarias para que los sistemas C2 y SIM puedan intercambiar información de forma precisa y sin ambigüedades. Está basada en estándares abiertos y es promovida por organismos como la OTAN, SISO (NATO Science and Technology Organization, 2024).

— Respecto a la amenaza:

- MISP (Multinational Intelligence Sharing Platform), dispone de una pequeña ontología que puede servir de punto de partida para estructurar la información sobre ciberamenazas. Sin embargo, esta ontología necesita ser ampliada y enriquecida, tanto en términos de atributos como de objetos, para cubrir de forma adecuada las necesidades de modelado de inteligencia de ciberamenazas en todos los niveles de la guerra, desde el técnico hasta el estratégico.
- Las «Matrices MITRE ATT&CK», que permiten representar las tácticas, técnicas y procedimientos (TTP) utilizados por los actores de amenazas.
- El «Modelo de Diamante» de análisis de incidentes de seguridad y ciberataques.

6.3 Aplicación de Inteligencia Artificial (IA)

La IA (DL[64] y ML[65]) desempeñará un papel clave en los procesos de análisis de datos e información. Gracias al diseño del sistema y a los módulos especializados de IA, el SCOMCE proporcionará una capacidad avanzada de procesamiento inteligente de datos, de modo que integrará capacidades de análisis, correlación y automatización que faciliten (Kirkpatrick,2024):

— Automatización de tareas[66]: el sistema también incorporará funcionalidades de inteligencia artificial orientadas a automatizar tareas repetitivas o de alto volumen, como:

[64] DL es una sigla que se corresponde con: «Deep Learning», Inteligencia Artificial basada en redes neuronales.

[65] ML es una sigla que se corresponde con: «Machine learning» o aprendizaje automático. Inteligencia artificial basada, principalmente, en estudios de análisis estadísticos de regresión.

[66] Este tipo de capacidades de automatización de actividades repetitivas y rutinarias podrán ser llevadas a cabo por agentes de IA, que permitirán reducir el personal necesario para este tipo de actividades rutinarias y que será esencial para poder reducir el tamaño de los Cuarteles Generales y, por lo tanto, su huella táctica, esencial en entornos en lo que las capacidades de detección del adversario por medios satélites, etc. son muy potentes.

- Búsqueda y extracción automática de información o datos desde un repositorio de documentos no estructurados, incluso se señala en qué documento y párrafo se encuentran las respuestas a la búsqueda.
- Generación de borradores de informes, productos de inteligencia y análisis y resúmenes, lo que agiliza el trabajo de documentación.
- Transcripción y análisis de reuniones, que incluye la identificación y extracción de ideas clave y elementos relevantes.
- Priorización inteligente de correos y tareas, lo que ayuda a enfocar los esfuerzos en lo más urgente y relevante. Contestar de forma automática correos rutinarios.
- Organizar y coordinar tareas y reuniones.
- Automatizar flujos de trabajo.
- Revisión gramatical, traducciones, mejoras de estilo, etc.

— Capacidades analíticas avanzadas:

- Correlar información compleja entre múltiples tipos de datos y objetos y detectar conexiones ocultas entre incidentes, comportamientos y entidades.
- Detectar patrones tanto en el comportamiento del sistema como en el de posibles actores de amenazas.
- Detectar anomalías, identificar comportamientos inusuales a partir del modelo habitual del sistema.
- Modelar actores y comportamientos, lo que representa grupos de amenazas en forma de vectores que representen el comportamiento de grupos de amenazas específicos
- Establecer atribuciones técnicas y tácticas, así como comparar el perfil de un incidente con el de actores conocidos para estimar la probabilidad de su autoría.
- Analizar vulnerabilidades históricas, lo que genera mapas de calor que muestran cuáles han sido más explotadas por diferentes tipos de amenazas.
- Reconstruir líneas de tiempo precisas de los eventos, para facilitar la comprensión del desarrollo de los incidentes.
- Relacionar datos actuales con registros históricos, como *logs* o reportes previos, para identificar similitudes o conexiones relevantes.

- Detectar tendencias y evoluciones y comparar comportamientos pasados con los actuales y anticipar movimientos futuros del adversario.
- Asistencia en la investigación de ciberataques, mediante consultas directas a los datos mediante IA, con preguntas del tipo: ¿qué ocurrió al mismo tiempo que ocurrió tal suceso?, ¿qué vulnerabilidades existían en un activo en tal momento en que se detectó tal evento?
- Clasificar y agrupar (incidentes, *logs*, alertas relacionados), lo que permite investigarlos de manera conjunta y eficiente.
- Reducir falsos positivos, lo que refina las reglas de detección y disminuye la carga de trabajo manual de los analistas.

— Análisis predictivo:

- Mediante técnicas de análisis predictivo, el sistema podrá anticipar acciones futuras del adversario y evaluar riesgos potenciales.

— Sensores de detección avanzados: los sensores basado en inteligencia artificial detectará no por firmas estáticas, ni reglas predefinidas por operadores, sino por patrones comunes:

- En *malware* conocidos: se comparan patrones de *malware* conocidos (modelados de *malwares*). Esto permitirá identificar nuevas variantes de *malware*, aunque el código haya sido modificado parcialmente. En lugar de usar firmas fijas, se identifican patrones comunes.
- En comportamiento de actores: mediante modelado de actores de forma automática por IA se podrá detectar comportamientos en los sistemas que se asemejen a los modelados de un actor. Esto permitirá detectar actividades maliciosas por medio de sensores configurados con reglas configurados por modelados de la amenaza directamente, sin intervención humana.

En conjunto, estas capacidades permitirán a SCOMCE mejorar la eficacia operativa, reducir tiempos de respuesta y aumentar la precisión del análisis y la defensa en el ciberespacio. La combinación de automatización, inteligencia artificial y análisis de datos avanzados convierte a esta herramienta en un pilar esencial para la ciberdefensa moderna.

6.4 Aplicación de técnicas de simulación

Una vez modelados los actores de la amenaza, sus comportamientos y el entorno del Ciberespacio, estos modelos pueden utilizarse para ejecutar simulaciones tácticas y operacionales, que permitan:

— Realizar ejercicios de *wargaming* automatizados.

— Evaluar COA[67] de defensa y reacción ante un ataque simulado.

— Realizar Análisis Operacionales, mediante una cooperación o confrontación exhaustiva de forma automatizada de las potenciales COA propias y adversarias a nivel táctico y técnico, mediante la definición de parámetros que diferencien las diferentes COA a definir de un lado y otro.

6.4.1 Simulación como herramienta estratégica

La simulación es una capacidad clave en el ámbito de la ciberdefensa, ya que permite:

— Recrear ataques sobre infraestructuras reales o virtuales.

— Verificar la efectividad de las defensas implementadas.

— Evaluar cómo responde un sistema frente a distintos tipos de amenazas.

En la actualidad, existen herramientas avanzadas que permiten simular el comportamiento de atacantes reales, conocidas como «Breach and Attack Simulations» (Ciberseguridad.blog, (s. f.).

Estas soluciones replican los métodos y tácticas utilizados por actores maliciosos, lo que permite poner a prueba los sistemas de defensa en un entorno controlado. Sin embargo, la mayoría de estas herramientas están desarrolladas por empresas estadounidenses o israelíes y operan desde la nube. Esto implica que, al utilizar estos servicios, se estaría compartiendo información sensible sobre nuestras vulnerabilidades con entidades extranjeras, lo cual representa un riesgo para la seguridad nacional.

Por esta razón, es fundamental que empresas nacionales desarrollen sus propias soluciones de simulación. La arquitectura de estas herramientas debe ser modular y permitir la creación de agentes específicos que simulen técnicas y tácticas utilizadas por diferentes atacantes. Esto facilita una simulación más precisa y flexible, ya que, en lugar de imitar a un atacante completo, se pueden reproducir secuencias específicas de acciones (*workflows*) que siguen el mismo patrón que utilizaría un atacante real.

Existen dos tipos principales de simulaciones:

— Simulación tipo *Live*: reproduce técnicamente el proceso de un ataque y utiliza herramientas y *software* malicioso (modificado o simulado para que no cause daño). Aunque interactúa con el sistema real

[67] COA son las siglas que se corresponden con «Course of Action» (Línea de acción).

y puede generar cierta resistencia por parte de los proveedores de servicios, estas simulaciones no suelen tener consecuencias negativas reales.

— Simulación tipo TTX (*Tabletop Exercise*): se trata de un ejercicio teórico que analiza un posible ataque con el que se comparan configuraciones, vulnerabilidades y herramientas, sin interactuar directamente con el sistema real. Es una forma más segura y menos invasiva de evaluar la preparación ante amenazas.

7 Conclusiones

El ámbito o dominio del ciberespacio ha dejado de ser un ámbito exclusivamente técnico para convertirse en un escenario estratégico de las operaciones militares. Esta transformación exige una evolución desde la ciberseguridad tradicional —centrada en la protección técnica de sistemas— hacia una ciberdefensa integral, basada en el análisis vulnerabilidades del entorno, dirigida por inteligencia de ciberamenazas y enfocada en el cumplimiento de la misión / operación militar.

Sin embargo, la evolución no es técnica, es doctrinal: pasar de proteger sistemas a anticipar ataques, de reaccionar a decidir antes que el adversario. Esa es la esencia de una verdadera ciberdefensa.

El papel de la Inteligencia de ciberamenazas ha sido clave en esta transición, lo que ha permitido anticiparse al adversario, comprender su comportamiento y preparar defensas proactivas y específicas. No se trata solo de proteger, sino de asegurar la libertad de acción en el ciberespacio y garantizar la continuidad de las operaciones militares frente a actores hostiles cada vez más sofisticados.

El proceso de «operacionalización del Ciberespacio», liderado por el MCCE, representa una respuesta innovadora y necesaria para enfrentar los retos actuales. No basta con defender sistemas, hay que defender la misión, identificar al adversario y preparar al entorno digital para resistir, responder y recuperarse ante cualquier ataque.

La verdadera defensa comienza cuando se protege lo que da sentido a los sistemas: la misión. Blindar solo la infraestructura, sin considerar su impacto operativo, es como fortificar un castillo sin custodiar al rey.

El avance de la ciberdefensa y, en particular, de la inteligencia de ciberamenazas depende directamente de la adopción inteligente de nuevas tecnologías no solo para proteger sistemas o elaborar inteligencia, sino para transformar la forma en que se opera y combate en el ciberespacio.

La implementación de plataformas como PICO y el desarrollo de sistemas más ambiciosos como SCOMCE —apoyados en tecnologías de *datalakes*,

inteligencia artificial y simulación— marcarán un punto de inflexión. Estas herramientas permiten automatizar procesos, modelar amenazas, atribuir incidentes, optimizar recursos y ejecutar operaciones defensivas con una base analítica y predictiva.

Por último, es fundamental consolidar una industria nacional de ciberdefensa, capaz de proporcionar las tecnologías necesarias con plena soberanía, de modo que evite la dependencia de terceros y fortalezca las capacidades estructurales del Estado para operar con eficacia en este dominio decisivo del siglo XXI.

En el siglo XXI, las guerras ya no se libran solo en tierra, mar o aire. Se infiltran en redes, se ejecutan en código y se deciden en servidores. El ciberespacio no es solo un escenario: es el frente más dinámico y menos visible de cualquier conflicto moderno.

Disclaimer

Las opiniones o ideas expresadas en este artículo son responsabilidad exclusiva del autor y no reflejan necesariamente las de la Unión Europea ni de la OTAN ni de las FAS de España ni de la Empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica), ni la Empresa INDRA; y no pueden ser consideradas responsables de la mismas, por lo tanto.

Agradecimiento

Las imágenes referentes a la herramienta PICO han sido cedidas y autorizadas para este artículo por la Empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica).

Las imágenes referentes al proyecto ECYSAP han sido cedidas y autorizadas tanto por la Empresa INDRA como por NATO ACT CyBER.

Bibliografía

Arteaga, F. y Alonso Lecuit, J. A. (2025). El concepto de Ciberdefensa Activa. Real Instituto Elcano. [Consulta: 2025]. Disponible en: https://www.realinstitutoelcano.org/analisis/el-concepto-de-ciberdefensa-activa/ LinkedIn+1Real Instituto Elcano+1

Corletti Estrada, A. (2017). Ciberseguridad (Una Estrategia Informático/ Militar). DarFe. [Consulta: 2025]. Disponible en: http://www.darfe.es

Gruber, T. R. (1993). *A translation approach to portable ontology specifications*. *Knowledge Acquisition*. Knowledge Acquisition. *5*(2), pp. 199-220. DOI: https://doi.org/10.1006/knac.1993.1008

Internet Security Auditors. (2025). Evolución del malware: tendencias y cómo combatirlo. Internet Security Auditors. [Consulta: 2025]. Disponibleen:https://blog.isecauditors.com/evolucion-del-malware-tendencias-y-como-combatirloBlog de Internet Security Auditors

Junta Interamericana de Defensa. (2023). *Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar* [en línea]. [Consulta: 2025]. Disponible en: https://jid.org/publicaciones/guia-de-ciberdefensa-orientaciones-para-el-diseno-planeamiento-implantacion-y-desarrollo-de-una-ciberdefensa-militar/

Kirkpatrick, R. G. (2024). The Saint Russ Initiative: AI's Cutting-Edge Tactics for Cyber Safety.

Kirvan, P. y Bigelow, S. J. (2023). TOSCA (Topology and Orchestration Specification for Cloud Applications). TechTarget. [Consulta: 2025] Disponible en: https://www.techtarget.com/searchcloudcomputing/definition/TOSCA-Topology-and-Orchestration-Specification-for-Cloud-Applications

Multinational Capability Development Campaign. (2017). *MCDC 2015–2016: MDCO Planning Guide (Version 1.0)*.

NATO Science and Technology Organization. (2024). *Technical description of C2SIM* (STO-EN-MSG-211-2.3). Disponible en: https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-211/EN-MSG-211-2.3.pdf

NATO. (2016). Warsaw Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 [en línea]. [Consulta: 2025]. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_133169.htmNATO+7NATO+7European Sources Online+7

Ramiro, R. (s. f.). Conoce la tecnología «Breach and Attack Simulation» (BAS) y resucita tu estrategia de ciberseguridad. Ciberseguridad. blog. [Consulta: 2025] Disponible en: https://ciberseguridad.blog/conoce-la-tecnologia-breach-and-attack-simulation-bas-y-resucita-tu-estrategia-de-ciberseguridad/

Rodríguez, D. (2023). Ni mar ni tierra ni aire ni espacio: el grupo especial del Ejército español que custodia el quinto dominio. *HuffPost*. [Consulta: 2025]. Disponible en: https://www.huffingtonpost.es/tecnologia/ni-mar-tierra-aire-espacio-grupo-especial-ejercito-espanol-custodia-el-quinto-dominio.html

Seguritecnia. (2023). ¿Qué es la ciberdefensa? [en línea]. Seguritecnia. [Consulta: 2025]. Disponible en: https://www.seguritecnia.es/actualidad/que-es-la-ciberdefensa_20230203.html

Simulation Interoperability Standards Organization (SISO). (2024). *SISO-REF-072-2024: Cyber DEM BONES (Base Objects, Networks, Effects, & Specifications)*. [Consulta: 2025]. Disponible en: https://cdn.ymaws.com/www.sisostandards.org/resource/resmgr/reference_documents_/siso-ref-072-2024.pdf

U.S. Department of the Army. (2009). FM 2-01.3: Intelligence preparation of the battlefield/battlespace. Washington, D.C., Headquarters, Department of the Army.

Winterfeld, S. P. (2002). *Cyber IPB*. Global Information Assurance Certification (GIAC). Disponible en: https://www.giac.org/paper/gsec/1752/cyber-ipb/103147Wikipedia+2GIAC+2GIAC+2.

Matrices de impacto cruzado y método estructural: una revisión parcial o de herramientas para la construcción de escenarios futuros

Licesio J. Rodríguez-Aragón

«All models are wrong, but some are useful». G. E. Box (1919-2013)

Resumen

Las matrices de impacto cruzado y el método estructural son herramientas usadas para la construcción de escenarios futuros. Estas técnicas permiten evaluar cómo la ocurrencia de un evento puede influir en la probabilidad de ocurrencia de otros eventos, facilitando la planificación estratégica en situaciones de incertidumbre. En este trabajo buscamos presentar algunas de las herramientas que se utilizan a la hora de trabajar con las matrices de impacto y que permiten analizar las relaciones indirectas y clasificar las variables del sistema, revelando variables ocultas que ganan relevancia a través de relaciones indirectas.

Palabras clave

Método estructural, Matrices de impacto cruzado, MICMAC, Multiplicación de la matriz de impactos.

Cross-impact matrices and structural method: a partial review of tools for the construction of future scenarios

Abstract

Cross-impact matrices and the structural method are tools used for constructing future scenarios. These techniques allow us to evaluate how the occurrence of an event can influence the probability of occurrence of other events, facilitating strategic planning in situations of uncertainty. In this work we seek to present some of the tools that are used when working with impact matrices and that allow us to analyze indirect relationships and classify system variables, revealing hidden variables that gain relevance through indirect relationships.

Keywords

Structural Method, Cross Impact Matrices, MICMAC, Impact Matrix Multiplication.

1 Introducción

Las matrices de impacto cruzado son una técnica de modelización de la realidad utilizada para evaluar cómo la ocurrencia de un evento puede influir en la probabilidad de otros eventos. Este método fue, en un inicio, planteado por Theodore Gordon, Olaf Helmer y Hans Goldschmidt en el año 1966. Estos autores se basaron en la idea de que los eventos no ocurren de manera aislada, sino que están interrelacionados.

La primera aplicación de la metodología de impactos cruzados fue lúdica. Con motivo de su veinte aniversario, la empresa Kaiser Aluminum & Chemical Corporation, ya experta en estimular la imaginación pública con ideas futuristas, distribuyó un juego de mesa conmemorativo llamado *Futures*. El objetivo principal del juego era incitar a los participantes a comprender y usar en su beneficio cómo diferentes eventos futuros podrían influenciarse mutuamente y cómo estos impactos cruzados podrían afectar el desarrollo de escenarios futuros. Esto se lograba mediante la evaluación de las probabilidades condicionales de que un evento ocurriera dado que otro evento ya había sucedido.

El juego[1], hoy descatalogado y que puede admirarse en algunos museos, consistía en una serie de sesenta cartas, cada una de las cuales describe un posible evento futuro. Este listado de eventos futuros surgió de un trabajo previo desarrollado por Gordon y Helmer-Hirschberg (1964) en el que se planteaban, a través de un Delphi, un ejercicio experimental de predicción de tendencias futuras en un horizonte de cincuenta años. Algunos de estos eventos eran: la aparición de metales ultraligeros, prohibición de circulación de vehículos por las ciudades, conexiones cerebro-ordenador o alianzas militares y económicas con Rusia. Cada carta contenía una breve descripción del evento y una probabilidad de ocurrencia, *a priori*, de dicho evento asignada por los expertos. Para cada evento, se ajustaba un deslizador de color en el tablero del juego, marcando la probabilidad determinada por los expertos y se fijaba un horizonte de veinte años, 1986, como objetivo para validar las predicciones (figura 1).

Durante el desarrollo del juego, para determinar si un evento ocurre, se lanza un dado, un icosaedro de veinte caras triangulares. Si alguno de los tres números en la cara superior coincide con la probabilidad establecida por los expertos, el evento se ha materializado en 1986 y al dar la vuelta a la carta del evento aparecen los eventos sobre los que esta ocurrencia influye o impacta: aumenta o disminuye su probabilidad de ocurrencia. Por ejemplo, si se logra desarrollar la antigravedad, aumentarían las probabilidades de poder construir bases de exploración en otros planetas y, sin embargo, el uso de cohetes como medios de transporte perdería

[1] Véase: https://patents.google.com/patent/US3473802.

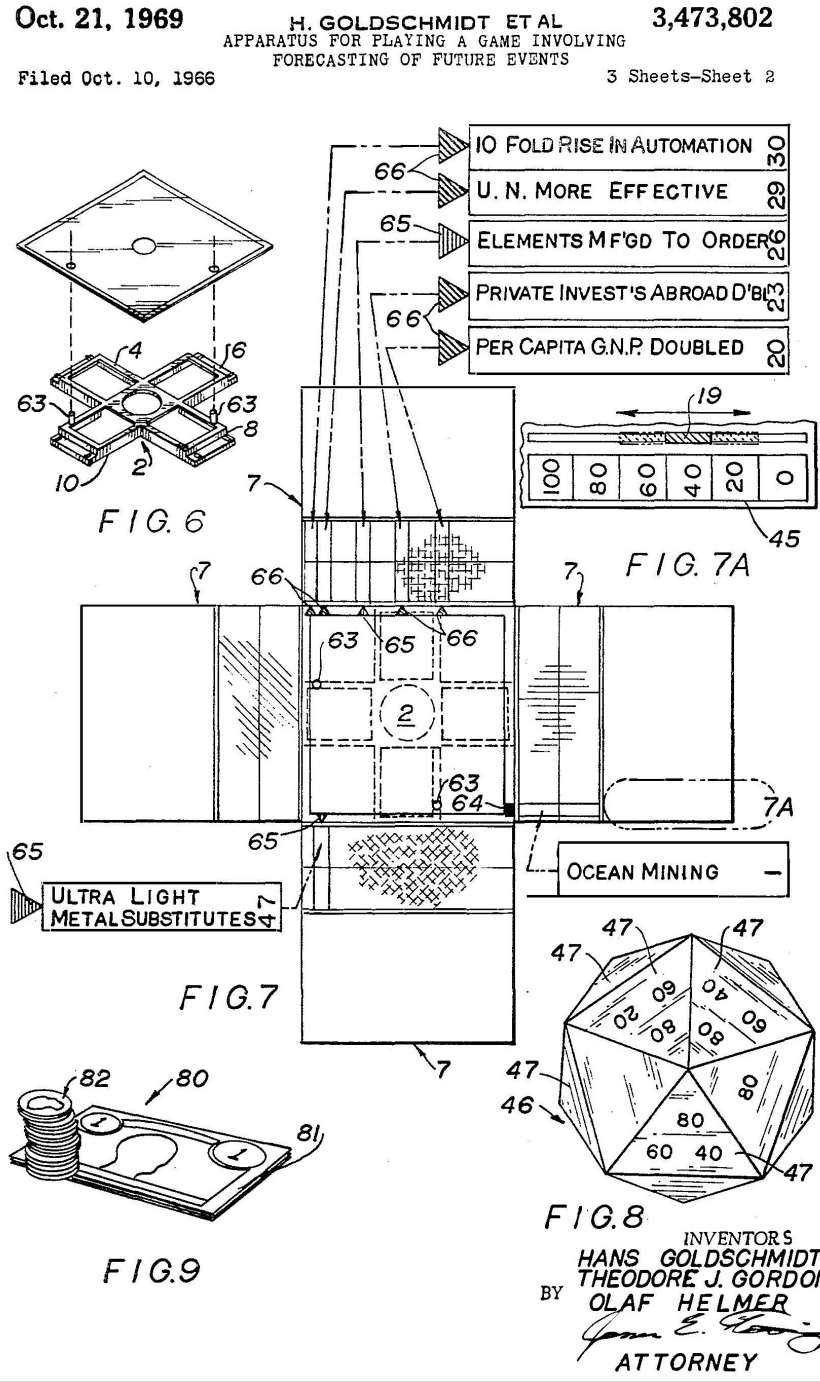


Figura 1: Patente USA US 3,473,802 del juego Futures: aparato para jugar un juego que implica la predicción de eventos futuros. Fuente: https://patents.google.com/patent/US3473802

popularidad. Esta influencia sobre otros eventos viene explicada de forma breve en cada carta mediante un razonamiento verosímil y con la ayuda del tablero se pueden actualizar sus probabilidades de ocurrencia.

De esta manera el juego avanza, de modo que quedan cartas boca arriba y, por lo tanto, sin haberse producido dicho evento o boca abajo cuando se han materializado. La ocurrencia o no de los eventos venía determinada por las probabilidades fijadas en un inicio por los expertos, el azar del dado y los impactos, positivos o negativos, de los eventos que se materializan. El juego se podía enriquecer con el uso de dinero, comprando probabilidades, impulsando o frenando diferentes innovaciones o avances sociales, de la misma manera que lo haría un plan de I+D+i. Una estrategia ganadora consistía en invertir en eventos que, de forma indirecta, terminaban impactando en tu propio beneficio. El ganador del juego sería entonces quien hubiera logrado sacar mayor provecho del futuro.

La metodología descrita en el juego fue implementada en un ordenador por Gordon y Hayward (1968) y permitía definir: *los eventos*, que, inicialmente, eran ordenados de forma aleatoria, y *las probabilidades* de impacto cruzado. Mediante una estrategia de simulación, esta operación se repetía varias veces y analizaba de forma cuantitativa qué escenarios se producían en cada jugada y cuáles, por lo tanto, serían más probables.

La estrategia de modelización y prospección de futuros que se quiere describir está basada en el Análisis Estructural y el Análisis de Escenarios. El primero busca identificar y analizar las relaciones entre factores o variables clave de un problema, seleccionando las que más influyen. El segundo implica el desarrollo de múltiples escenarios posibles para el futuro, basados en diferentes combinaciones de variables y factores. Sus orígenes se centran en la planificación empresarial y también militar desarrollada desde mediados del pasado siglo XX. El Análisis Estructural tiene sus orígenes en los trabajos de Michel Godet (Godet, 1974; Godet y Duperrin, 1975) y su equipo en el Instituto de Estudios Políticos de París mientras que el Análisis de Escenarios surge de la propuesta de Herman Kahn y la RAND Corporation (Kahn y Wiener, 1967). Ambas estrategias se complementan al proporcionar una comprensión detallada de las variables clave y sus interacciones, lo que permite desarrollar escenarios más robustos y útiles para la toma de decisiones estratégicas.

2 Modelización y Simulación en Prospectiva

Uno de los principales retos a los que se enfrentan las organizaciones y gobiernos es la toma de decisiones en situaciones de incertidumbre. Situaciones en las que hay un gran número de factores que influyen, lo que genera una gran variabilidad. En el ámbito de la prospectiva y la estrategia, donde la toma de decisiones se enfoca en el estudio y análisis de posibles

futuros para anticipar y preparar estrategias adecuadas, el uso de modelos y simulaciones es fundamental.

Se pueden recordar las siete ideas clave en el ámbito de la prospectiva que Godet (1986) plantea:

- Clarificar las acciones presentes a la luz del futuro.
- Explorar múltiples y futuros inciertos.
- Adoptar un enfoque global y sistémico.
- Tener en cuenta factores cualitativos y las estrategias de los actores.
- Hay que recordar siempre que la información y las previsiones no son neutrales.
- Optar por una pluralidad y complementariedad de enfoques.
- Cuestionar las ideas preconcebidas sobre las previsiones y los pronosticadores.

Ante un problema o situación novedosa, es fundamental identificar sus características principales y comprender cómo se relacionan entre sí y con los fenómenos que lo rodean. Este enfoque permite descomponer los fenómenos complejos en partes más sencillas, lo que facilita el análisis y la toma de decisiones. Al entender estas interacciones, se pueden desarrollar modelos que capturen los aspectos más relevantes del sistema, de modo que permite acercarse a la compresión del fenómeno, predecir su comportamiento y optimizar nuestras estrategias para abordar el problema de manera efectiva.

La realidad es siempre sorprendente y son pocas las ocasiones en las que somos capaces de anticiparnos a ella. Reconocer la dificultad de los problemas reales es fundamental para acercarse a ellos con humildad y espíritu crítico, característica fundamental para poder trabajar en la solución de los retos que presentan.

2.1 Modelización

La modelización es de gran utilidad, porque permite simplificar la complejidad inherente de la realidad y hace que los sistemas sean más comprensibles y manejables. Es muy importante entender que los modelos nunca pueden capturar todos los detalles de un sistema real, pero que proporcionarán una representación útil en la que deben destacar los aspectos más relevantes y permitirán realizar análisis y predicciones. Al enfocarse en las características más importantes, los modelos ayudan a entender mejor el comportamiento de los sistemas, tomar decisiones informadas y comunicar ideas de manera efectiva.

De manera muy breve, se pueden clasificar los modelos en:

— Físicos: como representaciones tangibles de objetos, maquetas, prototipos.

— Conceptuales: que permiten identificar, visualizar y entender las relaciones entre variables.

— Matemáticos: que utilizan fórmulas, ecuaciones, relaciones algebraicas, para definir las relaciones y que pueden incorporar componentes estocásticas (azar) para incluir la variabilidad propia de los fenómenos aleatorios.

— Computacionales: como implementaciones en software de los modelos, tanto físicos como matemáticos, de tal manera que es posible realizar simulaciones y experimentos virtuales de estos fenómenos gracias a la capacidad de cálculo de los ordenadores.

La modelización, es una herramienta útil en la toma de decisiones económicas, políticas y de gestión, pero se debe recordar que los modelos que describen explican y predicen procesos, no son infalibles y deben considerarse en su contexto específico, lo que reconoce, por tanto, sus fortalezas, pero, sobre todo, sus limitaciones. La claridad y la precisión son características deseables en los modelos y una de sus mayores ventajas es la capacidad de analizar escenarios, lo que evalúa el impacto de las posibles decisiones a tomar antes de implementarlas.

Los objetivos principales de cualquier modelo son proporcionar una comprensión más profunda de un sistema o proceso y utilizar este conocimiento para hacer predicciones y tomar decisiones. Sin embargo, los modelos son simplificaciones de la realidad y al usarlos hay que ser conscientes de sus errores y limitaciones. Es crucial que los responsables de la toma de decisiones comprendan estas limitaciones y las tengan en cuenta en sus interpretaciones.

Además, la modelización debe ser sencilla. El uso de modelos artificialmente complejos, que exceden nuestras capacidades físicas, conceptuales, matemáticas o computacionales presenta serios inconvenientes entre los que se puede citar: riesgos de interpretaciones incorrectas, falta de transparencia, suposiciones ocultas, dificultades en la validación, dependencia excesiva, sobreaprendizaje, falta de flexibilidad ante cambios, entre otros muchos inconvenientes.

La colaboración entre disciplinas cuantitativas y cualitativas es esencial para aprovechar al máximo el potencial de la modelización. Reconociendo sus complejidades y sus limitaciones, la modelización cooperativa e informada, usando distintas técnicas y entre distintas disciplinas científicas tiene un enorme potencial.

2.2 Simulación

Cuando el reto o la dificultad a la que nos enfrentamos cambia a lo largo del tiempo, influenciado por los factores o las variable que le rodean, se dice de él que tiene una característica dinámica y el modelo debe disponer de esa característica. El modelo debe ser entonces capaz de cambiar, de alguna manera, a lo largo del tiempo. Esto implica derivar la estructura futura del modelo bien mediante razonamientos lógicos o bien mediante relaciones matemáticas que incluyen cambios en el modelo dependientes del tiempo y de los factores que influyen.

Llevar a cabo una simulación, consiste en observar cómo, dadas unas condiciones iniciales para el problema, que definen momentáneamente el modelo, el modelo se adapta a los cambios producidos por los incrementos del tiempo. La ventaja de este procedimiento es que permite observar la evolución futura de nuestro problema siempre teniendo en cuenta que las condiciones iniciales o de partida influyen y determinan la evolución de la simulación del problema.

La validación de una simulación puede realizarse comparando evoluciones pasadas del problema y, por lo tanto, ya conocidas con el comportamiento del modelo en una o varias simulaciones llevadas desde las condiciones iniciales en las que se encontraba el problema.

La utilidad de la simulación es doble. Por un lado, permite entender cómo funciona el problema y qué factores influyen sobre él, al observar su evolución bajo distintas condiciones y horizontes temporales. Por otro, la simulación puede mostrar posibles situaciones futuras del problema con el paso del tiempo. Sin embargo, no se debe confundir este futuro con una predicción, ya que la dependencia de ese futuro de las condiciones iniciales proporciona no solo un futuro, sino un abanico de situaciones futuras posibles o probables, cada una en su medida.

La simulación se centra en el desarrollo de teorías acerca del comportamiento y la evolución del problema, en lugar de en el desarrollo de un modelado preciso del mismo. La simulación permite, dadas unas condiciones iniciales, analizar inductivamente, lo que generaliza los resultados obtenidos de las situaciones o experimentos simulados. Hay que tener en cuenta que la simulación requiere múltiples ejecuciones, ya que una única simulación proporciona información muy limitada, dada la dependencia de las simulaciones de las condiciones iniciales del problema y de los factores aleatorios propios de la simulación. La simulación tiene la gran ventaja de permitir trabajar con copias artificiales del problema, de modo que pueda actuar sobre ellas y explore su futura evolución.

3 Matrices de Impacto Cruzado (Cross-Impact Matrix Methods)

Las matrices de impacto cruzado (Cross-Impact Matrix Methods) son una herramienta utilizada para analizar cómo la ocurrencia de un evento puede influir en la ocurrencia de otros eventos. El trabajo de Gordon y Hayward (1968), titulado Initial *Experiments with the Cross-Impact Matrix Method of Forecasting* es un estudio pionero en el planteamiento de las matrices de impacto cruzado para la previsión y el análisis de escenarios futuros. Este método se diseñó para ayudar a prever cómo las relaciones entre eventos influirían sobre los resultados futuros, lo que reducía así la incertidumbre en la planificación y la toma de decisiones.

El análisis de impacto cruzado se basa en la creación de una matriz que evalúa las probabilidades de que ciertos eventos ocurran y conozcan la ocurrencia de otros eventos. Estas probabilidades se conocen como probabilidades condicionadas. Los pasos básicos en la definición de la matriz de impacto cruzado incluyen:

1. **Identificación de Eventos**: selección de eventos o variables relevantes que podrían influir en el sistema bajo estudio.
2. **Evaluación de Probabilidades**: asignación de probabilidades iniciales a cada evento.
3. **Análisis de Impacto**: evaluación de cómo la ocurrencia de un evento afecta la probabilidad de otros eventos.
4. **Construcción de la Matriz**: creación de una matriz que visualiza estas interacciones y probabilidades condicionadas.
5. **Interpretación de Resultados**: análisis de la matriz para identificar escenarios probables y las interacciones más significativas.

Una matriz de impacto cruzado puede entenderse como una tabla, cuadrada con n filas y n columnas, siendo n el número de eventos o variables relevantes que influyen en el sistema bajo estudio. Cada casilla de la tabla representa el impacto que tiene la ocurrencia del evento i –ésimo sobre evento j –ésimo, $P(j|i) = a_{ij}$. Esta probabilidad se conoce como probabilidad condicionada y expresa la probabilidad de que habiendo ocurrido el evento i –ésimo, ocurra el evento j –ésimo, $P(j|i) = a_{ij}$. Las diagonales indican el impacto que un evento produce sobre si mismo y en principio dicho impacto es nulo, apareciendo, por lo tanto, **0** en la diagonal de la matriz, $a_{ii} = 0$.

$$\begin{table} \begin{array}{c|ccc} \text{entonces $\rightarrow$ }& \text{Evento 1} & \text{Evento 2} & \text{Evento 3} \\ \text{Si ocurre $\downarrow$}& & & \\ \hline \text{Evento 1} & 0 & a_{12} & a_{13} \\ \text{Evento 2} & a_{21} & 0 & a_{23} \\ \text{Evento 3} & a_{31} & a_{32} & 0 \\ \end{array} \end{table} $$

Esta es la forma en la que Gordon y Hayward (1968) definen esta matriz, pudiéndose encontrar trabajos que utilizan el criterio traspuesto, llamando $a_{i,j} = P(i|j)$ al impacto sobre el evento i –ésimo de la ocurrencia del evento j –ésimo, $j \rightarrow i$. Este enfoque solo implica cambiar filas por columnas en la matriz.

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} \\ a_{21} & 0 & a_{23} \\ a_{31} & a_{32} & 0 \end{pmatrix}.$$

Existen en la literatura, al menos, tres formas diferentes de interpretar el impacto de unos eventos sobre otros a la hora de construir la matriz de impacto:

En primer lugar, si la matriz no contiene información cuantitativa, sino que solo busca determinar cadenas de causalidad que permitan construir escenarios probables, se puede rellenar la matriz con 0 y 1 (Chatziioannou *et al*., 2023). Se usará $a_{ij} = 0$ cuando no hay relación entre la ocurrencia del evento i y el evento j. Sin embargo, si la ocurrencia del evento i provoca la ocurrencia del evento j se usará $a_{i,j} = 1$.

En segundo lugar, se puede optar por cuantificar la influencia entre los eventos en una escala como, por ejemplo: 0 ,1 ,2 ,3 . Representando impacto despreciable el 0, pequeño para el 1, considerable para el 2 y grande para el 3. Entre las ventajas que se enumeran para usar escalas en la matriz de impactos están: una menor complejidad, una evaluación más rápida, mayor adaptabilidad y más claridad (Nazlabadi *et al*., 2023). En otros casos, se pueden usar escalas con impactos negativos, como por ejemplo del –5 al 5, lo que permite incluir no solo la magnitud del impacto sino también la dirección.

Por último, se puede optar por el enfoque original de Gordon y Hayward (1968) en forma de probabilidades condicionadas. Este enfoque también es el que utiliza Godet (1974) en su trabajo, en el que proponen el método SMIC 74 (Système de Matrices d'Impacts Croisés) y cuya aplicación, aunque matemáticamente pueda parecer más apropiada, presenta mayores dificultades. El trabajo de Godet y Duperrin (1975) provocó una interesante discusión a través de diferentes artículos publicados a lo largo de 1976 en la revisa *Futures*. El problema surge al regularizar los valores dados por los expertos, ya que las probabilidades expresadas resultan no ser consistentes y no cumplir con los axiomas de la probabilidad. El método utilizado para corregir esta inconsistencia produce soluciones no únicas al problema según detallan Mitchell y Tydeman (1976). La simplificación de la realidad necesaria para construir modelos causales produce entonces una paradoja por la aplicación de regularizaciones matemáticas que son necesarias para dotar de consistencia probabilística al modelo.

La reflexión con la que McLean (1976) cierra la discusión planteada en la revista *Futures*, destaca que la metodología de impactos cruzados no es una ciencia exacta, sino que debe entenderse como un método heurístico que puede ayudarnos a mejorar el conocimiento de problemas complejos en el área de la prospectiva. El mismo Gordon (1994) valora, años después, de forma positiva, la combinación de esta metodología con las técnicas de simulación y destaca la dificultad que supone para los expertos expresar juicios en términos probabilísticos. La aplicación de las técnicas de modelización causal mediante las matrices de impacto se centra solo en las interacciones entre parejas de eventos, cuando estas interacciones en el mundo real suelen producirse a través de estructuras más complejas y de mayor orden de interacción, triples, cuádruples, etc.

Existen métodos que combinan varias de las estrategias mencionadas hasta aquí, por ejemplo, el trabajo de Chao (2008) plantea un mecanismo de regularización de las probabilidades condicionadas y tiene en cuenta no solo las probabilidades expresadas por los expertos, sino también los impactos expresados en términos de escala.

4 Análisis Estructural de las Matrices de Impacto

La información recogida en una matriz de impacto puede representarse gráficamente en forma de un grafo formado por: *nodos*, que representan los eventos o variables, y *aristas*, que representan las relaciones entre los nodos con una dirección y un peso (Menéndez Velázquez, 1998). Esta representación en forma de grafo puede entenderse como un diagrama de causa-efecto y, en algunos casos simples, puede ayudar a entender las relaciones e influencias de unas variables en otras.

A modo de ejemplo, se presenta un fragmento de la matriz de impacto construida en el trabajo de Shi y Wu (2024) para las seis primeras variables $F1$, ..., $F6$, que se corresponden con los seis factores de riesgo, del ámbito personal, en accidentes de equipos elevadores: ($F1$) baja conciencia de seguridad, ($F2$) falta de conocimiento sobre la seguridad en ascensores, ($F3$) operación no autorizada, ($F4$) operación incorrecta, ($F5$) sin licencia para trabajar, ($F6$) medidas de protección de seguridad inadecuadas. La matriz de impacto considerada por los autores para estos seis factores y en escala de 0 a 6 es:

$$A = \begin{pmatrix} 0 & 0 & 6 & 3 & 0 & 3 \\ 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 3 \\ 0 & 0 & 5 & 0 & 0 & 2 \\ 0 & 0 & 3 & 3 & 0 & 0 \\ 0 & 0 & 2 & 5 & 0 & 0 \end{pmatrix}.$$

Esta matriz de impactos produce el grafo que se presenta en la figura 2 donde puede apreciarse cómo los factores *F*1, *F2* y *F5* solo influyen y no reciben influencia mientras que existen ciclos entre las parejas de factores *F3 – F4*, *F3 – F6* y *F4 – F6*, lo que implica una estructura de retroalimentación en la influencia. Además, se puede observar cadenas de influencia, por ejemplo, cómo la variable *F1* influye sobre *F3* de forma directa o bien de forma indirecta a través de *F4* o de *F6*.

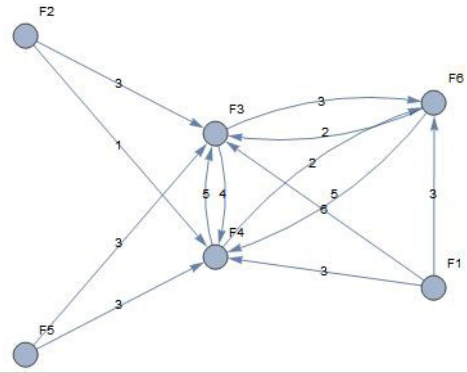


Figura 2: Gráfico causa-efecto para la matriz de impacto para los seis factores

Arcade *et al*. (1999) destacan la utilidad de este grafo, modelo de relaciones, y proponen la organización jerárquica de estos eventos o variables en forma de árbol. Para ello, es necesario eliminar cualquier ciclo que aparezca en el grafo y sugieren construir nuevas variables macro resultado de agrupar a las que forman ciclos. En nuestro caso, sería la agrupación en una única variable de los factores *F3, F4 y F6* para después formar una estructura jeraquizada con los factores *F1, F2 y F5*, en un primer nivel, y la nueva variable macro, en un segundo nivel, de modo que recibe la influencia de las anteriores.

La modelización de las relaciones entre las variables mediante el grafo asociado a la matriz de impactos permite aplicar la disciplina de la teoría de grafos sobre él, lo que puede determinar caminos de influencia indirecta, árboles de máximo impacto o máxima probabilidad, etc.

También, y de forma muy intuitiva, puede evaluarse la influencia y la dependencia de una variable o factor mediante la suma de las filas y las columnas de la matriz de impacto, esto es lo que se conoce como suma activa y suma pasiva. La primera, *suma activa*, se refiere a la suma de las influencias que cada elemento *ejerce* sobre otros elementos del sistema y corresponde con la suma de la i —ésima fila de la matriz de impacto. Mientra que la *suma pasiva* se refiere a la suma de las influencias que cada elemento *recibe* de otros elementos del sistema, dependencia y corresponde con la suma de la j —sima columna de la matriz de impacto. La interpretación de estas cantidades indica que una variable con un valor

alto de suma activa tiene un alto impacto sobre las demás variables, de la misma manera valores bajos indican bajo impacto o influencia. De forma análoga, se puede interpretar las suma pasiva, que indica un valor alto para una variable la alta dependencia de las demás variables, mientras que valores bajos indican independencia de las demás variables del sistema (Arcade *et al*., 1999).

entonces → si ocurre ↓,	F1	F2	F3	F4	F5	F6	Suma Activa	P
F1	0	0	6	3	0	3	12	0
F2	0	0	3	1	0	0	4	0
F3	0	0	0	4	0	3	7	133
F4	0	0	5	0	0	2	7	112
F5	0	0	3	3	0	0	6	0
F6	0	0	2	5	0	0	7	56
Suma pasiva	0	0	19	16	0	8		
Q	Indet.	Indet.	0,37	0,44	Indet.	0,88		

Una vez calculados los valores de suma activa (*influencia*) y suma pasiva (*dependencia*), para cada variable, pueden determinarse valores como el cociente o el producto de ambas, también para cada variable (Cole, 2006).

El cociente, valor *Q* o *índice de influencia*, de la suma activa entre la suma pasiva permite identificar a la variable más activa, la de mayor valor *Q*, que tiene el mayor impacto sobre las demás variables frente a la variable más pasiva, la de menor valor *Q*, que depende más de las demás variables. Las variables más activas son las que más influyen en el sistema y su control tendrá un importante impacto en el comportamiento del sistema. Las variables con suma pasiva cero producen una indeterminación a la hora de calcular el valor *Q*, estas variables no reciben influencia, son independientes y solo influyen sobre las demás.

El producto, valor P o *índice de centralidad*, de la suma activa por la suma pasiva da una medida de la importancia de una variable, valores P altos indican variables altamente influyentes y altamente dependientes, suelen denominarse variables críticas. Variables con valores P bajos son variables que influyen y dependen poco por lo que suelen denominarse inertes.

5 Gráfico de Influencia x Dependencia

Para obtener una visión global del sistema estudiado se puede construir el gráfico de influencia x dependencia en el que se representan las variables y la fuerza de sus relaciones (Arcade *et al*., 1999). El gráfico se forma representando en un diagrama de dispersión la suma pasiva (dependencia), eje x, frente a la suma activa (influencia), eje y. La figura 3 presenta el gráfico de dependencia x influencia para los seis factores del ejemplo.

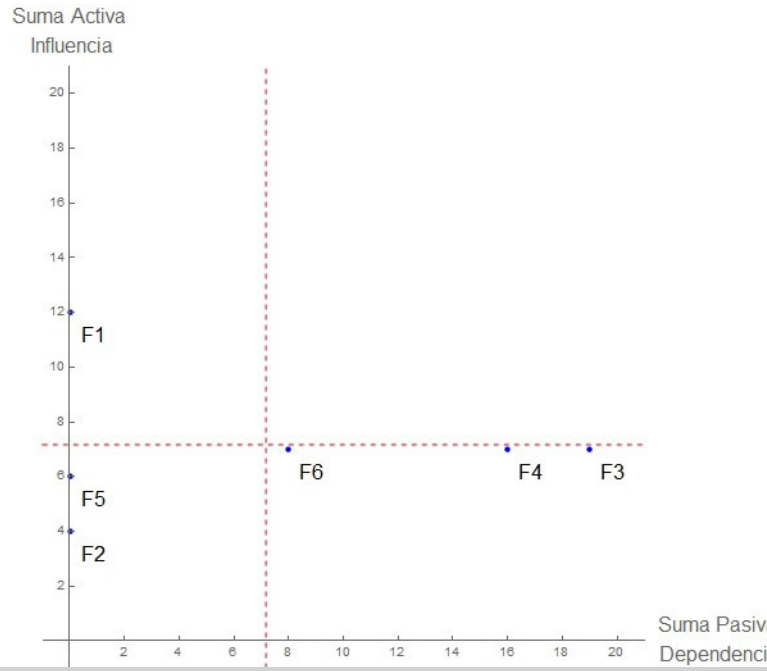


Figura 3: Gráfico de dispersión de Dependencia × Influencia para los seis factores del ejemplo

El centro de gravedad del gráfico divide la nube de puntos en cuatro cuadrantes y las variables o factores presentes en cada cuadrante suelen clasificarse según sus valores de influencia y dependencia, respectivamente. Hay varias formas de referirse a cada tipo de variable que puede representarse en el gráfico de dispersión y habitualmente se mencionan al menos cinco tipos de variables, una por cada cuadrante, más variables que ocupan el centro de gravedad del gráfico (Arcade *et al*., 1999; Asan, Erhan Bozdağ, y Polat, 2004; Linss y Fried, 2010).

El centro de gravedad del gráfico viene dado por el valor de dependencia media y de influencia media, alrededor de él se agrupan las llamadas variables **reguladoras**, que suelen determinar el funcionamiento del sistema en condiciones normales, también se pueden encontrar autores que las denominan variables **neutras** (figura 4).

Las variables con altos valores de dependencia e influencia (suma pasiva y suma activa) ocupan posiciones en el primer cuadrante y suelen denominarse **críticas**, **clave** o **reto**. Estas variables son fuente de inestabilidad en el sistema debido a sus altos valores de influencia y dependencia. Las variables **clave** o **reto** se sitúan por encima de la diagonal y suelen considerarse las más importantes en el sistema. También, por debajo de ellas, en este primer cuadrante, con valores de dependencia mayores al de

influencia aparecen las variables **objetivo**, su mayor grado de dependencia las hacen muy atractivas para poder influir sobre ellas.

En el segundo cuadrante, se encuentran las variables que presentan valores altos de influencia y bajos de dependencia, estas variables se conocen habitualmente como **influyentes** o de **entrada**. Estas variables actúan como un factor de inercia en el sistema, influyen sobre él y el control sobre ellas suele ser limitado. En la parte izquierda del cuadrante, la literatura suele situar a las variables de **entorno**, estas variables actúan como contexto del sistema.

Las variables con baja influencia y dependencia se sitúan en el tercer cuadrante, y suelen llamarse variables **inertes**, **autónomas** o **excluidas**. Algunos autores distinguen entre ellas a las variables **desconectadas**, colocadas cerca del origen de coordenadas con valores muy bajos, tanto de influencia como de dependencia, y a las **palancas secundarias**, con valores más altos de influencia que de dependencia. Estas últimas están relacionadas con las variables reguladoras, pero en un segundo nivel, actúan como palancas en el sistema por su grado de influencia, pero con menor importancia que éstas.

Por último, en el cuarto cuadrante se encuentran las variables **dependientes** que resultan ser muy sensibles por la influencia de las variables influyentes o críticas. Entre ellas, se distinguen a las variables **resultado** con dependencia más elevada, variables que suelen ser de interés en el sistema y sobre las que no se puede actuar directamente, sino a través de las variables que influyen en el sistema.

Figura 4: Gráfico de dispersión Dependencia Influencia con los tipos de variables según su interpretación

Esta metodología puede aplicarse para cualquier tipo de matriz de impacto como las que se ha presentado, cualitativas, de escala o en términos de probabilidades condicionadas, sin embargo, la clasificación de las variables no es única y existen en la literatura otras clasificaciones en función de la influencia (suma activa) y la dependencia (suma pasiva).

6 Multiplicación de la Matriz de Impactos Cruzados Aplicada a la Clasificación (Matrice d'Impacts Croisés Multiplication Appliquée à une Classification-MICMAC)

En algunas aplicaciones de la metodología de impactos cruzados, además de utilizar los conceptos de dependencia e influencia, se utiliza la multiplicación de la matriz de impactos propuesta por Godet (1986) para clasificar las variables del sistema.

El método MICMAC de potencias de matrices de impacto se basa en una de las propiedades de las matrices de impacto cualitativas en las que los elementos $a_{ij} = 1$ indican influencia directa de la variable i –ésima en la variable j –ésima, mientras que $a_{ij} = 0$ indican ausencia de influencia. Estas matrices solo muestran el impacto directo entre las parejas de variables del sistema, quedando sin tener en cuenta influencias indirectas a través de cadenas de variables. Las matrices de impacto booleanas tienen la propiedad que elevadas a la potencia n dan, en A^n, el número de cadenas de longitud n que van del vertice i –ésimo al vértice j –ésimo, a_{ij}^n (figura 5).

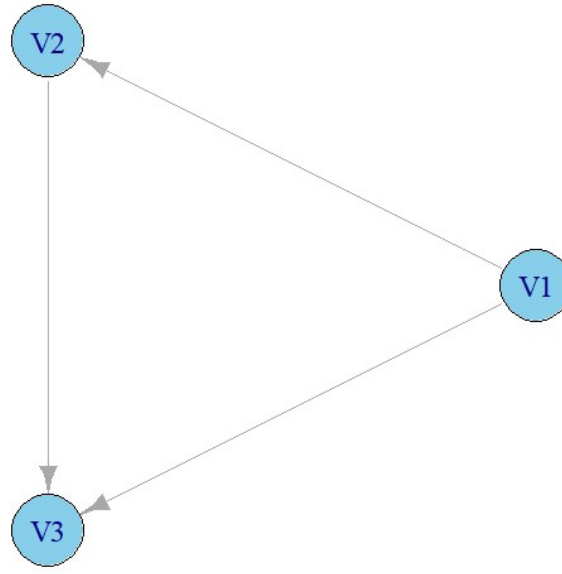


Figura 5: Grafo con tres vértices y tres aristas, sin peso

El grafo de tres vértices representado en la la figura 5 tiene asociada la matriz booleana A:

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Con tres aristas, dos de ellas saliendo del $V1$ y llegando a $V2$ y $V3$, respectivamente, y otra saliendo de $V2$ hacia $V3$.

Se eleva la matriz al cuadrado A^2, tal que los elementos a_{ij}^2 se calculan sumando los productos de la fila i –ésima por la fila j –ésima, $a_{ij}^2 = \sum_k a_{ik} \cdot a_{kj}$ se tiene que cada término $a_{ik} \cdot a_{kj}$ de la suma es 1 si existe una arista del vértice i al vértice k y otra del vértice k al vértice i. Por lo tanto, $a_{ik} \cdot a_{kj} = 1$ indica que existe un camino de longitud 2 desde i hasta j y pasa por k. Al sumar todos estos productos, para todos los posibles vértices k, se obtiene el número total de caminos de longitud 2 desde i hasta j. De esta manera, se tiene que el elemento a_{ij}^2 de A^2 da el número de caminos o, en este caso, cadenas de influencia o impacto, de longitud 2 que van del vértice i al vértice j. En el caso de la figura 5, es inmediato ver que existe un único camino de longitud 2 que une los vértices $V1$ y $V3$.

$$A^2 = A \cdot A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Este resultado se generaliza en el caso de matrices booleanas (cualitativas, en las que solo se utiliza 1 o 0 para definir impacto o ausencia de este), diciendo que la matriz A^n contiene en a_{ij}^n el número de cadenas de longitud n y describe así el impacto indirecto a través de $n-1$ variables de la variable i sobre la variable j. Un caso especial es el reflejado por los elementos de la diagonal de la matriz elevada, a_{ii}^n, que presenta el número de circuitos o ciclos que, al salir de la variable i, vuelven a impactar sobre ella.

En el caso en el que la matriz A sea una matriz de impacto expresada en escala o en probabilidades condicionadas, se tiene que la interpretación de sus potencias ya no es inmediata. El elemento a_{ij}^n es, en este caso, la suma de los productos de todos los pesos o impactos de todas las cadenas de influencia de longintud n que van desde la variable i a la variable j. También, por lo tanto, una medida, al menos relativa, de la influencia de la variable i en la variable j a través de cadenas de longitud n.

La idea de Godet (1986) incluye analizar las relaciones indirectas entre las variables del sistema y estudiar la difusión de los impactos a través de cadenas y ciclos en los que las variables intermedias expresan su influencia.

De esta manera, el método MICMAC busca clasificar las variables del sistema de acuerdo con la dependencia e influencia, teniendo en cuenta no solo relaciones directas entre las parejas de variables, sino todas las cadenas de relaciones expresadas en el grafo y la matriz de impacto.

La propuesta en el método MICMAC se basa primero en la *clasificación* de dependencia e influencia *directa* entre las parejas de variables del sistema. La variable con mayor suma activa (suma de las filas de A) ocupará la posición 1.ª en la clasificación de influencia, de modo que ocupará la posición 2.ª y sucesivas la siguientes en orden descendiente de suma activa. De la misma manera, se define la clasificación de dependencia basada en la suma pasiva (suma de las columnas de A). La posición 1.ª en esta clasificación será ocupada por la variable de mayor suma pasiva y en orden descendiente se complementaría la clasificación. De esta manera, se identifica, en esta clasificación, qué variables son más influyentes y qué variables son más dependientes en cuanto relaciones directas.

Esta misma clasificación puede obtenerse para relaciones *indirectas*, tanto de dependencia como de influencia. Al clasificar en orden la suma activa y suma pasiva de la matriz elevada al cuadrado, A^2, se obtiene la clasificación de dependencia e influencias indirectas a través de una tercera variable intermedia. El orden de la clasificación puede verse alterado, lo que revela variables *escondidas* que aumentan su influencia en el sistema a través de cadenas orden dos, es decir, influyen de forma indirecta a través de otra variable.

Repitiendo esta estrategia, pueden obtenerse sucesivas clasificaciones de las variables del sistema, tanto para dependencia como para influencia, A^2, A^3, A^4... El método busca obtener una estabilidad en estas clasificaciones tal que las clasificaciones no se vean alteradas a partir de una potencia, k, de la matriz de impacto.

La evolución de estas clasificaciones puede mostrarse bien en el gráfico de influencia x dependencia o bien en una tabla, de modo que se comparen las clasificaciones directas, obtenidas a partir de A, con las indirectas, obtenidas a partir de A^k. Es muy interesante comparar y analizar las variables que no son dependientes o influyentes de forma *directa* y sí de forma *indirecta*.

Esta propiedad de estabilidad en la clasificación es conjeturada por Godet (1986) y viene utilizándose desde entonces en la aplicación del método MICMAC, sin embargo, existen estudios que demuestran que no siempre se alcanza una estabilidad en las clasificaciones de dependencia e influencia de las potencias de la matriz de impacto. Jodlbauer *et al*. (2022) concluyen que, cuando la matriz de impacto A contiene un alto porcentaje de elementos nulos, del orden del 75% o más de los elementos de A, es

posible encontrar matrices que no alcancen la estabilidad en las clasificaciones de dependencia o influencia. También estas matrices llamadas «huecas», suelen presentar mayores diferencias entre las clasificaciones directas y las indirectas.

A modo de ejemplo, se presenta un fragmento de la matriz de impacto propuesta por Nazlabadi *et al*. (2023) en su trabajo sobre la gestión del agua y de aguas residuales. El fragmento que se presenta en este ejemplo coincide con las seis primeras variables $V1, \ldots, V6$ y la clasificación de dependencia e influencia de la matriz de impacto inicial viene dada por:

A	V1	V2	V3	V4	V5	V6	Suma Activa	Clasificación Influencia
V1	0	3	2	3	3	2	13	1°
V2	2	0	1	2	3	2	10	2°
V3	2	2	0	1	2	3	10	2°
V4	2	2	2	0	2	2	10	2°
V5	1	3	1	2	0	2	9	3°
V6	1	2	3	2	0	0	8	4°
Suma Pasiva	8	12	9	10	10	11		
Clasif. Dependencia	5°	1°	4°	3°	3°	2°		

En este pequeño ejemplo, la estabilidad se logra en el estudio de las cadenas de influencia de longitud dos, es decir A^2. Para esta clasificación indirecta, gana relevancia en cuanto a influencia la variable $V4$ y se deshace el empate en cuanto a dependencia de las variables $V4$ y $V5$. Las potencias superiores a 2 de la matriz de impacto producen las mismas clasificaciones.

7 Conclusión

En este trabajo, se ha presentado una descripción metodológica de las herramientas básicas en la construcción de modelos basados en el método estructural y la matriz de impacto cruzados aplicados a la construcción de escenarios futuros. Como se ha visto, estas herramientas surgen de un *juego*, como muchas otras herramientas usadas en el ámbito de las ciencias aplicadas. La complejidad de la realidad implica realizar simplificaciones sobre ella antes de poder utilizar técnicas de modelización conceptuales, físicas, matemáticas o estocásticas. La aplicación de estas técnicas en pequeños juegos es la base de las *investigaciones fundamentales*, abstractas, sin aplicación real inmediata pero que en muchas ocasiones son el germen de nuevas ideas, desarrollos, que, con la ayuda inestimable de los avances tecnológicos, pueden generalizarse y aplicarse poco a poco en la tarea de resolver problemas reales.

Hoy en día, los métodos de los que se ha hablado se aplican con éxito en la modelización de la realidad en ámbitos muy diferentes, combinados con otras técnicas y buscando tomar decisiones que produzcan beneficios permitiendo anticiparse al futuro o pudiendo influir sobre él.

A modo de ejemplos, se puede mencionar de forma muy breve algunos trabajos donde el lector interesado en estas técnicas pueda encontrar detalles, herramientas e inspiración sobre cómo aplicar esta metodología en su problema.

Chatziioannou *et al*. (2023) presentan un trabajo en el que crean una clasificación de los indicadores de movilidad urbana y su relación con políticas de transporte con objeto de mejorar la habitabilidad de las ciudades. El trabajo realiza un estudio cualitativo en la legislación y la literatura, pero lo más destacable es la síntesis de la experiencia de veintiocho expertos en desarrollo urbanístico que permiten relacionar indicadores clave de movilidad con políticas de transporte efectivas. En las conclusiones, los autores proponen combinar, en trabajos futuros, el análisis estructural con estudios cuantitativos.

Chen *et al*. (2025) realizan una modelización estructural de la cadena de suministro circular (CSMC). El estudio tiene como objetivo identificar, analizar y clasificar los factores determinantes que afectan la implementación de CSCM en el sector logístico de Corea del Sur. En este caso, se trabaja con un panel de seis expertos y se identifica la importancia que tienen las regulaciones gubernamentales y los incentivos financieros en la adopción de estos modelos de gestión.

El estudio de las barreras o dificultades que presenta el uso de drones en la agricultura se ha enfocado con una estrategia híbrida que combina diferentes métodos para la toma de decisiones como el método DEMATEL (Decision Making Trial and Evaluation Laboratory) aplicado con medidas de incertidumbre basadas en lógica difusa, el método estructural y el método MICMAC (Singh, Sharma y Adhikari, 2024).

Para terminar, me gustaría mencionar una línea metodológica que permite la incorporación de la evolución temporal sobre el sistema a analizar. En el caso de Serdar Asan y Asan (2007), incorporan esta dependencia mediante la construcción de una matriz de tiempo y utilizan algoritmos propios de la teoría de grafos para encontrar caminos mínimos. De forma parecida, el trabajo de Nazlabadi *et al*. (2023) presenta un análisis estructural para determinar las variables determinantes y su influencia en la gestión del agua en entornos urbanos, de modo que considera la influencia del tiempo en el sistema y propone una variación metodológica que denominan MICMAC-T.

Bibliografía

Arcade, J., Godet, M., Meunier, F. y Roubelat, F. (1999). *Structural Analysis with the MICMAC Method*. American Council for the United Nations University, The Millennium Project.

Asan, U., Erhan Bozdağ, C. y Polat, S. (2004). A Fuzzy Approach to Qualitative Cross Impact Analysis. *Omega*. 32(6), pp. 443-458. DOI: https://doi.org/10.1016/j.omega.2004.02.006

Chao, K. (2008). A new look at the cross-impact matrix and its application in futures studies. *Journal of Futures Studies*. 12(4), pp. 45-52.

Chatziioannou, I., Nikitas, A., Tzouras, P. G., Bakogiannis, E., Alvarez-Icaza, L., Chias-Becerril, L., Karolemeas, C., Tsigdinos, S., Wallgren, P. y Rexfelt, O. (2023). Ranking sustainable urban mobility indicators and their matching transport policies to support liveable city Futures: A MICMAC approach. *Transportation Research Interdisciplinary Perspectives*. 18, p. 100788. DOI: https://doi.org/10.1016/j.trip.2023.100788

Chen, J. R., Bang, S. H., Ha, M. H., Shin, K. S. y Seo, Y. J. (2025). A Structural Analysis of the Influential Factors Affecting the Implementation of Circular Supply Chain Management in South Korea. *Journal of Cleaner Production* 494, p. 145005. DOI: https://doi.org/10.1016/j.jclepro.2025.145005

Cole, A. (2006). *The Influence Matrix Methodology: A Technical Report*. Palmerston North, Landcare Research New Zealand Ltd.

Godet, M. (1974). Méthode de hiérarchisation des variables et de construction de scénarios. *Metra*. XIII(4), pp. 455-478.

Godet, M. (1986). Introduction to la prospective. *Futures*. 18(2), pp. 134-157. DOI: https://doi.org/10.1016/0016-3287(86)90094-7

Godet, M. y Duperrin, J. C. (1975). SMIC 74: A Method for Constructing and Ranking Scenarios. *Futures*. 7(4), pp. 302-312. DOI: https://doi.org/10.1016/0016-3287(75)90048-8

Gordon, T. J. (1994). *Cross Impact Analysis*. United Nations Development Program's African Futures Project in collaboration with the United Nations University's Millennium Project Feasibility Study.

Gordon, T. J. y Hayward, H. (1968). Initial Experiments with the Cross Impact Matrix Method of Forecasting. *Futures*. 1(2), pp. 100-116. DOI: https://doi.org/10.1016/S0016-3287(68)80003-5

Gordon, T. J. y Helmer-Hirschberg, O. (1964). *Report on a Long-Range Forecasting Study*. Santa Monica, RAND Corporation.

Jodlbauer, H., Tripathi, S., Brunner, M. y Bachmann, N. (2022). Stability of Cross Impact Matrices. *Technological Forecasting and Social Change*. 182, p. 121822. DOI: https://doi.org/10.1016/j.techfore.2022.121822

Kahn, H. y Wiener, A. (1967). *The Year 2000: A Framework for Speculation on the Next Thirty-Three Years*. Washington, D.C., The Hudson Institute.

Linss, V. y Fried, A. (2010). The ADVIAN® Classification A New Classification Approach for the Rating of Impact Factors. *Technological Forecasting and Social Change*. 77(1), pp. 110-119. DIO: https://doi.org/10.1016/j.techfore.2009.05.002

McLean, M. (1976). Does cross-impact analysis have a future? *Futures*. 8(4), pp. 345-349. DOI: https://doi.org/10.1016/0016-3287(76)90130-0

Menéndez Velázquez, A. (1998). Una breve introducción a la teoría de grafos. *Suma: Revista sobre Enseñanza y Aprendizaje de las Matemáticas*. 28, pp. 11-26.

Mitchell, R. B. y Tydeman, J. (1976). A Note on SMIC 74. *Futures*. 8(1), 64-67. DOI: https://doi.org/10.1016/0016-3287(76)90097-5

Nazlabadi, E., Maknoon, R., Alavi Moghaddam, M. R. y Daigger, G. T. (2023). A novel MICMAC approach for cross impact analysis with application to urban water/wastewater management. *Expert Systems with Applications*. 230, p. 120667. DOI: https://doi.org/10.1016/j.eswa.2023.120667

Serdar Asan, S. y Asan, U. (2007). Qualitative Cross-Impact Analysis with Time Consideration. *Technological Forecasting and Social Change*. 74(5), pp. 627-644. DOI: https://doi.org/10.1016/j.techfore.2006.05.011

Shi, F. y Wu, Z. (2024). Construction of Knowledge Graph of the Elevator Safety Accidents and Analysis of Key Risk Factors Based on KG-DEMATEL-ISM-MICMAC Method. *IEEE Access*. 12, pp. 43615-43631. DOI: https://doi.org/10.1109/access.2024.3375879

Singh, S. Pal., Sharma, A. y Adhikari, A. (2024). Investigating the Barriers to Drone Implementation in Sustainable Agriculture: A Hybrid Fuzzy-DEMATEL-MMDE-ISM-Based Approach. *Journal of Environmental Management*. 371, p. 123299. DOI: https://doi.org/10.1016/j.jenvman.2024.123299

La tecnología al servicio de la disuasión

Emilia José Peña Ruiz

Resumen

Hoy más que nunca, el régimen de no proliferación se encuentra tensionado por los diferentes conflictos que transcurren y por el desafío de algunos países proliferantes cuyas actividades nucleares parecen alejarse del curso pacífico. Es por esto por lo que las actividades de monitorización necesitan de herramientas que den valor añadido y que puedan sobreponerse a las actividades de decepción. Las imágenes satélite y su análisis se han consolidado como una herramienta pilar en las actividades de verificación del OIEA y su sistema de salvaguardias, a pesar de los intentos de reducir su eficacia y enterrar las instalaciones o recubriendo con edificios las partes más vitales.

Palabras clave

Satélite, Inteligencia, Proliferación, Salvaguardias, Nuclear.

Technology for deterrence

Abstract

Today more than ever, the non-proliferation regime is under stress due to various conflicts that are taking place and the challenge of certain proliferating countries whose nuclear activities seem to be moving away from a peaceful course. For this reason, monitoring activities need value-added tools that can overcome deception activities. Satellite images and their analysis have established themselves as a mainstay tool in the IAEA's verification activities and its safeguards system, despite attempts to reduce their effectiveness by burying or covering the most facilities' vital parts.

Keywords

Satellite, intelligence, proliferation, safeguards, nuclear.

1 Introducción

La disuasión nuclear se refiere a un principio de las relaciones internacionales que trata de evitar un ataque nuclear basado en el potencial mismo de las armas nucleares. Todo el mundo podría convenir en la capacidad de destrucción de este armamento, sobre todo, teniendo en cuenta los efectos destructivos de *Little Boy* y *Fat Man* sobre Hiroshima y Nagasaki. Sin embargo, paradójicamente, siempre han existido dudas sobre su eficacia y eficiencia en el ámbito de la disuasión.

Desde el punto de vista militar, el resultado fue decisivo al provocar la derrota de Japón, pero, al mismo tiempo, se desveló su vertiente estratégica y su capacidad de proyección de fuerza. Las explosiones nucleares de Hiroshima y Nagasaki determinaron la capitulación japonesa el 2 de septiembre de 1945, iniciándose una nueva etapa histórica de la humanidad conocida como la Era Atómica (Calduch, 1991: 6).

En ese momento, solo Estados Unidos corría la carrera armamentística, lo que le situaba en un escalón por encima del resto de adversarios, ya que lideraba el monopolio nuclear. Situación que estaba condenada a desaparecer, precisamente, porque el resto de adversarios no iban a permanecer durante mucho tiempo en esa situación de desventaja tanto militar como estratégica. Esto propició la carrera armamentística entre Estados como Rusia, Francia, China o Reino Unido.

Esos cinco países terminaron por ser los Estados nucleares *de iure*, pero también existen Estados que han logrado ese estatus nuclear *de facto,* como Corea del Norte, la India, Israel o Pakistán y han puesto a prueba su capacidad armamentística, de modo que han llevado a cabo numerosos ensayos nucleares como muestra de su potencial militar.

En 1958, Thomas K. Finletter, quinto embajador de Estados Unidos para la OTAN dijo que «el desarme estaba a la orden del día». Sesenta y siete años después, la situación está girando hacia los 180 grados y el club de países nucleares corre el riesgo de incrementarse con más miembros. Además de la seria candidatura que se le adjudica a Irán para ser uno de los primeros Estados en destaparse como un país nuclear de facto, ya se asume como algo más que una intención la anunciada por Arabia Saudí y la ya histórica y conocida, aunque paralizada, aspiración turca.

El régimen de no proliferación nuclear basado durante 45 años en el Tratado de No Proliferación de armas nucleares (TNP) se enfrenta en la actualidad a importantes desafíos encabezados, sin duda, por el desarrollo de capacidades nucleares poco claras y muy significativas por el Gobierno iraní. Por otra parte, las necesidades energéticas mundiales y los problemas de abastecimiento a futuro han dado lugar a la consolidación de proyectos que hace años solo eran ideas o aspiraciones y donde la energía nuclear es

la respuesta a necesidades energéticas, lo que ha supuesto un salto cualitativo y cuantitativo en el desarrollo de esta tecnología de forma global.

Dado el carácter dual civil y militar de la tecnología nuclear, este proceso es un reto importante para la comunidad internacional, que debe perseverar en el mantenimiento de un equilibrio entre el progreso técnico y económico y la estabilidad mundial en el marco del TNP (Salazar, 2015).

Como se ve, la arquitectura internacional del régimen de no proliferación y desarme está cada vez más cuestionada y presionada, en un entorno de seguridad que, además, no le favorece. La agresión de Rusia sobre Ucrania que comenzó en el año 2022 y ya ha cumplido su tercer año, no ha hecho más que favorecer la corrosión de los ya oxidados anclajes de las iniciativas de desarme y, por ende, del Tratado de No Proliferación, su piedra angular.

Sergei Karaganov, uno de los arquitectos intelectuales de la política exterior rusa y director del muy influyente Consejo de Política Exterior y de Defensa, figura clave del pensamiento estratégico ruso y partidario del uso de armas nucleares en el actual conflicto con Ucrania, lo explica de forma espléndida y en pocas palabras. «El eslogan de hace medio siglo —La guerra nuclear nunca debe desatarse, porque no puede haber vencedores— es magnífico, pero también idealista. Como ha demostrado el conflicto de Ucrania, abre la puerta a grandes guerras convencionales. Y estas guerras pueden ser y serán cada vez más frecuentes y mortíferas, sin dejar de estar al alcance de la mano, a menos que se las contrarreste con una política activa de paz» (Laruelle, 2024).

Sin embargo, el marco geopolítico actual, como se ha visto no está en esa línea. Es cierto que, actualmente, no hay veinticinco potencias nucleares en el mundo como pronosticó la administración del presidente estadounidense John F Kennedy en 1960, pero no hay intenciones de apostar por el desarme. Al contrario, la competición y la desconfianza entre Estados están más vivas que nunca y pueden detectarse en el gasto militar y en los diferentes usos de la inteligencia artificial. Los Estados buscan mantener su seguridad y su supervivencia y esta propensión de ciertos países a «adquirir más y más poder con el fin de escapar del impacto del poder de los otros» fue interpretada también por John Herz en el concepto dilema de seguridad, refiriéndose a la propensión de ciertos países a caer en una espiral viciosa armamentística mutua que conduce de manera inexorable a la paradoja de la seguridad (Wheeler, 2007: 27).

Para poder frenar una carrera armamentística, se necesita un ecosistema geopolítico bipolar estable y, sin embargo, el ecosistema geopolítico que nos envuelve es multipolar e inestable donde, además, las nuevas tecnologías han ayudado a evolucionar los arsenales militares y las armas nucleares parecen haber recuperado su cuota de protagonismo, ya sea como

elementos coercitivos o disuasorios, lo que ha alentado una nueva carrera armamentística (Cartagena y Garrido, 2024).

Debido a este trasfondo, el concepto de proliferación horizontal ha emergido de nuevo a la actualidad. Este fenómeno, que tuvo su origen durante el periodo de la Guerra Fría, consiste en el aumento del número de Estados con capacidad nuclear militar y, actualmente, ha experimentado una evolución importante como consecuencia del cambio de circunstancias internacionales desarrollada en tres ejes fundamentales. Primero, en el aumento del poder destructivo de las armas nucleares. En segundo lugar, en las nuevas características sociopolíticas y económicas que presentan los Estados proliferadores pos Guerra Fría. Y, en tercer lugar, en el aumento de los riesgos que implican las armas nucleares para la paz y la seguridad internacional (Marrero Rocha, 2002).

Los riesgos que vierte la proliferación nuclear horizontal en la seguridad internacional son tan evidentes que se puede apreciar rápido su nexo con el sistema de salvaguardias y las actividades de monitorización que el OIEA lleva realizando durante casi setenta años con el objetivo de evitar la proliferación de armas nucleares y proporcionar garantías creíbles de que la obligación jurídica de los Estados, de utilizar la tecnología nuclear solo con fines pacíficos, se cumple.

El mantenimiento de un régimen de salvaguardias sigue siendo esencial, pero debe contar con el apoyo y el compromiso de todas las partes interesadas. Al mismo tiempo, este sistema debe apoyarse en un marco jurídico sólido, pero también, debe ir acompañado de los últimos avances e innovaciones científicas que aporten más firmeza al sistema de verificación para que no existan grietas que den lugar a nuevos programas nucleares sin detectar o para confirmar que esta tecnología se utiliza con fines exclusivamente pacíficos. Sobre todo, en un momento geopolítico difícil que demuestra la necesidad de renovar el compromiso con el principio de no proliferación (VV. AA., 2015: 2).

1.1 La necesidad de un sistema de salvaguardias

El OIEA ofrece una definición muy sencilla de las salvaguardias. Un conjunto de medidas técnicas que aplica el Organismo a las instalaciones y materiales nucleares. Se trata de verificar de forma independiente que las instalaciones nucleares de un Estado parte se utilizan de forma debida y el material nuclear no se desorienta hacia fines que no sean pacíficos, por medio de estas pautas técnicas. Estas medidas incluyen compromisos políticos, tratados multilaterales, así como otros acuerdos jurídicamente vinculantes en los que se inscriben los compromisos de no proliferación y, sobre todo, las salvaguardias del OIEA. Los Estados aceptan estas medidas

mediante la concertación de sus respectivos acuerdos de salvaguardias, por lo que terminan siendo obligaciones jurídicas que ellos mismos se comprometen a cumplir (IAEA, s. f.).

El mecanismo de las salvaguardias es homólogo a cualquier otro proceso de examen donde el último objetivo es que los procedimientos fomenten la confianza en la conducta de los Estados. Esto exige que los explotadores de instalaciones nucleares mantengan y declaren registros contables detallados de todos los movimientos y transacciones relacionados con materiales nucleares, lo que se traduce en que el Organismo monitoriza casi novecientas instalaciones nucleares y varios centenares de otros lugares en 57 países mediante inspecciones periódicas. Los registros y auditorías se complementan con otras medidas como cámaras de vigilancia e instrumentación remota (World Nuclear Association, 2021).

El OIEA lleva, desde 1970, realizando inspecciones periódicas de las instalaciones nucleares, así como auditando el movimiento de materiales nucleares. Es por esto por lo que se puede afirmar que durante más de cincuenta años el Organismo ha impedido con éxito la diversificación de material fisionable para convertirlo en armas y ha alertado en múltiples ocasiones de actividades nucleares no declaradas.

La mayoría de los acuerdos de salvaguardias se han alcanzado con Estados no nucleares (NNWS) que, al mismo tiempo, son parte del TNP y se han comprometido a no desarrollar o adquirir armas nucleares. Sin embargo, curiosamente, dentro de la Unión Europea este sistema difiere.

El capítulo VII del Tratado de EURATOM, firmado en Roma el 27 de marzo de 1957, estableció su propio sistema de control de los materiales nucleares[1]. Aunque en la práctica sea equivalente a un sistema de salvaguardias, no es un sistema de no proliferación de armas nucleares. Esto es así debido a que sus disposiciones no impiden el uso militar del material nuclear, solo es de obligado cumplimiento el declarar sobre el uso de este).

La entrada en vigor del TNP dentro de la Unión Europea (por entonces, la Comunidad Económica Europea) obligó a aplicar en paralelo los regímenes de salvaguardias de la Comunidad EURATOM y del OIEA. Para evitar duplicidad en las actividades de control y asegurar un uso racional de esfuerzos y recursos, los Estados miembros hicieron constar la condición de que los acuerdos de salvaguardias que se concertaran con el OIEA, *a posteriori* el Acuerdo recogido en el INFCIRC/193, tendría un ámbito de aplicación análogo al modelo marco del Organismo para la aplicación coordinada del sistema de salvaguardias, el documento INFCIRC/153.

[1] Las disposiciones del Capítulo VII del Tratado se desarrollan en el Reglamento Euratom 302/2005.

La aplicación de las salvaguardias sigue un ciclo anual y comprende cuatro procesos principales. La recopilación y evaluación de información pertinente para la aplicación de las salvaguardias; la elaboración de un enfoque concreto de salvaguardias para un determinado Estado destinadas a conseguir los objetivos de verificación establecidos; planificar, realizar y evaluar esas actividades diseñadas, ya sean sobre el terreno o de forma remota en la sede del Organismo para alcanzar los propósitos identificados y, por último, elaborar las conclusiones obtenidas basadas, obviamente, en el grado de cumplimiento (IAEA, s. f.).

Es de sobra evidente que la tecnología avanza y evoluciona de forma continua, lo que afecta a cualquier ámbito y, por tanto, a la esfera nuclear. El material y el número de instalaciones sometidas a Salvaguardias del Organismo crece de forma constante, lo que se ha traducido en quince nuevos acuerdos de salvaguardias en los quince últimos años treinta nuevos protocolos adicionales.

Las salvaguardias del OIEA tendrán que seguir evolucionando, precisamente, por la necesidad de introducir más mejoras y optimizar los procesos de garantía que dan lugar a unas salvaguardias creíbles. Es vital poder dar respuestas eficaces a rápidas a nuevas demandas de verificación y aplicar la tecnología más evolucionada. Tanto para el Organismo como para la sociedad global es necesario estar al tanto de posibles desarrollos fuera de los límites marcados por las salvaguardias.

Aunque el factor más importante del régimen de salvaguardias sea la presión internacional que se realiza para disuadir a un Estado de su intención de desarrollar un programa de armas nucleares, en ocasiones, la solución más eficaz a la proliferación es más política que técnica. Sin embargo, el mayor riesgo siempre recaerá en dos clases de Estados. Los países que no se han adherido al TNP y tienen importantes actividades nucleares no sometidas a salvaguardias, y los que sí se han adherido, pero hacen caso omiso de los compromisos contraídos en virtud de los tratados (World Nuclear Association, 2021).

Dentro de esta tesitura, se encuentran los casos de Irak, Irán y Corea del Norte, que ilustran tanto las fortalezas como las debilidades del sistema de salvaguardias internacionales. Irak e Irán aceptaron un sistema de salvaguardias en sus instalaciones declaradas y, al mismo tiempo, establecieron instalaciones y equipos en otros lugares no declarados en un intento de enriquecer uranio fuera de los límites marcados por el Organismo.

Corea del Norte utilizó reactores de investigación y desarrolló una planta de reprocesamiento para producir plutonio apto para armas, antes de que decidiera retirarse del TNP en el año 2003. Aunque, por fortuna, esas actividades fueron detectadas, actualmente Corea del Norte representa el mayor desafío al que se enfrenta el OIEA.

Por tanto, aunque el sistema de salvaguardias encierre un conjunto de actividades complejas que tengan como objetivo garantizar el uso pacífico de los desarrollos nucleares, este sistema de control requiere de herramientas de apoyo para monitorizar y analizar esas evoluciones técnicas. Los sistemas de información geográfica aportan un apoyo para la verificación más importante de lo que a priori puede pensarse.

1.2 Cómo participan los sistemas de información geográfica en el sistema de salvaguardias

El primer paso de la verificación es la información que aportan los Estados miembros al OIEA. Sin embargo, como se ha dicho ya, existen casos de Estados proliferantes fuera del Organismo, por lo que se necesitan herramientas en las que apoyar las tareas de verificación ajenas a los Estados implicados. En 1998, el OIEA promovió una investigación sobre la viabilidad y rentabilidad del uso de imágenes de satélite comerciales como medio de apoyo a la aplicación de las salvaguardias. Los resultados confirmaron que la alta resolución de las imágenes representaba una fuente de información más que significativa no solo para el seguimiento de las actividades nucleares, sino para la verificación de emplazamientos (Poucet, Contini y Bellezza, 2002).

El OIEA obliga a todos los Estados con instalaciones de enriquecimiento a supervisar todos los materiales fisibles conforme a ciertos protocolos y en caso de incoherencias o insuficiencia de datos, el Organismo realiza peticiones adicionales[2]. Esta información se divide en tres modelos interconectados: topológico, funcional y operativo. El modelo topológico comprende todos los datos referenciados geográficamente representados, es decir, la localización del emplazamiento. En relación con el emplazamiento, se consideran varios mapas temáticos, por ejemplo, el mapa *raster* de disposición del emplazamiento, los límites de las instalaciones y las plantas relacionadas, las áreas de balance de materiales (áreas en las que se manipula el material nuclear), la ubicación de los puntos clave de medición asociados (puntos clave en los que se mide el material nuclear), la disposición de los

[2] Todos los Estados-No-Nuclearmente-Armados Partes en el TNP, así como los Estados Parte en los Tratados Sobre Zonas Libres de Armas Nucleares Regionales (ZLAN Tratados), están obligados a celebrar Acuerdos de Salvaguardias Amplias (CSA) con el OIEA. Tales acuerdos se celebran sobre la base del documento INFCIRC / 153 (Corregido). El Estado se compromete a aceptar las salvaguardias del OIEA en todos los materiales nucleares en todas las actividades nucleares con fines pacíficos en su territorio, bajo su jurisdicción o efectuadas bajo su control en cualquier lugar. Bajo estos acuerdos, el OIEA tiene el derecho y la obligación de garantizar que las salvaguardias se aplican en todo el material nuclear de esta índole con la exclusiva finalidad de verificar que dichos materiales no se desvían hacia armas nucleares u otros artefactos explosivos nucleares. [sic] Traducción propia. Para consultar texto original ver: Circular Informativa OIEA, INFCIRC/153 (1971).

edificios, etc. En el modelo funcional técnico, la información se refiere a la descripción de las instalaciones nucleares, es decir, los procesos, las características técnicas de la instalación materiales utilizados y procedimientos, flujos de materiales, zonas de balance de materiales y los correspondientes puntos clave de medida, procedimientos, etc. (Poucet y Contini, 2000).

La información declarada se compara con los datos observados y con información de fuentes abiertas, de bases de datos especializadas, literatura científica, información interna del OIEA, así como con la cartografía de la zona, con el objetivo de verificar el modelo topológico declarado.

Dentro del OIEA, la responsabilidad de verificar que los Estados miembros cumplen sus acuerdos le corresponde al departamento de Salvaguardias y la División de Gestión de la Información (SGIM), que maneja la información geoespacial ayuda al Departamento de Salvaguardias en apoyo de su mandato por medio de la Sección de Análisis de Infraestructuras Estatales (ISI), dedicada al análisis de imágenes de satélites comerciales y la gestión de datos geoespaciales desde el año 2002.

Desde entonces, la información geoespacial y las imágenes de satélites comerciales se han convertido en una de las principales fuentes de información que contribuyen a la capacidad del OIEA para mejorar la eficacia de la aplicación de las salvaguardias, la confianza en las conclusiones de las salvaguardias y el proceso de toma de decisiones (Colakovic, Duckworth y Lafitte, 2023: 1).

La utilidad de las imágenes satélite dentro de las actividades de monitorización y verificación de las salvaguardias expuso que, por medio de ciertas imágenes, se podían verificar los mapas de los emplazamientos, detectar actividades no declaradas, nuevas actividades mineras, detectar cambios en instalaciones ya clausuradas, así como planificar la inspección de una instalación (IAEA, 1998).

Imágenes 5 m y hasta 10 m de resolución espacial se demostraron útiles para verificar la disposición de un emplazamiento y las imágenes de alta resolución disponibles en ese momento, de entre 1 y 2 m de resolución eran adecuadas para planificar inspecciones en los emplazamientos, ya que permitían distinguir múltiples características de una instalación y de sus alrededores, lo que ayuda a precisar su localización y las actividades que se hayan podido llevar a cabo dentro, en los alrededores o en el subsuelo. De este modo, los análisis de detección de cambios son muy útiles para detectar actividades no declaradas, aunque no el único, ya que la detección de fuentes de calor es una perspectiva muy interesante también para las actividades de monitorización (Truong, 2000 y Jasani y Larsson, 1998).

El ciclo de combustible nuclear engloba todas las actividades relacionadas con la producción de electricidad a partir de reacciones nucleares. Este

ciclo comienza con la extracción y la molienda del mineral de uranio. El uranio natural contiene dos isótopos: U_{235} y U_{238}. Para mantener la cadena de fisión, el contenido de U_{235} debe aumentar del 0,7 % al 34 %, lo que se consigue en las plantas de enriquecimiento. Por otro lado, el uranio natural hay que convertirlo en hexafluoruro de uranio (UF_6)[3] y este en dióxido de uranio (UO_2), que posteriormente se prensa en pequeñas pastillas cilíndricas y se cargan en tubos que formarán las barras de combustible, ensambladas por conjuntos para formar los elementos del núcleo del reactor. En general, una central nuclear puede llegar a utilizar 75 toneladas de combustible al año.

La cadena de fisión que se produce dentro de un reactor nuclear produce calor y, a su vez, vapor que se reutiliza para mover las turbinas conectadas a generadores eléctricos. Este combustible se va gastando hasta que ya no puede ser reutilizado debido a la concentración de isótopos, lo que provoca que al menos un tercio de ese combustible tenga que ser cambiado cada año. Este combustible que se descarga del reactor emite radiación y calor, por lo que necesita ser almacenado en piscinas de agua durante meses, para que vaya enfriando. Por tanto, dentro de una instalación nuclear se tendrían dos fuentes caloríficas muy potentes.

Los satélites tienen la ventaja de buscar y localizar emplazamientos por medio de su frecuencia de revisita y su resolución y, en la actualidad, los avances en ambas características les dotan de una capacidad de adquisición soberbia. Las plantas de reprocesamiento de uranio o plutonio viable para la fabricación de armas tienen unos rasgos muy distinguibles en imágenes satélite de 1 m de resolución como la cúpula o las torres de refrigeración de los reactores o las chimeneas, así como otras firmas de estructura visibles en las imágenes de alta resolución.

Por ejemplo, en una figura tomada por un satélite CORONA de la planta de reprocesamiento de Seversk, Rusia, el 15 de septiembre de 1971, ya se podía distinguir el edificio en forma de «cañón» (típico de las grandes plantas de reprocesamiento), así como la altísima chimenea, que se podía identificar de forma fácil por su larga sombra. Además, es factible identificar también el perímetro de seguridad o los edificios de enriquecimiento en las zonas de producción sur y norte, a partir de los cuales se podría estimar la escala de producción.

Para detectar los reactores de una instalación se identifican las torres de refrigeración o masas de agua natural, tomas y puertos de descarga, por ejemplo. Para localizar las plantas de reprocesamiento son muy útiles las chimeneas, como ya se ha visto, a través de su sombra, un edificio largo en forma de «cañón» o sus respiraderos, como también se pueden identificar los estanques o depósitos para residuos.

[3] O se convierte en dióxido de uranio (UO_2), directamente.

Las plantas de enriquecimiento por gas suelen ser edificios de gran superficie, por lo que tienen tejados muy largos con múltiples aberturas de ventilación y torres de refrigeración. También se podrá localizar más o menos cerca un río o un lago, así como una central o subestación eléctrica (Zhang, 2001) (figura 1).

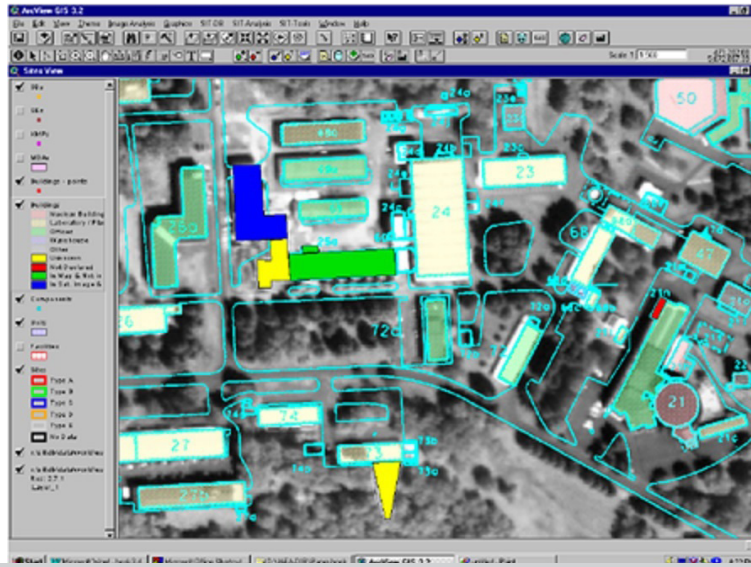


Figura 1. Ejemplo de una actividad de verificación de un mapa del emplazamiento sobre una imagen de satélite IKONOS. Fuente: Poucet, A., Contini, S. y Bellezza, F. (2001). A Gis-Based Support System for Declaration and Verification. IAEA-SM-367/CD. En: Symposium on international safeguards: Verification and nuclear material security. *Proceedings*. Viena

El conjunto de datos originales e interpretados, así como la información extraída de fuentes abiertas y la aportada por los Estados, generan la base de datos geoespacial y la base de datos de observación estructurada (SOM), forman un conjunto de datos geoespaciales que dan lugar a productos como planos de emplazamientos georreferenciados, mapas temáticos o geoportales. La gestión estructurada de las observaciones complementa el conjunto de datos geoespaciales de base y proporciona un sistema que permite recoger observaciones adicionales realizadas dentro de un marco estructurado (SOM) que se recopilan como parte del proceso de análisis de imágenes y, por lo general, se refieren a características efímeras que se pueden localizar en una figura como, por ejemplo, el movimiento de equipos de construcción y sus equipos de apoyo que, por lo general, no van a formar parte de los datos geoespaciales de base de la instalación pero sí que implican análisis más amplios del lugar (Colakovic, 2023: 7).

Como se ha podido analizar a lo largo del texto, la alta resolución de las imágenes hace cada vez más complicado poder ocultar ciertas actividades

de proliferación, sin embargo, en contrapartida a esto, algunos Estados comenzaron hace años ya a adoptar contramedidas antisatélite y ocultar sus instalaciones en el subsuelo, a pesar del gran coste que supone y que, una vez descubiertas, las actividades de monitorización continuarían sobre ese emplazamiento, ya que existen características que pueden seguir siendo detectables como carreteras de acceso, vías férreas o las entradas o salidas del emplazamiento.

Un ejemplo de instalación nuclear subterránea es la planta de reprocesamiento del complejo nuclear israelí de Dimona, que se terminó de construir a mediados de la década de 1960, con una capacidad de reprocesamiento de plutonio de entre cinco y diez cabezas nucleares al año. En una figura IKONOS de 2 m de resolución tomada el 4 de julio del año 2000 y en otras imágenes desclasificadas de este emplazamiento, pueden verse de forma clara la alta chimenea asociada a la planta de reprocesamiento, así como las vallas de seguridad que rodean el complejo, el edificio del reactor y las torres de refrigeración mecánica —con dos respiraderos— son claramente visibles en las imágenes (Zhang, 2001: 7).

Aunque, sin duda, los dos Estados proliferantes que han trabajado más por ocultar sus instalaciones de los esfuerzos del OIEA han sido Irán y Corea del Norte.

2 Un ejemplo práctico: el caso de Corea del Norte

El valor de las imágenes por satélite para la aplicación de las salvaguardias se demuestra en el caso de Corea del Norte. Las imágenes ayudan al OIEA a monitorizar la evolución del programa nuclear de este país proliferante, aunque no se puedan llevar a cabo inspecciones físicas sobre el terreno y en el caso del seguimiento y evolución de Yongbyon es especialmente importante (Quevenco, 2016).

Resumido en pocas líneas, los orígenes del problema nuclear de Corea del Norte nacen en a finales de 1945 con la división de la península a la altura del paralelo 38°. Al norte, se estableció un régimen comunista liderado por Kim Il-Sung y, en el sur, un Gobierno militar apoyado por Estados Unidos. Cinco años más tarde, con la invasión de la parte sur por parte de Corea del Norte, los dos países se enfrentaron durante tres años en una guerra (Garrido Rebolledo, 1994: 104-113).

Al término de las hostilidades, la presencia norteamericana se intensificó y, en 1953, Seúl firmó un pacto de seguridad con Estados Unidos que permitió la instalación de misiles norteamericanos tipo «Matador» en terreno surcoreano, hecho que violó algunas de las disposiciones del «Acuerdo de Pam Mun Jon» de 1953 y provocó la reacción del régimen de Kim Il-Sung, que en 1959 comenzó a mostrar interés en desarrollar un programa nuclear

ambiguo[4]. En 1965, Moscú le suministró a Corea del Norte su primer reactor de investigación de 8 MWt de potencia, un reactor nuclear experimental tipo LRT-2M, reactor que no fue sometido a Salvaguardias hasta 1977.

Corea del Norte se adhirió al TNP en 1985 y un acuerdo de garantías con el OIEA en 1992, pero rechazó las inspecciones propuestas por el Organismo, en concreto, sobre su Centro Nuclear de Yongbyon (Bunn, 2005: 8). En 1993, los satélites norteamericanos detectaron la construcción de instalaciones sospechosas que podían albergar actividades de reprocesamiento de plutonio, lo que provocó que el Gobierno de Pyongyang amenazara con abandonar el TNP. Esa crisis fue resuelta con la firma de un Acuerdo-Marco en 1994 entre Estados Unidos y Corea del Norte. En virtud de ese acuerdo, el Gobierno de Pyongyang se comprometió a desmantelar su programa nuclear, no abandonar el TNP y aceptar las Salvaguardias del OIEA. Sin embargo, el 10 de enero de 2003, Corea del Norte abandonó el Tratado de No Proliferación Nuclear y el 9 de octubre de 2006 realizó su primer ensayo nuclear.

Las estimaciones más recientes sobre el arsenal nuclear de Corea del Norte datan de 2023 y cifran el rango de cabezas nucleares entre 35 y 65

Figura 2. Análisis de la imagen del Complejo Nuclear de Yongbyon, 4 de octubre de 2023. Fuente: Albright, D., Burkhard, S., Cheng, V. y Faragasso, S. (2024). North Korea's ELWR: Finally Operational After a Long Delay. Institute for Science and International Security. Disponible en: https://isis-online.org/isis-reports/detail/north-koreas-elwr-finally-operational-after-a-long-delay/10#images

[4] Este Acuerdo era contrario a la introducción de nuevos tipos de armas, o de modelos más avanzados de las mismas en el territorio de la península coreana. Para ampliar información sobre el programa nuclear y de misiles de Corea del Norte, ver: VV. AA. (2009a y 2009b).

unidades. En 2024, se detectó actividad en las instalaciones del Complejo Nuclear Yongbyon, que albergan el reactor experimental de agua ligera (ELWR), aunque no se ha podido llegar a determinar si opera alcanzando su actividad máxima de cien megavatios térmicos (MWth).

Su actividad se detectó gracias a las descargas de agua al cauce del río próximo a la instalación. Ese punto de descarga se construyó hace más de diez años, en 2013, y parece estar conectado directo al reactor. Por tanto, es una parte crítica del sistema secundario de enfriamiento y las descargas frecuentes de agua caliente al cauce del río son evidencias del funcionamiento del reactor.

El punto de descarga del agua de refrigeración del reactor se encuentra hacia el sur de la estación de bombeo y a unos 85 m de la presa del embalse. La primera descarga fue detectada en las imágenes del 4 de octubre de 2023, siendo visible en diferentes imágenes de forma constante hasta enero de 2024. En las imágenes tomadas en invierno, es mucho más fácil apreciar que el agua está caliente, ya que el río está congelado y el terreno está cubierto de hielo y nieve, excepto en las zonas donde pasa el agua caliente. Otra zona donde se puede apreciar la nieve derretida o la ausencia de ella es en los techos planos del edificio donde se alojan las turbinas del reactor, por lo que se puede confirmar con alto grado de probabilidad que el reactor está funcionando, aunque no se pueda determinar su grado de rendimiento.

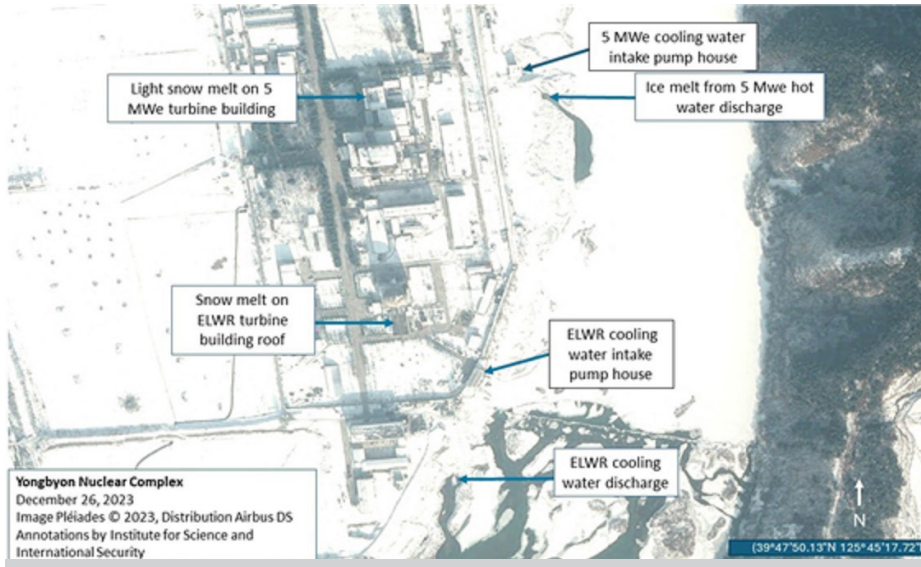


Figura 3. Análisis de la imagen del Complejo Nuclear de Yongbyon del 26 de diciembre de 2023. Fuente: Albright, D., Burkhard, S., Cheng, V. y Faragasso, S. (2024). North Korea's ELWR: Finally Operational After a Long Delay. Institute for Science and International Security. Disponible en: https://isis-online.org/isis-reports/detail/north-koreas-elwr-finally-operational-after-a-long-delay/10#images

3 Conclusión

Los avances en la tecnología de imágenes satélite han mejorado la resolución y la claridad de tal manera que, hoy en día, se han convertido en un pilar fundamental en la monitorización de las actividades de proliferación, debido principalmente a que las imágenes electro-ópticas de alta resolución o las de tipo SAR pueden capturar detalles de hasta 30 cm por píxel en tomas nocturnas o condiciones climatológicas adversas, lo que ofrece un valor añadido a las labores de inteligencia.

Tanto las operaciones militares como las de seguridad y defensa necesitan de herramientas que les permitan obtener información de calidad, datos que poder analizar y transformar en inteligencia en tiempo y forma, ya que, si reducir la incertidumbre y poder elaborar escenarios futuros, son pilares fundamentales en la disciplina de inteligencia, se antojan mucho más imprescindibles si se tienen que aplicar al ámbito de la proliferación nuclear.

Aunque el análisis de imágenes satélite se aplica como herramienta de apoyo a las salvaguardias y el Protocolo Adicional del Organismo desde el año 2002, se ha comprobado que se ha convertido en una herramienta fundamental en las labores de monitorización del OIEA y que participa de forma transversal en todas las actividades relacionadas, desde la planificación de una inspección hasta la comprobación de los datos suministrados por los Estados asociados a los emplazamientos nucleares o la detección de localizaciones no declaradas.

Sin embargo, también se ha comprobado cómo, con el tiempo, de forma lógica, se desarrollan actividades contrasatélite con el objetivo de limitar o inutilizar sus ventajas, por lo que se asume que las formas más avanzadas de teledetección como las imágenes térmicas, hiperespectrales o las tipo SAR, radar de apertura sintética, terminarán siendo contrarrestadas por alguna medida que desafíe sus capacidades o las capacidades de los analistas para tratar de encontrar evidencias, de la misma forma que se ha visto que se lleva a cabo en la actualidad, con las imágenes de instalaciones que han sido total o parcialmente soterradas.

Disponer de un catálogo más amplio de satélites comerciales, así como sus imágenes, no solo aumentaría la discusión y el monitoreo de ciertas localizaciones, sino que dificultaría las labores de decepción a los organismos de seguimiento y vigilancia como el OIEA. Además, un escrutinio desde múltiples frentes y grupos de las diferentes afirmaciones de la comunidad de inteligencia imposibilitaría bastante desafiar los tratados internacionales, ayudaría a las labores de verificación y reduciría el riesgo de un conflicto por un error en la interpretación de evidencias provocado por los efectos secundarios de una carrera armamentística.

Bibliografía

Bunn, G. (2005). The world's non-proliferation regime in time. *IAEA Bulletin*. IAEA. Nº 46/2, p. 8. [Consulta: 2025]. Disponible en: https://www.iaea.org/sites/default/files/46203590809_es.pdf

Calduch, R. (1991). Relaciones Internacionales. Madrid, Ediciones Ciencias Sociales, p. 6.

Cartagena, I. y Garrido Rebolledo, V. (2024). *La roca de Sísifo: pasado, presente y futuro del régimen de no proliferación nuclear*. J.B. Bosch.

Colakovic, M., Duckworth, S. y Lafitte, M. (2023). *Geospatial data capabilities to support safeguards understanding and awareness*. Institute of Nuclear Materials Management, p. 1.

Garrido Rebolledo, V. (1994). Corea del Norte: Entre el desarme y el rearme nuclear. Asistencia Humanitaria: Vida o Muerte. N.º 32-33, pp. 104-113.

IAEA. (1998). *Technical Workshop on Safeguards: Sources and applications of Commercial Satellite Imagery*. Viena.

IAEA. (s. f.). Safeguards explained [en línea]. Safeguards and verification, Basics of IAEA Safeguards. [Consulta: 2025]. Disponible en: Nuclear safeguards explained | IAEA

Jasani, B. y Larsson, C. (1998). Security implications of remote sensing. *Space Policy*. 4(1), pp. 46-59.

Laruelle, M. (2024). El multilateralismo nuclear de Karaganov [en línea]. *El Grand Continent*. [Consulta: 2025]. Disponible en: https://legrandcontinent.eu/es/2024/12/02/el-multilateralismo-de-karaganov/

Marrero Rocha, I. (2022). *La proliferación nuclear horizontal en el nuevo régimen de seguridad* [tesis doctoral]. Director, Diego J. Liñán Nogueras. Granada, Universidad de Granada.

Organismo Internacional de Energía Atómica. (1971). *Estructura y contenido de los acuerdos entre los Estados y el Organismo requeridos en relación con el Tratado sobre la no proliferación de las armas nucleares.* Circular Informativa OIEA, INFCIRC/153. [Consulta: 2025]. Disponible en: https://www.iaea.org/sites/default/files/infcirc153_sp.pdf

Poucet, A., Contini, S. (2000). Use of Geographical Information Systems and Satellite Images for Safeguards. En: Foggi, C. (ed.). *Proceedings of the ESARDA Seminar on Strengthening of Safeguards: Integrating the New and the Old*. Dresden, EURReport 19587.

Poucet, A., Contini, S. y Bellezza, F. (2002). GIS and satellite images in nuclear safeguards. En: Brebbia y Pascolo (eds.). *Management Information Systems*. MIT Press.

Quevenco, R. (2016). Completing the picture: using satellite imagery to enhance IAEA safeguards capabilities. *IAEA Bulletin*.

Salazar, Gonzalo de. (2015). El Tratado De No Proliferación de Armas Nucleares: los temas clave en la Conferencia de examen en 2015. *Revista UNISCI*. 38.

Truong, Q. S. B. (2000). Potential Applications of Commercial Satellite Imagery inInternational Safeguards. En: Foggi, C. (ed.). *Proceedings of the ESARDA Seminar on Strengthening of Safeguards: Integrating the New and the Old*. Dresden, EURReport 19587.

VV. AA. (2009a). North Korea's Chemical And Biological Weapons Programs. *Asia Report*. International Crisis Group. n.º 167.

VV. AA. (2009b). North Korea's Nuclear And Missile Programs. *Asia Report*. International Crisis Group. N.º 168.

VV. AA. (2015). IAEA Safeguards: serving nuclear non-proliferation. IAEA, p. 2.

Wheeler, N. y Booth, K. (2007). *The Security Dilemma. Fear, Cooperation and Trust in World Politics*. Londres, MacMillan Palgrave, p. 27.

World Nuclear Association. (2021). Safeguards to Prevent Nuclear Proliferation [en línea]. Safety and Security. [Consulta: 2025]. Disponible en: Safeguards to Prevent Nuclear Proliferation - World Nuclear Association

Zhang, H. (2001). Streghtening IAEA Safeguards using high resolution commercial satellite imagery. IAEA-SM-367/16/01. En: IAEA (ed.). *Symposium on International Safeguards: Verification and Nuclear Material Security*. Vienna.

Transformación del ciclo JISR en la era digital: innovación tecnológica para alcanzar la superioridad informativa

Begoña Rojo Carralero

Resumen

Este capítulo analiza la transformación del ciclo de Inteligencia, Vigilancia y Reconocimiento Conjunto (JISR) en el contexto de la era digital, impulsada por tecnologías emergentes y disruptivas. La integración de capacidades como la inteligencia artificial, los sensores distribuidos, las plataformas no tripuladas, el *edge computing* y los sistemas espaciales está redefiniendo la forma en que se planifica, ejecuta y explota la inteligencia en operaciones cada vez más multidominio.

A lo largo del texto, se examina el impacto de estas tecnologías en cada fase del proceso JISR (TCPED), así como los retos derivados de su uso: desde la necesidad de garantizar la interoperabilidad y la seguridad de los datos, hasta la gestión de riesgos asociados a la automatización, los sesgos algorítmicos o las vulnerabilidades frente a ciberataques.

El capítulo subraya que esta transformación no es únicamente técnica, sino también doctrinal y organizativa. Exige nuevas arquitecturas, un modelo de «dato único» y una cultura orientada a compartir, analizar y decidir con mayor agilidad. La inteligencia artificial no sustituye al factor humano, pero sí lo potencia. En definitiva, la innovación tecnológica aplicada al proceso JISR es una condición necesaria para alcanzar la superioridad informativa en los entornos operativos actuales y futuros.

Palabras clave

JISR, Tecnologías emergentes, IA, Superioridad informativa, Interoperabilidad.

Transformation of the JISR cycle in the digital age: technological innovation to achieve information superiority

Abstract

This chapter examines the transformation of the Joint Intelligence, Surveillance and Reconnaissance (JISR) cycle in the context of the digital age, driven by emerging and disruptive technologies. The integration of capabilities such as artificial intelligence, distributed sensors, unmanned

platforms, edge computing and space-based systems is redefining how intelligence is planned, executed and exploited in increasingly multi-domain operations.

The text analyses the impact of these technologies on all phases of the JISR cycle (TCPED) and highlights some of the main the challenges: the need for interoperability, secure and reliable data sharing, and the risks associated with automation, algorithmic bias and vulnerability to cyber threats.

The chapter emphasizes that this transformation is not only technical, but also doctrinal and organizational. It requires new ISR architectures, a 'single data' philosophy, and a cultural shift towards faster, more collaborative and adaptive intelligence processes. Artificial intelligence does not replace the human factor; it enhances it. Ultimately, technological innovation applied to the JISR cycle is a strategic imperative to achieve information superiority in today's and tomorrow's operational environments.

Keywords

JISR, AI, Emerging Technology, Information Superiority, Interoperability.

«En el siglo XXI, el éxito no será del que más datos obtenga, sino del que más rápido y mejor los convierta en decisiones acertadas».

1 Introducción

La información sigue siendo un factor clave para el éxito en los ámbitos de la seguridad y la defensa. No se trata solo de procesarla, sino también de disponer de ella y trasladarla al nivel de decisión correspondiente, en el momento oportuno y en el formato adecuado.

En un entorno operativo cada vez más digital, automatizado y multidominio, como el de hoy en día, el papel de la inteligencia sigue siendo esencial, pero su forma de generarse, procesarse y aplicarse está cambiando de forma radical. La capacidad de observar, analizar y decidir con rapidez está redefiniendo las reglas del juego. En pleno siglo XXI, el acceso a información precisa y en tiempo real se ha convertido en un factor crítico para obtener ventaja frente a un adversario.

En este contexto, el proceso de inteligencia, vigilancia y reconocimiento conjunto (*Joint ISR o JISR*) se consolida como una herramienta esencial de apoyo al planeamiento y la conducción de operaciones. El volumen, la diversidad y la velocidad de los datos disponibles superan las capacidades de los sistemas convencionales, por lo que la innovación es una herramienta de apoyo para su mejora continua.

Innovar consiste en introducir ideas nuevas o transformar lo ya existente para mejorar los resultados. En el ámbito de la inteligencia militar, esta mejora podría traducirse en la capacidad de tomar decisiones más rápidas, mejor informadas y adaptadas a un entorno operativo cada vez más complejo.

La innovación tecnológica, impulsada por el desarrollo de tecnologías emergentes y disruptivas, está transformando el proceso JISR en profundidad. La inteligencia artificial, el *edge computing*[1], los sensores distribuidos, las plataformas no tripuladas y el uso de fuentes abiertas están dando lugar a un nuevo modelo de arquitectura ISR, más automatizado, interoperable y adaptativo.

La propia OTAN ha reconocido este cambio. En su Concepto Estratégico más reciente, establece el conocimiento superior del entorno como una condición necesaria para mantener la disuasión y responder eficazmente a las amenazas actuales. En este contexto, el enfoque de operaciones

[1] *Edge Computing* o computación en el borde es un paradigma tecnológico que permite procesar los datos cerca de su fuente de generación (sensores, plataformas), lo que reduce la latencia y mejora la capacidad de respuesta en tiempo real.

multidominio (MDO) adquiere especial relevancia como modelo operativo integrado, en el que el proceso JISR permite coordinar capacidades en los ámbitos terrestre, marítimo, aéreo, ciberespacial y cognitivo.

Este capítulo analiza cómo el proceso JISR está evolucionando hacia un sistema más eficiente y multidominio, capaz de operar en entornos altamente digitalizados. A lo largo del texto, se examinarán tanto las oportunidades que ofrecen estas tecnologías como los riesgos y desafíos que plantean.

Innovar en el proceso JISR no es solo una opción tecnológica, sino una necesidad estratégica para anticiparse, adaptarse y decidir con ventaja. En definitiva, el objetivo no es recopilar más datos, sino convertirlos más rápido y de manera fiable en información útil. Y para eso, las tecnologías emergentes y disruptivas, en particular la inteligencia artificial, resultan determinantes.

2 Conceptos básicos del proceso ISR

La Inteligencia, Vigilancia y Reconocimiento Conjunto (JISR) es una capacidad clave para dotar de conciencia situacional al mando y facilitar una toma de decisiones oportuna.

Dentro de la doctrina conjunta de los países aliados, el término JISR se define como el conjunto de capacidades de inteligencia y operaciones que integra las capacidades de recopilación con el procesamiento, explotación y difusión de la información resultante[2].

El proceso JISR se define como un proceso de coordinación a través del cual la recopilación de inteligencia y las actividades de explotación proporcionan datos e información para satisfacer una necesidad de información o inteligencia, en un marco temporal deliberado, *ad hoc* o dinámico, en apoyo de la planificación y ejecución de las operaciones.

Este proceso tiene como objetivo apoyar directamente la planificación, preparación y ejecución de las operaciones, apoyándose en los siguientes elementos constitutivos, los cuales se resumen a continuación:

— Inteligencia: este componente abarca todas las disciplinas de recopilación de inteligencia, incluidas sus capacidades y activos de recolección, procesamiento, explotación y difusión. Las disciplinas de recopilación de inteligencia incluyen: inteligencia acústica (ACINT), inteligencia humana (HUMINT), inteligencia de imágenes (IMINT), inteligencia de medición y firma (MASINT),

[2] Extracto de la definición del proceso JISR según publicaciones y procedimientos de organismos aliados.

inteligencia de fuentes abiertas (OSINT) e inteligencia de señales (SIGINT)

— Vigilancia: la vigilancia consiste en la observación sistemática en todos los ámbitos operativos. Se lleva a cabo mediante medios visuales, electrónicos, fotográficos o de otro tipo y puede abarcar grandes áreas o enfocarse en objetivos específicos.

— Reconocimiento: el reconocimiento permite obtener información mediante observación visual u otros métodos de detección. Su propósito es recopilar datos sobre las actividades y recursos de un adversario o conocer las características meteorológicas, hidrográficas o geográficas de una zona determinada.

Junto con los elementos descritos con anterioridad, este proceso, consta de cinco fases conocidas como TCPED (T*ask, Collect, Process, Exploit and Disseminate*):

— *Task* (Asignación): recopilación de necesidades ISR y planificación interna de recursos, gestión y asignación de capacidades.

— *Collect* (Recopilación): obtención de datos e información a través de sensores terrestres, aéreos, navales, espaciales, cibernéticos y cognitivos, así como de fuentes humanas o abiertas.

— *Process* (Procesado): organización, filtrado y análisis inicial de los datos. Esta fase puede realizarse mediante personal especializado o algoritmos automatizados.

— *Exploit* (Explotación): interpretación avanzada de la información. También puede dar lugar a nuevas necesidades.

— *Disseminate* (Difusión): entrega de la información a los usuarios adecuados en el momento preciso, a través de canales seguros y adaptados al nivel táctico, operacional o estratégico.

Figura 1. Esquema de fases del ciclo JISR

Este proceso no funciona de forma aislada. Está vinculado con el proceso de gestión de las necesidades de inteligencia y gestión de la obtención, conocido como IRM&CM (*Intelligence Requirements Management & Collection Management*). Su objetivo es garantizar que las necesidades de información sean correctamente formuladas, priorizadas y cubiertas mediante los medios más adecuados y optimizar el uso de recursos ISR.

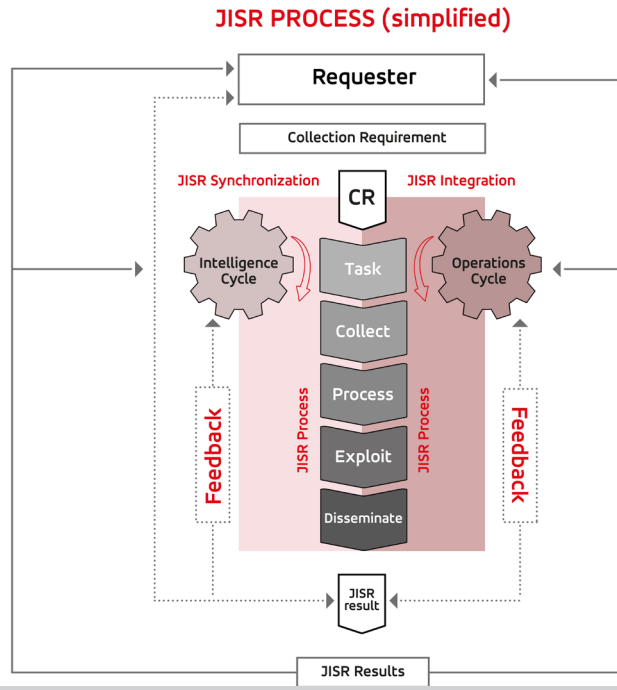


Figura 2. Relación entre el Ciclo de Inteligencia y su Integración en las Operaciones

La figura 2 muestra de manera esquemática la interconexión entre ISR y los ciclos de inteligencia y operaciones.

3 JISR en las operaciones multidominio y el campo de batalla transparente

El concepto de operaciones multidominio (*Multi-Domain Operations*, *MDO*) está ganando un protagonismo creciente como modelo de actuación militar que busca la sincronización de capacidades a través de los dominios terrestre, marítimo, aéreo, espacial, cibernético y cognitivo. Este enfoque permite generar efectos coordinados y simultáneos, de modo que explota sinergias entre dominios y reduce los tiempos de respuesta ante amenazas complejas y dinámicas.

En este nuevo entorno operativo, profundamente digitalizado y caracterizado por una densa malla de sensores y fuentes de información, ha emergido lo que de modo informal se denomina «campo de batalla transparente». Esta nueva realidad no responde tanto a una capacidad deseada, sino al resultado inevitable de la hiperconectividad: sensores militares y civiles, plataformas no tripuladas, redes sociales, dispositivos inteligentes y satélites que generan información constante y multidominio. Todo emite, todo es observado, todo deja rastro.

La consecuencia directa de esta transformación es que el proceso JISR ha tenido que adaptarse a un ecosistema donde la accesibilidad, la veracidad y la velocidad de los datos se han convertido en variables operativas críticas. En un entorno permanentemente observado, cualquier evento relevante puede ser detectado, geolocalizado, interpretado y compartido, por lo que la capacidad de actuar con rapidez es un factor decisivo.

En este contexto, la fusión de información procedente de múltiples fuentes de imágenes (IMINT), señales (SIGINT), fuentes abiertas (OSINT) y combinarla con inteligencia geoespacial (GEOINT) o inteligencia humana (HUMINT), se convierte en el eje central del valor añadido que aporta el sistema JISR. Este nivel de integración se está viendo beneficiado gracias a la inteligencia artificial (IA), que automatiza la explotación, detecta patrones, señala anomalías y facilita decisiones en tiempo real.

La IA, junto con el resto de las tecnologías innovadoras descritas en este capítulo como la «computación en el borde», la sensorización avanzada o los sistemas distribuidos, actúa como catalizador del cambio. El proceso ISR debe ser, por tanto, un sistema distribuido, alimentado por datos de múltiples dominios, orientado a generar información útil, oportuna y verificable.

4 Iniciativas OTAN y europeas relacionadas con el ciclo de inteligencia

La densidad informativa se ha incrementado exponencialmente con la incorporación de sensores comerciales, plataformas autónomas, constelaciones de pequeños satélites, sistemas HAPS (*High Altitude Platform Systems*), sistemas IoT (*Internet of the Things*) y datos abiertos. Todo ello conforma un entorno donde el reto no es solo recoger información, sino organizarla, explotarla y compartirla eficazmente, de modo que garantice coherencia y accesibilidad en tiempo real.

En este entorno, la OTAN ha introducido el concepto de «vigilancia persistente»[3] como un requisito clave para garantizar una respuesta eficaz ante esta nueva realidad operativa. Esta vigilancia exige la integración de medios en múltiples dominios y el desarrollo de nuevas estructuras, procesos y capacidades. La capacidad de utilizar y fusionar distintas herramientas será esencial para lograr este objetivo.

En esta línea, se enmarca la iniciativa *Allied Persistent Surveillance from Space* (APSS), que busca establecer una capacidad aliada de vigilancia persistente desde el espacio e integra activos nacionales y comerciales para proporcionar productos ISR que apoyen la toma de decisiones conjuntas. Esta capacidad incluye la recopilación, análisis

[3] The future of NATO- C4ISR-Assesment and recommendations after Madrid y «The Future of NATO C4ISR» (NCI Agency). JDN 1/23 (UK) y doctrina organismos aliados.

Figura 3. Alliance Ground Surveillance (AGS) RQ-4D «Phoenix». Foto OTAN

y diseminación de datos obtenidos por satélites y sensores espaciales, con el apoyo de herramientas de inteligencia artificial, y bajo estándares compartidos como el STANAG 4559[4], cuyo objetivo es promover la interoperabilidad para el intercambio de productos de inteligencia, vigilancia y reconocimiento entre los sistemas C4ISTAR (*Command, Control, Comunications, Computers, Intelligence, Surveillance Target Acquisiton and Reconnaissance)* accesibles a la OTAN.

Por su parte, la Unión Europea, a través del *Capability Development Plan* (CDP) 2023 de la Agencia Europea de Defensa (EDA), ha identificado como prioridad estratégica el desarrollo de capacidades C4ISTAR persistentes, interoperables y basadas en datos para la defensa colectiva, la gestión de crisis y la resiliencia estratégica.

Además, el Fondo Europeo de Defensa (EDF, por sus siglas en inglés) ha financiado múltiples proyectos de innovación orientados al refuerzo de la arquitectura ISR europea:

— LOTUS, centrado en plataformas terrestres no tripuladas para vigilancia y reconocimiento.

— ODIN'S EYE, orientado a la alerta temprana desde el espacio y sensores de observación estratégicos.

— ABIDE, que explora el uso de inteligencia artificial y *big data* para la toma de decisiones en C4ISR.

[4] STANAG 4559- NATO standard ISR library interfaces and services.

— REACT, enfocado en fusión de datos y arquitectura de sistemas ISR federados.

— SAURON, especializado en vigilancia persistente para protección de infraestructuras críticas.

Estas iniciativas evidencian una apuesta clara por arquitecturas abiertas, distribuidas y colaborativas, capaces de reforzar la innovación y la autonomía tecnológica europea y su integración con las capacidades aliadas.

5 Transformación del proceso JISR: del modelo clásico al digital y multidominio

Las condiciones descritas en los apartados anteriores, junto con la innovación aportada por las tecnologías emergentes y disruptivas, obligan a replantear de forma profunda la organización, ejecución y arquitectura del sistema JISR.

La transición a la era digital ha generado un entorno operativo profundamente transformado, en el que la información de dominio público, procedente de redes sociales, sensores urbanos, dispositivos inteligentes o comunicaciones máquina a máquina, supera en volumen y diversidad a las fuentes militares tradicionales. Este cambio ha desdibujado las fronteras entre lo civil y lo militar.

El volumen, la variedad y la velocidad de los datos superan la capacidad de procesamiento manual y las operaciones actuales se desarrollan de forma simultánea en múltiples dominios. Además, se integran capacidades de aliados y socios, con arquitecturas técnicas diversas y fuentes de información cada vez más descentralizadas. La proliferación de fuentes y formatos exige sistemas capaces de operar en red, en entornos federados y con interoperabilidad semántica, para evitar duplicidades, ambigüedades o sesgos en la producción de la información requerida en el proceso.

Esta evolución plantea retos específicos para el proceso JISR, derivados de las características del *big data*: volumen, variedad, velocidad y veracidad. La capacidad para obtener datos ya no es el principal problema: lo son su validación, priorización, fusión y explotación eficaz en tiempo útil.

Este nuevo escenario exige un sistema ISR distribuido, automatizado y multidominio, capaz de integrar flujos de datos heterogéneos, operar con flexibilidad y generar información útil en tiempo real[5]. La digitalización está reforzando esta tendencia y facilita la convergencia entre capacidades ISR, guerra electrónica, ciberdefensa y plataformas de combate. En este nuevo

[5] Tal y como recogen documentos doctrinales de la OTAN, la JDN 1/23 del Reino Unido y el informe *Science & Technology Trends 2023-2043*, esta es una transformación en curso actualmente.

paradigma, la ISR se consolida como una capacidad funcional central, lo que supera su rol tradicional de apoyo auxiliar y se conecta de forma transversal con los procesos de planificación, ejecución y evaluación de operaciones.

Para operar eficazmente a los desafíos del entorno actual, las arquitecturas ISR deben diseñarse, implementarse y gestionarse conforme a una serie de principios y criterios operativos fundamentales[6]:

- Flexibilidad: para adaptarse rápido a los cambios del entorno operacional. Esto implica reconfiguración dinámica de sensores, priorización automatizada y adaptación a nuevas amenazas o áreas de interés.
- Misión a medida: de modo que cada despliegue ISR responda a las necesidades específicas de la operación, en función de los dominios implicados y el tipo de información requerida.
- Interconectividad: que garantice la integración fluida entre sensores, plataformas, niveles de mando, dominios operativos y socios aliados. Debe facilitarse tanto la conexión vertical como horizontal entre capacidades ISR.
- Compatibilidad: mediante el cumplimiento de estándares técnicos y doctrinales comunes, como los definidos por la OTAN o los marcos de interoperabilidad de la UE. Esto permite compartir productos ISR en entornos multinacionales.
- Automatización: las redes ISR deben operar con el mayor grado posible de automatización y permitir el ajuste autónomo de prioridades y la activación oportuna de sensores.
- Escalabilidad: deben disponer de capacidad suficiente para adaptarse al crecimiento del volumen de datos e incluir recursos de almacenamiento, análisis y diseminación segura.
- Ancho de banda y conectividad: la arquitectura debe garantizar una infraestructura de comunicaciones robusta, segura, capaz de soportar flujos de datos intensivos, minimizar latencias y asegurar la disponibilidad en condiciones adversas.
- Resiliencia y redundancia: de forma que la arquitectura pueda mantener funcionalidad básica incluso en entornos degradados. Cuando la red integrada no esté disponible, deben activarse estructuras alternativas que aseguren la continuidad de la obtención y la diseminación de la información necesaria.

[6] UK Joint Doctrine Note 1/23 (JDN 1/23), que adapta con una exposición más explícita y moderna los principios fundamentos del diseño del proceso JISR según OTAN.

Este conjunto de principios y transformaciones técnicas tiene un objetivo final: garantizar que el sistema ISR no solo responda a las necesidades actuales de las operaciones, sino que esté preparado para adaptarse, anticiparse y operar de forma resiliente en entornos cada vez más interconectados, competitivos y saturados de información.

6 Impacto de las tecnologías emergentes en el proceso JISR

La innovación tecnológica está transformando de manera acelerada el proceso JISR. Esta evolución afecta a toda su arquitectura: desde la expansión de sensores y fuentes de información hasta la automatización de los procesos de análisis y difusión de información.

Tanto la OTAN como la Unión Europea han identificado un conjunto de áreas tecnológicas prioritarias, conocidas como tecnologías emergentes y disruptivas que están redefiniendo los modelos operativos, las capacidades militares y la forma en que se genera inteligencia en los entornos modernos.

En el caso de la OTAN, la clasificación como *Emerging and Disruptive Technologies (EDT)* incluye diez grandes categorías: inteligencia artificial (IA), sistemas autónomos y robótica, *big data* y tecnologías de información, espacio, sistemas hipersónicos, energía y propulsión, materiales avanzados, electrónica y electromagnetismo, tecnologías cuánticas y tecnologías de mejora humana y biotecnología.

Por su parte, la Unión Europea, a través de la EDA y el Fondo Europeo de Defensa ha desarrollado una agenda convergente centrada en el refuerzo de la autonomía estratégica, el entorno electromagnético, la ciberdefensa, el espacio, las plataformas no tripuladas y los sensores colaborativos.

Esta convergencia en las prioridades estratégicas de OTAN y UE evidencia una clara alineación en cuanto al papel esencial que tendrán estas tecnologías para el desarrollo futuro de las capacidades militares.

Este desarrollo tecnológico está transformando de manera acelerada el ciclo de inteligencia. Esta evolución no se limita a la automatización del análisis de datos, sino que afecta a toda la arquitectura ISR, desde la proliferación de sensores hasta la explotación descentralizada en tiempo real.

A continuación, se analiza el impacto de algunas de ellas en las distintas fases y dimensiones del proceso JISR.

6.1 IA y Computación en el borde (edge computing)

Uno de los principales retos del proceso JISR es gestionar de forma eficaz el enorme volumen de datos generado por sensores distribuidos, plataformas no tripuladas y fuentes abiertas. La inteligencia artificial y la

computación en el borde están transformando este proceso, de modo que permite automatizar tareas complejas de análisis, reducir los tiempos de respuesta y optimizar el ciclo de toma de decisiones.

La IA facilita la fusión de datos provenientes de múltiples fuentes (IMINT, SIGINT, OSINT, GEOINT, HUMINT) y permite detectar patrones, anticipar amenazas, clasificar objetos o generar alertas en tiempo real. Además, contribuye a reducir la carga cognitiva del operador, priorizar lo relevante y ofrecer productos listos para la explotación operativa.

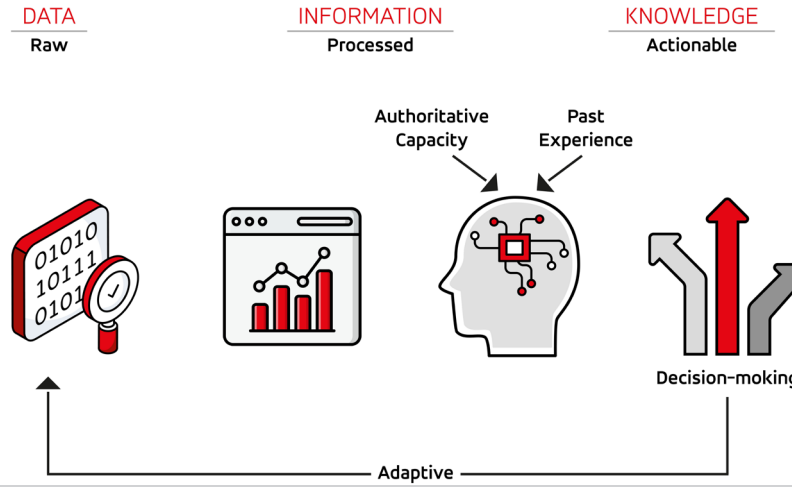


Figura 4. Flujo de datos a información. Fuente: Internetofwater.org

En paralelo, la computación en el borde (*edge computing*) permite procesar la información directamente en el sensor o en plataformas cercanas al punto de obtención, sin necesidad de enviarla a centros centralizados. Esta capacidad mejora la autonomía operativa, aumenta la resiliencia ante interrupciones en la red y es especialmente útil en UAV, sensores desplegados en zonas remotas o sistemas que operan en entornos degradados.

La digitalización impulsada por el Internet Militar de las Cosas (IoMT), genera nuevas exigencias en interoperabilidad, conectividad y gestión de datos. Esta evolución tecnológica está favoreciendo el despliegue de plataformas autónomas o en enjambre, capaces de actuar de forma coordinada, con una supervisión humana más centrada en los efectos que en la gestión técnica del sistema.

Esta transformación tiene también un impacto directo en los perfiles profesionales requeridos. Se demandan operadores con capacidades híbridas, capaces de interactuar con sistemas inteligentes, interpretar salidas automatizadas y tomar decisiones en entornos altamente digitalizados.

Esto obligará a adaptar los programas de formación y entrenamiento en ISR, con un enfoque más técnico, cognitivo y multidominio.

6.2 Expansión y diversificación de sensores

Los sensores son la base del proceso JISR. El avance de la tecnología ha permitido desplegar una gran diversidad de sensores en todos los dominios operativos (terrestre, marítimo, aéreo, espacial, cibernético y cognitivo) con capacidad para recopilar datos ópticos, térmicos, acústicos, electromagnéticos o gravitacionales. La miniaturización y la mejora en eficiencia energética han aumentado la persistencia, adaptabilidad y cobertura de estos sistemas en entornos complejos y multidominio.

El concepto de red de sensores interconectados permite configurar sistemas distribuidos de vigilancia, donde la información se obtiene, transmite y analiza de forma colaborativa. La implementación de procesamiento avanzado en el propio sensor, combinado con *edge computing*, reduce la necesidad de transmitir grandes volúmenes de datos, mejora la fiabilidad de la información y optimiza el uso del ancho de banda.

Además, los sensores civiles y comerciales, como los integrados en redes sociales, dispositivos móviles o sistemas IoT[7], amplían las capacidades del proceso ISR. Estos dispositivos, que recogen vídeo, audio, posicionamiento por satélite o datos de proximidad, proporcionan fuentes complementarias de información con un alto valor operativo, sobre todo, en entornos urbanos o híbridos.

La integración de datos procedentes de redes sociales y sensores tradicionales permitirá avanzar en tareas como el filtrado y resumen de contenido, la detección y seguimiento de eventos, el análisis de dinámicas sociales o la identificación de anomalías en tiempo real. Esta fusión de fuentes y tecnologías mejora la capacidad de respuesta ante amenazas emergentes y consolida un ecosistema de inteligencia más preciso, adaptable y resiliente frente a amenazas electrónicas o cibernéticas.

6.3 Uso de plataformas no tripuladas

El empleo de plataformas no tripuladas (UxV) ha supuesto un cambio cualitativo en las capacidades de inteligencia, vigilancia y reconocimiento. Su integración en operaciones es ya una realidad, impulsada por su capacidad para operar con bajo riesgo, mantener prolongados tiempos de permanencia y posicionarse con flexibilidad en entornos complejos o de difícil acceso.

[7] Internet of the Things.

En particular, los vehículos aéreos no tripulados (UAV) en sus distintas categorías: micro, mini, tácticos o estratégicos, permiten cubrir distintas zonas de interés con sensores ligeros (EO/IR, radar, magnéticos, entre otros), lo que mantiene una vigilancia adaptable y continua. Estas plataformas han demostrado ser especialmente eficaces en operaciones prolongadas, misiones de patrullaje y entornos con escasa cobertura ISR tradicional.

En escenarios urbanos o de combate asimétrico, los micro-UAV desplegables están mejorando de forma significativa la conciencia situacional en tiempo real. Facilitan la adquisición de objetivos, el reconocimiento inmediato y la protección de fuerzas, a la vez que reducen el riesgo para el personal desplegado.

En paralelo, se están desarrollando capacidades de enjambres coordinados de UxV, en los que múltiples unidades cooperan de forma autónoma mediante reparto dinámico de tareas. Estas arquitecturas permitirán ampliar la cobertura ISR, reducir los tiempos de respuesta y optimizar los recursos en operaciones distribuidas y multidominio.

Figura 5. Sistema ISR no tripulado Clase I SEEKER de AUREA Avionics

El uso masivo e inteligente de UxV seguirá creciendo, en especial, cuando se integren con IA, *edge computing* y redes ISR interoperables. Su papel como nodos dinámicos de obtención consolidará su valor dentro del ecosistema JISR.

6.4 Tecnologías cuánticas

Las tecnologías cuánticas, aunque aún en fases de desarrollo incipientes, se perfilan como habilitadores disruptivos claves para el proceso JISR en el horizonte 2030-2040. Su potencial transformador abarca capacidades de

obtención, comunicación, análisis y protección de la información, con implicaciones directas en todos los dominios operativos.

En primer lugar, los sensores cuánticos permitirán detectar con extrema precisión variaciones gravitacionales, geomagnéticas o inerciales. Esta capacidad será especialmente útil en entornos donde los sistemas de navegación por satélite han sido negados o degradados. También se contempla su empleo para mapeo subterráneo, navegación en zonas GNSS-denegadas (entornos donde las señales de navegación por satélite no están disponibles o están limitadas) o seguimiento de objetos submarinos, ampliando las capacidades ISR en entornos difíciles.

En segundo lugar, las comunicaciones cuánticas, en especial mediante técnicas de distribución cuántica de claves (QKD), permitirán establecer enlaces de transmisión prácticamente inmunes a la interceptación o manipulación externa. Estas soluciones reforzarán la seguridad de redes ISR entre plataformas móviles, nodos distribuidos y enlaces espaciales.

Por último, la computación cuántica ofrece una capacidad teórica para resolver problemas complejos no abordables con los sistemas actuales. Su aplicación potencial al análisis masivo de datos, la optimización de misiones, la simulación avanzada de escenarios operativos o la toma de decisiones en tiempo real podría suponer un salto cualitativo para el sistema JISR. Sin embargo, estas aplicaciones aún enfrentan importantes desafíos técnicos, como la estabilidad de los *cúbits*, las condiciones extremas de funcionamiento o la escalabilidad de los sistemas.

Según el informe NATO Science & Technology Trends 2023-2043, los sensores cuánticos son la línea más próxima a una aplicación operativa real, mientras que las comunicaciones y la computación cuántica requerirán más tiempo para alcanzar una madurez funcional. Aun así, su desarrollo anticipado será esencial para mantener la superioridad informativa y la resiliencia frente a actores tecnológicamente avanzados.

6.5 Espacio / satélites

El espacio se ha consolidado como un dominio estratégico crítico para las capacidades ISR modernas. Su valor reside tanto en la obtención de información como en la vigilancia, observación y superioridad informativa en entornos operativos complejos. Durante la próxima década, se espera un aumento exponencial de las capacidades espaciales, impulsado por la miniaturización de plataformas, la reducción de costes de lanzamiento y la madurez tecnológica de sistemas orbitales.

Uno de los desarrollos más significativos es la proliferación de pequeños satélites (*smallsats*) en órbitas bajas (LEO) y medias (MEO). Estas plataformas, más económicas y flexibles que los grandes satélites tradicionales, permiten una vigilancia más frecuente, mayor resiliencia frente a amenazas

antisatélite y una capacidad de observación más ágil. Las constelaciones de *smallsats*, equipadas con sensores ópticos, infrarrojos o radar de apertura sintética (SAR), ofrecen una resolución y latencia cada vez más competitivas.

En este contexto, la iniciativa *Allied Persistent Surveillance from Space* (APSS) de la OTAN, mencionada en apartados previos, impulsa el desarrollo de una arquitectura aliada de vigilancia permanente desde el espacio. Esta capacidad integrará activos nacionales y comerciales para proporcionar productos ISR basados en satélites y sensores embarcados, combinados con herramientas de procesamiento avanzado, fusión de datos e inteligencia artificial. Todo ello bajo estándares OTAN como el STANAG 4559, que garantizan la interoperabilidad entre aliados.

Paralelamente, se están desarrollando soluciones intermedias como los HAPS (*High-Altitude Pseudo-Satellites*). En el marco de la PESCO (Permanent Structured Cooperation) y el Fondo Europeo de Defensa, el proyecto EuroHAPS está experimentando con dirigibles estratégicos, plataformas híbridas y globos estratosféricos, diseñados para operar durante largos periodos de tiempo. Estas plataformas ligeras ofrecen una vigilancia persistente en escenarios donde los satélites pueden tener limitaciones.

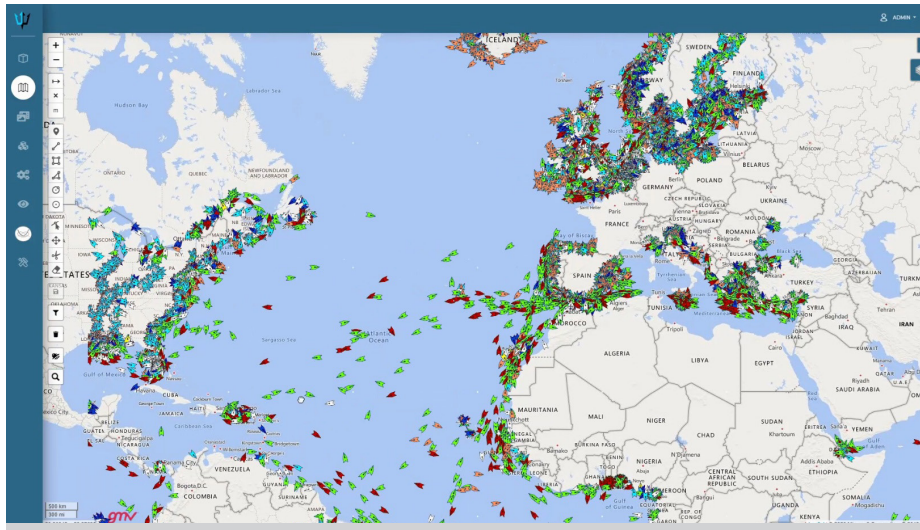


Figura 6 Sistema C2 SOCRATES de GMV para la detección y clasificación de buques

Por último, los programas de satélites de comunicaciones militares de nueva generación, como SPAINSAT *Next Generation* (SPAINSAT NG), están diseñados para reforzar la conectividad segura y la resiliencia de los flujos de información en operaciones conjuntas y multidominio. Su integración en arquitecturas ISR interoperables será esencial para asegurar el dominio informativo y la continuidad operativa en todo el espectro de misiones.

6.6 Sistemas hipersónicos

Actualmente, se están explorando las posibilidades de emplear plataformas hipersónicas con fines ISR y aprovechan su alta velocidad y baja detectabilidad para realizar misiones de reconocimiento estratégico a gran altitud. Este tipo de plataformas permitiría una recolección de datos e información más ágil y flexible que la ofrecida por los satélites tradicionales, sobre todo, en escenarios donde se requiera una cobertura puntual, rápida y de difícil detección.

Desde el punto de vista de la amenaza, los sistemas hipersónicos representan un desafío tecnológico emergente de primer orden. Su combinación de velocidad extrema, capacidad de maniobra y baja firma los hace difíciles de detectar, seguir e interceptar. Estas características obligan a rediseñar las arquitecturas actuales de alerta temprana, seguimiento y respuesta, ya que reducen drásticamente los márgenes temporales para la toma de decisiones.

Para enfrentarlos, será necesario integrar redes de sensores distribuidos, tanto terrestres como espaciales, apoyadas en capacidades de análisis automatizado e inteligencia artificial. Solo una arquitectura ISR adaptativa, con detección en múltiples dominios y capacidad de respuesta en tiempo casi real, podrá ofrecer cobertura efectiva frente a este tipo de amenazas.

6.7 Tendencias transversales en tecnologías emergentes aplicables a ISR

Además de las tecnologías específicas ya analizadas, existen líneas de desarrollo que están impactando de forma transversal en el ecosistema JISR y aportan capacidades complementarias que refuerzan su precisión, adaptabilidad y resiliencia.

Los nuevos materiales, como metales avanzados, recubrimientos inteligentes o superficies autolimpiables, permiten fabricar antenas más potentes, estructuras más ligeras y resistentes y componentes capaces de operar en condiciones extremas. La «fabricación aditiva», por su parte, está revolucionando la logística militar, al posibilitar la producción *in situ* de piezas críticas para sensores o plataformas ISR.

En el ámbito de la biotecnología, se están incorporando sensores biométricos al equipamiento del combatiente, lo que permite el monitoreo en tiempo real del estado físico y cognitivo del operador. Estas tecnologías, combinadas con interfaces avanzados y realidad aumentada, contribuyen a mejorar la conciencia situacional y la toma de decisiones bajo presión.

Las tecnologías de energía avanzada, como baterías de nueva generación, sistemas de propulsión eléctrica o armas de energía dirigida (láseres, microondas), permitirán desplegar plataformas ISR más sostenibles,

silenciosas y autónomas. Esto cobra especial relevancia en misiones prolongadas, entornos denegados.

Finalmente, la convergencia entre inteligencia artificial y computación cuántica abre nuevas posibilidades para el análisis de datos complejos, la simulación de escenarios y la gestión segura de comunicaciones. Estas capacidades permitirán conectar redes ISR distribuidas en todos los dominios (terrestre, marítimo, aéreo, espacial, cibernético y cognitivo), con mayor precisión, velocidad y resiliencia.

Estas tendencias no solo ampliarán las funciones tradicionales de la ISR, sino que contribuirán a consolidar un entorno más distribuido, robusto y adaptativo. Su adopción deberá realizarse bajo principios éticos, marcos normativos aliados y criterios de interoperabilidad que garanticen su eficacia operativa y su integración segura en entornos multinacionales.

7 Posibles mejoras en cada una de las fases del proceso JISR

Como ya se ha visto con anterioridad, el proceso JISR se organiza en torno a cinco fases conocidas como TCPED (Task, Collect, Process, Exploit, Disseminate). Cada una de ellas ha sido clásicamente abordada mediante procedimientos secuenciales y sistemas especializados. Sin embargo, la transformación digital y la introducción de tecnologías disruptivas están permitiendo avances concretos que podrían favorecer la eficacia de cada etapa.

A continuación, se describen estas mejoras con un enfoque basado en la aplicación de las tecnologías descritas previamente, de una manera realista y con base en el conocimiento disponible en GMV gracias al desarrollo de la suite de herramientas JISR SAPIIEM[8]. Estas herramientas se han probado con excelentes resultados en distintos ejercicios de la OTAN, como Unified Vision, Steadfast Cobalt, MAJEX, OPTIMAX, Trident Juncture, entre otros.

7.1 Tasking – *Planificación y asignación de recursos*

La fase de asignación de tareas y gestión de necesidades de inteligencia ha sido tradicionalmente un proceso lento, manual y muy dependiente de la experiencia del operador. Sin embargo, la integración progresiva de inteligencia artificial está transformando esta etapa y permite automatizar tareas como la identificación de zonas o áreas de interés donde operaran los medios de obtención, la asignación óptima de medios ISR o la priorización de requerimientos en función de criterios operativos, disponibilidad y contexto.

[8] SAPIIEM, es la suite de productos JISR, compatibles con las iniciativas de interoperabilidad de la OTAN (STANAG) y la doctrina de la OTAN, desarrollada por GMV.

Ejercicios como el JFX[9] han demostrado que establecer dinámicas de trabajo más flexibles, apoyadas en herramientas como SAPIIEM, mejora significativamente la planificación y la trazabilidad de la obtención de la información. Interfaces adaptadas y asistentes inteligentes permitirán en el futuro realizar simulaciones de escenarios, identificar redundancias en los requerimientos o proponer alternativas de asignación según cambios en el entorno operativo.

7.2 Collection – *Obtención de información*

La fase de recogida de datos se beneficia directamente de la proliferación de sensores terrestres, navales, aéreos, espaciales y cibernéticos. El despliegue de UAV de última generación, sensores distribuidos y redes IoT permite una recolección de información más persistente, diversa y automatizada, adaptada a entornos operativos cada vez más complejos.

El uso de inteligencia artificial en esta fase permite programar dinámicamente sensores, redirigirlos ante eventos imprevistos o activar de forma autónoma plataformas de observación. Este tipo de automatización mejora la eficiencia del sistema y permite responder con mayor rapidez a nuevas necesidades de obtención.

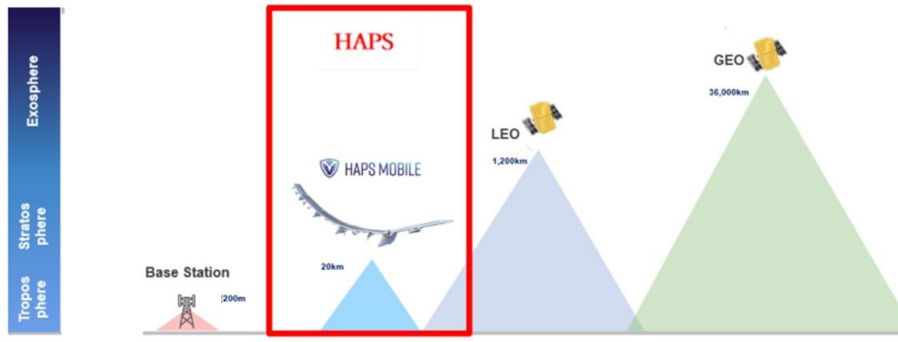


Figura 7. Altitudes operación HAPS. Fuente HAPS Alliance

En particular, esta lógica resulta especialmente útil en entornos urbanos densos, donde tecnologías como los micro-UAV desplegables a nivel táctico facilitarán la vigilancia, la protección de fuerzas y la recopilación de datos en tiempo real, incluso en condiciones adversas o degradadas.

[9] Joint Force Exercise (Ejercicio de la Fuerza Conjunta), un ejercicio militar nacional español organizado por el Estado Mayor Conjunto de las Fuerzas Armadas (EMACON). Su objetivo es adiestrar a la estructura operativa de las FAS en la planificación y conducción de operaciones conjuntas e integrar sistemas ISR, C2, etc. Su ejecución es anual.

7.3 Processing – *Tratamiento y clasificación de datos e información*

El procesamiento de datos es una fase crítica, donde se organiza y estructura la información recopilada. Gracias al uso de *edge computing*, muchas tareas de procesamiento pueden realizarse ahora en el propio sensor o en nodos cercanos, lo que reduce la latencia y mejora la resiliencia ante cortes de red.

Además, técnicas de reconocimiento de objetos mediante IA permiten catalogar de forma automática la información de sensores, imágenes satelitales o vídeos. Estas herramientas pueden detectar anomalías, etiquetar datos e incluso generar metadatos útiles para su explotación posterior.

7.4 Exploitation – *Análisis de los datos y la información*

La explotación de datos ha sido tradicionalmente una tarea intensiva en recursos humanos. En la actualidad, gracias al *big data*, al aprendizaje automático y a nuevas técnicas de análisis automatizado, es posible realizar explotaciones más rápidas de grandes volúmenes de datos, de modo que se detecan patrones ocultos y genera información que pueda servir a la elaboración de inteligencia en menor tiempo.

La inteligencia artificial ya permite realizar búsquedas inteligentes mediante lenguaje natural (NLP), elaborar resúmenes automáticos o incluso generar contenido directamente a partir de la información estructurada mediante sistemas de tipo RAG (*Retrieval-Augmented Generation*). Estas capacidades permiten al analista concentrarse en las tareas de validación, contraste y contextualización y deja a los algoritmos las funciones repetitivas de análisis primario.

El objetivo de esta fase sigue siendo el mismo: generar la información relevante, oportuna y adaptada al nivel de decisión, pero con un grado de automatización que acelere los procesos dentro de esta fase, mejore la trazabilidad y permita reaccionar con mayor agilidad ante escenarios en evolución.

7.5 Dissemination – *Difusión y uso de la información*

En esta fase, el objetivo es asegurar que la información y los datos lleguen al usuario adecuado, en el momento oportuno y en el formato más útil. Para lograrlo, es esencial contar con sistemas interoperables, redes seguras y una arquitectura basada en la filosofía del «dato único».

Herramientas como SAPIIEM permiten sincronizar los nodos ISR y garantizar la trazabilidad desde la necesidad hasta la difusión de la información. Al mismo tiempo, plataformas más recientes introducen productos

de inteligencia interactivos, adaptativos y reutilizables, que se ajustan dinámicamente al perfil del usuario y al contexto operativo.

La inteligencia artificial contribuye también en esta fase mediante funciones como la generación automática de resúmenes personalizados o la clasificación automática de productos según su propósito (planeamiento, *targeting*, operaciones). Estas capacidades ayudan a evitar la sobrecarga cognitiva del usuario y a asegurar que la información se entrega en condiciones óptimas para ser explotada.

7.6 Lecciones aprendidas y condiciones de éxito

Para aprovechar plenamente el potencial de las tecnologías emergentes aplicadas al proceso JISR, es fundamental combinar una estructura organizativa clara y flexible, personal, formado en herramientas ISR, procesos revisados y orientados a la automatización, y una cultura de interoperabilidad real entre niveles y dominios.

Ejercicios como el JFX-22, organizado por el Estado Mayor Conjunto (EMACON), han demostrado que estas condiciones no son solo teóricas. En ese contexto, se emplearon herramientas como SAPIIEM para gestionar el proceso IRM&CM y la explotación de la información. Los resultados evidenciaron una mejora sustancial en la trazabilidad, la coordinación entre niveles y la rapidez en la generación de productos útiles.

Asimismo, la suite ATENEA ha demostrado su potencial para integrar planeamiento, asignación y explotación en una única plataforma digital, aumenta la coherencia del proceso y facilita su adaptación a distintos escenarios. La formación anticipada de los operadores y la unificación de criterios doctrinales fueron elementos clave para su implementación eficaz durante los ejercicios.

Estas experiencias en ejercicios muestran que la transformación tecnológica del proceso JISR requiere tanto soluciones técnicas como cambios culturales y doctrinales, orientados a una explotación más eficaz de la información.

8 Interoperabilidad y filosofía del «dato único»

Uno de los desafíos principales del proceso JISR es asegurar que la información generada sea accesible, coherente y utilizable por todas las unidades y actores implicados en un entorno de operaciones conjuntas. En escenarios multidominio y en operaciones multinacionales, la interoperabilidad ha dejado de ser un ideal deseable para convertirse en una condición imprescindible.

Ningún sistema ISR opera hoy de forma aislada. La integración de capacidades nacionales, aliadas y comerciales requiere que sensores,

plataformas, sistemas de mando y herramientas de análisis compartan no solo datos, sino también formatos, protocolos y lenguajes comunes. Esto es especialmente crítico en el marco de operaciones OTAN o UE, donde el éxito depende de generar una imagen operativa común basada en inteligencia compartida y validada.

La interoperabilidad debe abordarse en tres niveles: técnico (*hardware*, *software* y conectividad), semántico (coherencia en la interpretación de datos) y organizativo (procesos y doctrina). La ausencia de interoperabilidad genera fragmentación, retrasos y pérdida de eficacia en la toma de decisiones.

En este contexto, la filosofía del dato único se convierte en un principio rector. Consiste en que un dato obtenido por un sensor, generado por un analista o producido por una IA, se registre una sola vez y quede disponible, de forma segura y trazable, para todos los usuarios autorizados. Este enfoque evita duplicidades, mejora la calidad del análisis y permite:

— Trazabilidad y control de versiones.

— Reducción de la carga sobre redes tácticas.

— Explotación cruzada mediante herramientas de IA.

— Coherencia y velocidad en el ciclo de decisión.

Su implementación exige arquitecturas distribuidas, redes seguras, normas técnicas comunes y una cultura organizacional basada en la necesidad de compartir, no solo en la necesidad de conocer.

La OTAN ha desarrollado estándares como el STANAG 4559, que regula el funcionamiento del *Coalition Shared Data* (CSD). Plataformas como INTEL-FS y BICES permiten compartir inteligencia de forma estructurada entre centros de análisis aliados.

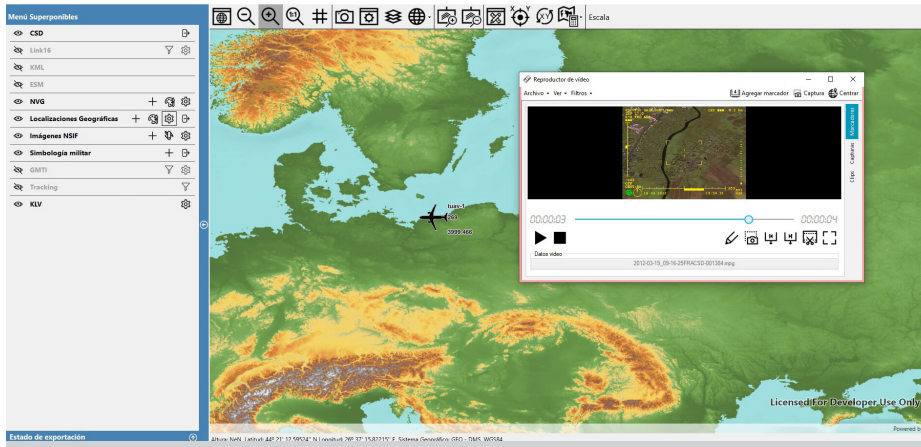


Figura 8. Sistema SEISMO de GMV

En el ámbito nacional, el sistema SAPIIEM ha demostrado su compatibilidad con estas estructuras internacionales, tanto en ejercicios conjuntos[10] como en operaciones reales. Estas infraestructuras permiten que el proceso JISR funcione de forma federada, de modo que aumente la eficacia colectiva y acelere la generación de inteligencia útil.

9 Innovación tecnológica como amenaza al proceso JISR

Hasta este punto, el capítulo ha expuesto las oportunidades que las tecnologías emergentes ofrecen para transformar el proceso JISR. Sin embargo, esa misma innovación tecnológica también genera nuevas vulnerabilidades que no pueden ser ignoradas. En muchos casos, las mismas herramientas que potencian la eficacia del sistema (IA, sensores inteligentes, automatización, computación en el borde) también amplían la superficie de exposición a riesgos operativos, cibernéticos o cognitivos.

En este apartado, se analizan dos de los aspectos más críticos en los que la innovación puede actuar como amenaza: la ciberseguridad del proceso JISR y las vulnerabilidades de la inteligencia artificial.

9,1 La importancia de la ciberseguridad en el Proceso JISR

La digitalización del proceso JISR ha multiplicado sus capacidades, pero también ha incrementado su exposición a amenazas cibernéticas. La incorporación de sensores distribuidos, redes de intercambio de información, plataformas diversas, herramientas de análisis automatizado y sistemas de mando y control interconectados ha convertido a los entornos ISR en un objetivo prioritario para actores hostiles. En este contexto, ya no se trata solo de proteger la infraestructura física, sino de asegurar la integridad, disponibilidad, trazabilidad y confidencialidad de la información a lo largo de todas las fases del ciclo.

El ecosistema JISR depende de una interconexión segura entre sensores, nodos de procesamiento, plataformas de explotación y usuarios finales. Cada uno de estos elementos puede convertirse en un vector de ataque. Por ejemplo, los sensores pueden ser objeto de suplantación o manipulación (*spoofing*), las redes pueden ser saturadas o intervenidas, los algoritmos pueden sufrir ataques mediante técnicas de *adversarial AI*[11] y los productos de inteligencia pueden ser interceptados o alterados durante su transmisión.

[10] Se ha mencionado previamente el JFX.

[11] *Science & Technology Trends 2023-2043*, volumen 2. Este documento describe el uso adversario de la inteligencia artificial y el aprendizaje automático como una colección de técnicas diseñadas para obstaculizar o engañar a los sistemas inteligentes, impactando sensores militares, sistemas de armas y sistemas de apoyo a la decisión.

Estas amenazas no son hipotéticas. En ejercicios y operaciones reales, se han identificado múltiples vectores de ataque: inserción de datos falsos, interceptación de flujos de información, denegación de servicio a plataformas ISR críticas o incluso alteraciones en la lógica de los sistemas de procesamiento automatizado. Todo ello pone de manifiesto que el entorno JISR debe ser activamente protegido frente a las ciberamenazas.

En contextos multinacionales, como los marcos OTAN o UE, el intercambio de información entre aliados exige especial atención a la seguridad de red, el cifrado, la autenticación y la trazabilidad. Un fallo en un solo nodo puede comprometer la seguridad de toda la red. Por ello, la interoperabilidad debe ir acompañada de garantías de ciberseguridad comunes, robustas y auditables.

La arquitectura de los procesos y sistemas JISR debe diseñarse desde el inicio bajo el principio de *security by design*[12] e integrar la ciberseguridad como parte estructural del sistema y no como un complemento posterior. Esto incluye controles de acceso, detección de intrusiones, auditoría de procesos, validación de datos y resiliencia ante fallos a lo largo de todo el ciclo.

Además, es fundamental reforzar la cultura de seguridad entre operadores, analistas y gestores del ciclo de inteligencia. El factor humano sigue siendo uno de los vectores de riesgo más relevantes, en especial, por errores involuntarios. La concienciación, la formación continua y los protocolos de buenas prácticas son elementos clave para mitigar estos riesgos.

Finalmente, el desarrollo de capacidades de ciberdefensa activa específicas para entornos JISR debe considerarse una línea de acción prioritaria. Esto incluye la protección dinámica de sensores y enlaces, la supervisión constante de plataformas de procesamiento y explotación y la capacidad de recuperación rápida ante incidentes. Todo ello requiere una estrecha colaboración entre responsables de ciberdefensa, desarrolladores de sistemas y analistas de inteligencia.

9.2 Sesgos y vulnerabilidades de la inteligencia artificial en el proceso JISR

El despliegue de tecnologías de inteligencia artificial en el proceso JISR promete una mejora sustancial en la velocidad, precisión y adaptabilidad de las operaciones. No obstante, esta transformación conlleva también nuevos riesgos operativos que deben ser considerados con rigor. Entre los más relevantes, destacan los sesgos algorítmicos, la opacidad de los modelos de decisión y la vulnerabilidad frente a manipulaciones o ataques cognitivos.

Uno de los desafíos clave es el sesgo de entrenamiento. Los modelos de IA utilizados para la clasificación de imágenes, la detección de amenazas o el análisis de comportamiento se entrenan con conjuntos de datos

[12] *Science & Technology Trends 2023-2043* – OTAN

previamente definidos. Si estos datos están incompletos, mal etiquetados o reflejan prejuicios históricos o contextuales, el sistema puede reproducir o amplificar errores, lo que genera falsos positivos o falsos negativos críticos en entornos operativos. Esto podría implicar decisiones erróneas, priorizaciones defectuosas o incluso consecuencias no deseadas.

Además, muchos modelos de aprendizaje profundo funcionan como «cajas negras», difíciles de auditar o explicar. Esta falta de transparencia afecta de forma directa a la confianza del mando en los sistemas automatizados, especialmente cuando las decisiones deben tomarse con rapidez y bajo alta presión.

Otro punto crítico es la vulnerabilidad a ataques adversarios. Existen técnicas (*adversarial AI*) capaces de manipular los resultados de un sistema de IA las cuales modifican mínimamente los datos de entrada (imágenes, señales, texto). Estas técnicas podrían utilizarse para confundir algoritmos y generar errores en la fase de explotación del proceso JISR. Este riesgo es, en especial, relevante en conflictos híbridos, donde actores hostiles pueden contar con capacidades cibernéticas sofisticadas.

La integración de IA en arquitecturas distribuidas, como *edge computing* o plataformas autónomas, amplía la superficie de exposición del sistema JISR a ciberataques o fallos sistémicos. La proliferación de sensores inteligentes y la automatización de procesos hacen que cualquier error no detectado en la IA pueda replicarse y escalar rápido en toda la red.

La inteligencia artificial puede ser un multiplicador de capacidades sin precedentes en el entorno JISR, pero solo si se gestiona de forma responsable. Frente a los riesgos mencionados, se hace imprescindible desarrollar e implementar soluciones de IA bajo principios de seguridad, explicabilidad y gobernanza robusta, de modo que se incorporen entre otras medidas como las siguientes:

- Validación continua de los datos de entrenamiento.
- Evaluación de sesgos y explicabilidad de modelos.
- Simulación de escenarios para robustecer los sistemas.
- Supervisión humana en decisiones críticas (*Human-in-the-loop* / *Human-on-the-loop*).
- Gobernanza de algoritmos bajo marcos normativos OTAN/UE.

10 Conclusión

Las innovaciones que derivan de las tecnologías emergentes y disruptivas, identificadas como prioritarias por la OTAN y la Unión Europea, están redefiniendo de forma transversal las capacidades militares, los ciclos de inteligencia y los procesos de toma de decisiones. Sensores inteligentes,

plataformas no tripuladas, *big data*, computación cuántica, materiales avanzados o tecnologías espaciales forman ya parte de un ecosistema ISR cada vez más interconectado, automatizado y distribuido.

Esta revolución tecnológica no afecta solo al plano técnico, sino también al doctrinal y organizativo. Las arquitecturas ISR deben adaptarse a un entorno en el que la información es abundante, diversa y generada desde múltiples fuentes, muchas de ellas fuera del ámbito militar tradicional. En este escenario, el proceso JISR se convierte en una capacidad continua, horizontal y multidominio, que debe ser capaz de operar en tiempo real y de integrar datos útiles desde el nivel táctico al estratégico.

Dentro de este conjunto, la inteligencia artificial se ha consolidado como el motor de cambio más inmediato, innovador y transformador. Su aplicación a lo largo de las fases del proceso TCPED permite automatizar la asignación de medios, elaborar planes dinámicos, anticipar amenazas, procesar grandes volúmenes de datos y proporcionar información de manera más rápida. La inteligencia artificial no sustituye al factor humano: lo ha de potenciar, liberándolo de tareas repetitivas y permitiéndole su enfoque en el análisis crítico, la validación y la toma de decisiones.

Esta transformación alcanza también a las plataformas, que se convierten además de sensores ISR avanzados, en elementos capaces de recolectar e incluso procesar información de manera previa en tiempo real. Su integración con sistemas de ciberdefensa, *targeting* o guerra electrónica refuerza la coherencia operativa y la eficacia en entornos complejos.

En este sentido, la arquitectura ISR del futuro deberá ser:

— Flexible, para adaptarse a escenarios cambiantes;

— interconectada, para integrar sensores y dominios;

— automatizada, para acelerar el ciclo de decisión;

— escalable y segura, para gestionar el volumen de datos y proteger su integridad.

Además, este ecosistema más conectado, automatizado e inteligente debe sustentarse en una estrategia de ciberseguridad transversal y adaptativa, que garantice la continuidad operativa y la protección de la ventaja informativa frente a amenazas sofisticadas y persistentes.

En definitiva, innovar en ISR es anticiparse, adaptarse y decidir con ventaja. El éxito no dependerá de quién obtenga más información, sino de quién sepa protegerla, compartirla, explotarla y convertirla en decisiones oportunas y acertadas más rápido y con mayor fiabilidad.

La transformación constante del proceso JISR no es solo un desafío tecnológico, es una necesidad estratégica ineludible.

Bibliografía

España. (2021). Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. *Boletín Oficial del Estado*. 31 de diciembre, núm. 314, pp. 167795-167830.

European Defence Agency. (2023a). *Enhancing EU military capabilities beyond 2040. Main findings from the 2023 Long-Term Assessment of the Capability Development Plan*. European Defence Agency (EDA). DOI: 10.2836/360180.

European Defence Agency. (2023b). *The 2023 EU Capability Development Priorities*. European Defence Agency (EDA).

Gómez Gómez, Juan de Dios. (2025). ESFAS. La inteligencia de comunicaciones contra el crimen organizado: un arma fundamental ante la amenaza híbrida. *Noticia IEEE 09/2025*. [Consulta 24 marzo 2025).

Gómez González, Á. S. (2021). Tendencias de evolución de la inteligencia militar. *Documento de Opinión IEEE 35/2021*. [Consulta: 5 febrero 2024).

Gordon B., D. Jr. (2023).The future of NATO C4ISR after Madrid summit. Assessment and Recommendations. NCI Agency. ISBN-13 978-1-61977-273-1.

Kerth, C., Klotz, P. y Essendorfer. (2019). *A new approach for information dissemination in distributed JISR coalitions*. Proc. SPIE 11015, Open architecture / Open Business Model Net-Centric Systems and Defense Transformations 2019. Fraunhofer IOSB. 110150N. [Consulta: 10 marzo 2025]. Disponible en: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/e23811eb-b3a6-432f-8250-64cc94c02b99/content

Kerth, C.; Klotz, P. y Essendorfer, B. (2020). *A new approach for information dissemination in distributed JISR coalitions*. Karlsruhe, Fraunhofer IOSB.

Ministry of Defence (UK). (2023). *Joint Doctrine Note 1/23 Intelligence, Surveillance and Reconnaissance*. Gov.uk. [Consulta: 2025]. Disponible en: https://www.gov.uk/government/publications/intelligence-surveillance-and-reconnaissance-jdn-123

NATO. (2022) *Strategic Concept for the Alliance at the Madrid Summit on 29 June 2022*. NATO.

NATO Science & Technology Organisation. (2023). *Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains*. Volume 1. NATO Science & Technology Organisation.

Pérez-Breva, L. (2018). Innovar: un manifiesto de acción. Deusto. ISBN 978-84-234-2933-2.

Sánchez Sánchez, J. L. (2025) Inteligencia artificial en apoyo a la inteligencia militar. Eje fundamental del éxito o fracaso en la competición estratégica entre grandes potencias. *Documento de Análisis IEEE 09/2025*. Ministerio de Defensa, Instituo Español de Estudios Estratégicos.

Adaptación de nuevas tecnologías en la comunidad JISR. Particularidades del ámbito marítimo

Alfonso Herrero Pita

Resumen

Hace décadas que las comunidades de inteligencia llevan adaptándose al nuevo paradigma introducido por la revolución de la información. Este proceso ha supuesto una alteración profunda de estructuras organizativas, lo que ha conectado y sincronizado entidades jerárquicamente dispersas como resultado de la necesidad de acceso instantáneo a la información, velocidad de flujos informativos y reducción de tiempos requeridos para su explotación.

La implantación de la capacidad JISR ejemplifica esta evolución de los órganos de inteligencia para adaptarse al escenario introducido por esta revolucionaria manera de interactuar con la información y suscita una profunda transformación en conceptos de operación, doctrina, organización, mando y control y adiestramiento.

Transformar los nuevos conceptos y estrategias JISR en una capacidad operacional real plena no es sencillo. La integración de herramientas conlleva un desafío para las estructuras organizativas objeto de su implantación.

Trasladar estos cambios a la conducción de operaciones ISR en el ámbito marítimo ofrece unas particularidades debido a la singular organización de una fuerza naval en un MCC (Mando Componente Marítimo), donde existen unos centros PED (Procesamiento, Explotación y Difusión), por lo general, con capacidades limitadas debido a la inherente restricción en el ancho de banda disponible.

Palabras clave

Acceso instantáneo, Estandarización, Interoperabilidad, Modelo de datos, Estructuras organizativas.

Adaptation of new technologies for the JISR community. Particularities of the maritime domain

Abstract

Intelligence communities have been adapting to the new paradigm introduced by the information revolution for decades. This process has

entailed a profound alteration of organizational structures, connecting and synchronizing hierarchically dispersed entities as a result of the need for instant access to information, speed of information flows and reduction of time required for its exploitation.

The implementation of the JISR capability exemplifies this evolution of intelligence agencies to adapt to the scenario introduced by this revolutionary way of interacting with information, causing a profound transformation in concepts of operation, doctrine, organization, command and control and training.

Transforming the new JISR concepts and strategies into a full-fledged operational capability is not simple. The integration of tools entails a challenge for the organizational structures targeted for implementation.

Translating these changes to the conduct of ISR operations in the maritime domain offers particularities due to the unique organization of a naval force in an MCC, where there are PED centers usually with limited capabilities due to the inherent restriction in available bandwidth.

Keywords

Instant access, Standardization, Interoperability, Data model, Organizational structures.

«[…] The naive view is wrong to believe that creating more powerful information technology will necessary result in a more truthful understanding of the world […]»

Yuval Noah Harari

1 La revolución de la información y la comunidad de inteligencia

Nada nuevo de dice ya al mencionar la profunda transformación que la llamada revolución de la información está causando en la forma de comunicarnos, trabajar y consumir productos y servicios. Esta transformación moldea cada aspecto del mundo en que se vive. Y la comunidad de inteligencia se encuentra justo en el centro de esa revolución, nada extraño puesto que trata casi exclusivamente con la obtención, el análisis y la difusión de información. La adaptación de los órganos de inteligencia para explotar las ventajas y oportunidades que esta revolución, iniciada hace ya décadas, está alterando profundamente su naturaleza organizativa.

2 Vectores de cambio

Se observa que el impacto organizativo en la comunidad de inteligencia está fundamentalmente impulsado por dos vectores de cambio:

1. El aumento exponencial del set de objetivos informativos; debido a la proliferación de grupos de personas y organizaciones que pueden operar y organizarse de forma eficiente al margen de Gobiernos nacionales. El acceso instantáneo a la información y su facilidad de explotación, lo que multiplica el número de actores en la escena mundial, causa la emergencia de unas motivaciones cada vez más difíciles de analizar. Como resultado, el desafío no es solo el incremento cuantitativo de potenciales amenazas, sino la creciente complejidad del entorno; una complejidad que demanda la exigencia de unos productos analíticos con aportaciones multidisciplinares.
2. Las nuevas tecnologías de información fomentan la implantación de herramientas de trabajo que implican una revolucionaria manera de interactuar con esta, resolver problemas e implementar soluciones. La velocidad de flujos de información y su accesibilidad instantánea estimulan un ecosistema de cambios que suscitan una profunda transformación en conceptos de operación, doctrina, organización, mando y control y adiestramiento. Una lección fundamental ha emergido tras años de adaptación: las nuevas tecnologías no pueden ser completamente explotadas si no existe, simultáneamente, una evolución de la organización, sus procesos y doctrina.

3 Adaptación de estructuras tradicionales

Se reconoce que muchos de los tópicos de la inteligencia de hoy en día son diferentes a aquellos que nos concernían años atrás, están modulados ahora por el acceso instantáneo, velocidad de flujos informativos y facilidad de explotación. Ello conlleva la adopción de nuevas tecnologías, cuyo proceso de implantación implica a menudo una «disrupción de jerarquías» y favorece redes descentralizadas sobre los modelos tradicionales de organización.

Los factores descritos llevan tiempo presionando con la necesidad de compartir información más rápido cruzando las fronteras administrativas tradicionales de unas burocracias de planificación centralizada y cadenas de mando jerarquizadas y organizadas verticalmente. Existen unas nociones de organización tradicional que han ido quedando obsoletas para ciertas funciones, fundamentalmente ese modelo tradicional donde los niveles inferiores reportan a los niveles superiores hasta que se alcanza el nivel superior apropiado de autoridad.

Nuevos esquemas organizativos se han ido implementando en los órganos de inteligencia desde hace décadas para unas burocracias entonces tradicionalmente estáticas, creadas en tiempos de información escasa, difícil de obtener y proporcionada en exclusiva por pocas entidades con aceptadas credenciales de autoridad. Para ilustrarlo, se recuerda la creación del SIFAS (Sistema de Inteligencia de las FAS) en 2012, uno de los hitos organizativos impulsados por el nuevo paradigma, en el que órganos que llevan a cabo cometidos de inteligencia sin estar incluidos necesariamente en la misma cadena de mando, establecen unas relaciones funcionales, de modo que proporcionan agilidad y flexibilidad al flujo tradicional de tareas/información del ciclo de inteligencia.

Uno de los ejemplos que más ilustran la adaptación de estructuras tradicionales de inteligencia a la revolución de la información es la implantación de la capacidad JISR (Inteligencia, vigilancia y reconocimiento conjunto). No obstante, esta adaptación está todavía lejos de plasmarse en una organización eficiente y es necesario un esfuerzo continuo en identificar desafíos y acometer una aproximación prudente a la hora de implementar los cambios necesarios derivados de estos.

4 JISR como paradigma de innovación

La implantación del proceso JISR en las FAS ejemplifica notablemente el proceso de adaptación de unas estructuras tradicionales preservadas durante décadas. Los modelos existentes tienden a romperse cuando surge la necesidad de compartir información más rápido, cruzando fronteras administrativas, donde se difuminan los límites entre etapas del ciclo de inteligencia tradicional: esto es, proporcionar al cliente información relevante y puntual mediante un proceso de dirección, obtención, procesamiento y difusión.

El nuevo entorno tecnológico proporciona una vasta capacidad para obtener y procesar información, lo que hace posible tomar las decisiones correctas, pero resulta irónico que el tiempo disponible para tomar tales decisiones se reduzca de forma drástica en muchos casos. JISR supone, en cierto modo, un cortocircuito en las etapas del proceso formal del ciclo de inteligencia cuando la información se necesita en tiempo real. El volumen de información disponible ha sufrido un ascenso exponencial en misiones ISR y el tiempo requerido para crear valor derivado de la explotación se ha reducido hasta segundos.

5 Desafíos en la adaptación tecnológica a la capacidad JISR

Pensemos en el proceso TCPED (Acrónimo en inglés de Dirección, Obtención, Procesamiento, Explotación y Difusión), este viene de la necesidad de un procedimiento soporte, suficientemente robusto y flexible, para unos sensores ISR en continua evolución tecnológica. El resultado de este proceso TCPED es un producto JISR. El proceso TCPED se ejecuta en la fase de dirección y obtención del ciclo de inteligencia tradicional y en todas las fases del ciclo de operaciones y *targeting*. Así el resultado JISR, derivado de una sola disciplina de obtención, es procesado con posterioridad en la fase de elaboración del ciclo tradicional de inteligencia.

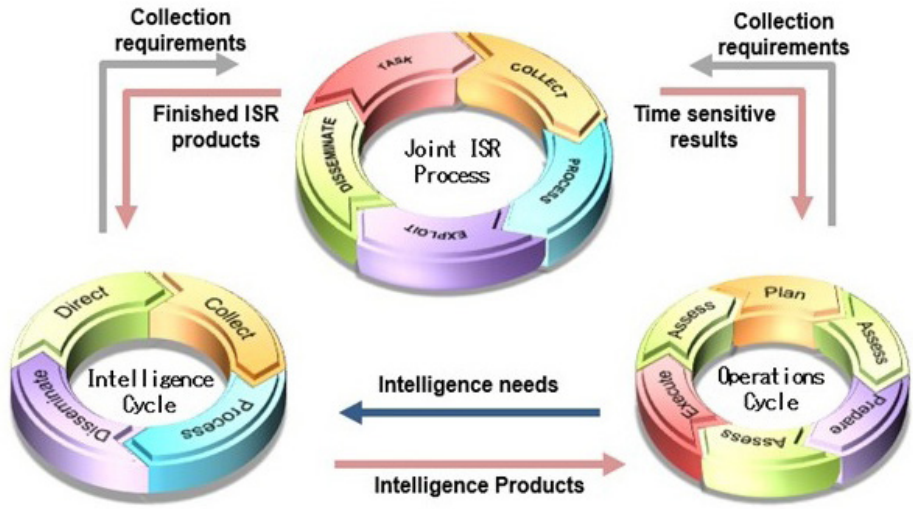


Figura 1. Presentación NCIA sistemas C4ISR

5.1 Entorno original

Llegados a este punto, se ve necesario explorar el contexto en el que se originó esta capacidad, el entorno que propició su surgimiento. Una descripción interesante de los inicios de la denominación PED se puede encontrar

con detalle en la publicación TCPED TACMEMO (EE. UU. Fleet Intelligence TCPED, febrero 2013). En esta, se menciona que los orígenes de la denominación PED se popularizó en los años noventa al surgir la necesidad de centros de procesamiento y explotación para una nueva generación de sensores montados en plataformas ISR aéreas en apoyo de fuerzas terrestres implicadas en operaciones antiterroristas y antiinsurgencia. La demanda de EO/IR/SAR/FMV en tiempo real y el desarrollo de sensores de altas capacidades, junto con el aumento creciente del ancho de banda disponible, propiciaron el concepto de unos centros de procesamiento de datos y explotación (PED) para proporcionar una rápida estimación a decisores que demandaban un tiempo crítico de explotación.

En definitiva, JISR nació de un contexto con unos requerimientos derivados de:

— Creciente velocidad y facilidad de acceso a la información.

— Amenazas/entorno operacional volátil.

— Necesidad de mecanismos que rápidamente asignen recursos allí donde sean necesarios.

— Necesidad de que los recursos fluyan de forma flexible y lo más libre posible dentro de una misma red de medios de obtención, analistas y directores donde las fronteras organizativas no pueden ser barreras. De hecho, uno de los principales desafíos para la integración de tecnologías ISR es la compatibilidad de sistemas y migración de datos, bases de datos compatibles e interoperabilidad de plataformas/medios de obtención con sistemas ISR.

— Un proceso que debe operar continuamente minimizando la distancia entre productores y consumidores de información y permitir una interacción rápida y necesaria que permita adaptar el producto a las necesidades del cliente.

— Información predominantemente EO/IR/SAR/FMV obtenida desde sensores montados sobre plataforma aérea.

Subrayo así ese entorno inicial de conducción de operaciones y soluciones ISR centradas, sobre todo, en sensores sobre plataforma aérea. De hecho, la doctrina conjunta actual es una evolución de la originada en el entorno del NATO AIRCOM (Mando Componente Aéreo de la OTAN). No obstante, su desarrollo tiende, en la actualidad, a diluir en cierta medida esa preeminencia del enfoque tradicional al incorporar un concepto más integrador, una aproximación que incorpora los dominios terrestre, marítimo, espacial y ciberespacial, además del aéreo tradicional. No obstante, como se ve más adelante, las diferentes versiones de herramientas a implementar son desarrollos de soluciones predominantemente *air centric*.

5.2 Herramientas tecnológicas para ISR, ¿ISR = I + SR?

A la hora de desvelar algunas claves sobre la dificultad que plantea la integración de nuevas tecnologías en las estructuras descritas por la Directiva del JEMAD 02/23, se estima de suma importancia abundar en el concepto JISR. Como ya se ha mencionado, el proceso JISR consta de cinco pasos secuenciales: planeamiento de tareas, obtención, tratamiento, explotación y difusión, conocido como proceso TCPED, que se desarrollan en las fases de dirección y obtención del ciclo de inteligencia.

Para el ISR Marítimo, el proceso TCPED es el proceso soporte de ISR; el reconocimiento (R) proporciona conocimiento del entorno (*awareness*) y la vigilancia (S) el contexto, de modo que son pasos secuenciales anteriores a la etapa de procesamiento del ciclo de inteligencia (I) y proporciona este una valoración. Es decir, el esfuerzo TCPED está limitado a proporcionar *awareness* y contexto correspondiente a una necesidad informativa (IR) de un comandante en el curso de una operación para apoyar un proceso de decisión; lo que proporciona datos e información (MISR – Maritime ISR) provenientes de una única disciplina de obtención (figura 2).

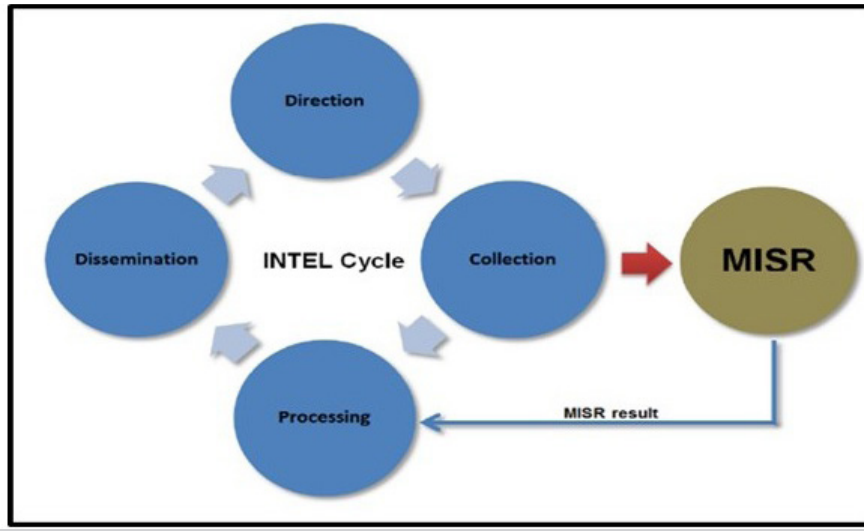


Figura 2. Ciclo de inteligencia y MISR

Creo importante enfatizar que la «I» de inteligencia, se refiere a un producto resultante de un proceso analítico alimentado por varias disciplinas de obtención (resultante de la fase de elaboración – processing). La etapa de elaboración es inherentemente más larga que las de vigilancia (S) y reconocimiento (R) y más amplia en fuentes de información y es el elemento cognitivo resultante una valoración (*assessment*). Esta etapa del ciclo de inteligencia, elaboración, utiliza técnicas de análisis, evaluación, integración

e interpretación que apoya la elaboración de productos de carácter predictivo, una finalidad por tanto diferente al resultado ISR del proceso TCPED.

Es decir, si bien el producto ISR es el resultado del proceso TCPED, el ciclo completo ISR incluye en cierto modo la «I» del ciclo de inteligencia al incorporar este resultado a su fase de elaboración. Esto tiene sus consecuencias a la hora de integrar el ciclo completo JISR en un set de sistemas y servicios compatibles e interoperables. Se observa, en principio, que las herramientas tecnológicas utilizadas en el proceso TCPED, orientadas a vigilancia (S) y reconocimiento (R) no tienen el mismo propósito que las de la fase de elaboración del ciclo tradicional (I). A mayor abundamiento, como se verá más adelante, las herramientas del proceso TCPED deben atenerse a estándares de interoperabilidad/modelo de datos muy complejos que implicarían gran dificultad hacerlos extensivos a las herramientas analíticas de la etapa del ciclo tradicional de inteligencia. Para ilustrar este aspecto, hay que pensar en la herramienta ROBIN, un sistema orientado para analistas en la etapa de elaboración del ciclo; pero cuya base de datos de inteligencia que lo alimenta no es compatible con los estándares JISR del STANAG 4559 (ver para 5.4) para el proceso TCPED.

5.3 El entorno marítimo

Como se ha mencionado, la doctrina JISR es el legado de esa demanda de información EO/IR/SAR/FMV en tiempo real proveniente de sensores con crecientes capacidades montados sobre plataformas aéreas; es decir, una doctrina que nació *air-centric* con periodos de ejecución siguiendo el ciclo del ATO (Air Tasking Order). El control centralizado es uno de los principios fundamentales de la doctrina actual JISR, un control que facilita la asignación de recursos en breve periodo de tiempo allí donde se necesitan.

Se considera la organización de una fuerza naval tipo. Se habla de la adaptación de una doctrina, con los consiguientes sistemas C4ISR (Acrónimo en inglés de Mando, Control, Comunicaciones, Ordenadores, Inteligencia, Vigilancia y Reconocimiento) asociados, a un modelo organizativo muy singular. A diferencia de un JFAC (Acrónimo en inglés de Mando Componente Aéreo), en el que prevalece la organización horizontal, en el MCC destaca la descomposición vertical con unos niveles de delegación de mando acordes a la necesaria descentralización y flexibilidad que requiere la fuerza naval. Se puede pensar, en principio, que las jerarquías con muchos niveles perjudican el flujo de información en el nuevo escenario tecnológico. Sin embargo, la planificación y conducción de operaciones navales tiende a ser descentralizada a través de toda una jerarquía de mandos. De hecho, el OTC (Officer in Táctical Command, Oficial de Mando Táctico) y CWC (Composite Warfare Commander, comandantes subordinados para áreas de guerra específicas) son construcciones únicas en la doctrina conjunta. Un CTF (Comandante de una Task Force) descompone su fuerza en TG, TU y TE (Task Groups,

Task Units y Task Elements) para ejercitar el control a nivel táctico y destaca el flujo de información horizontal entre mandos subordinados durante las misiones ISR, a los que se les otorga gran libertad de acción.

Por consiguiente, al considerar esos niveles de flujo horizontal de información, en el ámbito de una fuerza naval se pueden considerar tres niveles de conducción del proceso TCPED: nivel operacional, nivel táctico y nivel TF/TG; este último conducido por el estado mayor del MCC. De hecho, la publicación ATP 102 establece la segregación entre medios de obtención de una fuerza naval: «orgánicos y de teatro, dependiendo si son parte integral de las unidades y controladas por los comandantes a nivel táctico o aquellos que operan independientemente de la organización MCC o unidad y son dirigidos y coordinados a nivel joint en el ciclo JISR por el comandante operacional de la campaña».

Esta descomposición vertical de la organización de un MCC supone una dificultad adicional al considerar la integración de herramientas ISR en una red común de sistemas y servicios; de hecho, cabe preguntarse qué conjunto de sensores deben estar conectados para una misión en concreto. En el entorno marítimo cada plataforma es un sensor que idealmente debería estar integrado en una red común ISR en tiempo real de toda la fuerza, expandiendo el radio y la efectividad de los sensores en apoyo de esta. Para ilustrar esto, hay que considerar en enlace de datos de unidades por link-16. Se trata de una red TDL (*Tactical Data Link*) que permite generar y compartir SA (*Situational Awareness*) entre unidades muy dispersas sobre una red común de comunicaciones. La integración de datos compartidos en una red común JISR tiene sus implicaciones. Este caso, a modo de ejemplo, supondría, básicamente, pasar de un radioenlace encriptado a una red IP con unos requisitos para IRM & CM, explotación de sensores, bases de datos comunes con modelos estándar y una infraestructura de servicios y capacidades C2 (Mando y Control) y este entorno tecnológico para una fuerza con las inherentes restricciones de ancho de banda que tienen las unidades navales en la mar.

Cada disciplina de obtención tiene su ciclo TCPED; con diversos grados de disponibilidad, volumen de datos y capacidad de respuesta de los centros PED embarcados. Como se ha visto, estos centros PED, repartidos en una estructura vertical de una TF/TG tipo explicada con anterioridad, tienen una limitada capacidad de respuesta para acomodarse a un volumen creciente de datos. El planeamiento debe tener en cuenta, por tanto, que un indicador de buena obtención en el ámbito marítimo es evitar gran volumen de datos, pues van a ser explotados por unos centros PED normalmente con capacidades limitadas; «una mejor obtención no implica gran volumen de datos».

5.4 Estándares de Interoperabilidad. MAJIIC2. ¿Proyectos frustrados?

La capacidad JISR implica un ecosistema coherente de sensores, plataformas y centros de explotación integrados en una red común de

sistemas y servicios donde la interoperabilidad de estos es el factor clave para su funcionalidad. La interoperabilidad de todos los elementos implica la estandarización de datos, información, productos y flujo de tareas ISR. La directiva 04/23 de JEMAD establece sobre la arquitectura ISR «[...] deberá cumplir con los estándares y guías de implantación, así como responder a los procesos comunes de interoperabilidad recogidos en los STANAG aplicables de la OTAN y de la arquitectura MAJIIC2 (Multi-Intelligence All-Source Joint Intelligence Survillance and Reconnaissance Interoperability Coalition) [...] para asegurar la interoperabilidad con nuestros aliados [...]».

Creo necesario comentar algunos aspectos del proyecto MAJIIC2. El proyecto arrancó el año 2012 para «desarrollar estándares y tecnologías que permitieran a las fuerzas de una coalición, desde el nivel operacional hasta el táctico compartir y gestionar recursos y resultados ISR [...] promoviendo y facilitando el logro de objetivos tácticos y operacionales en el contexto de una operación». El proyecto adopta estándares de la OTAN para garantizar que datos y productos ISR sean compartidos e interpretados de manera correcta entre diferentes sistemas nacionales. El propósito es facilitar que la información generada por un sistema sea utilizada por otros al procesar formatos de datos y protocolos de comunicación comunes conforme los STANAG de la OTAN.

El STANAG 4559 establece los estándares clave para que diferentes naciones conduzcan operaciones ISR de forma colaborativa. Se está considerando un proyecto que lleva desarrollando modelos durante casi quince años y cabe preguntarse hasta qué punto existe actualmente una comunidad madura en la OTAN capaz de llevar a cabo actividades ISR rutinarias bajo estándares MAJIIC2 en su rango completo de aplicación (datos, productos y flujo de tareas). No se estima exagerado afirmar que el proyecto no ha cristalizado aún en una solución madura al no estar por completo operacionalizado en la OTAN, donde se viene observando la adopción de soluciones híbridas, esto es, sistemas solo compatibles en parte con los estándares MAJIIC2.

Se concluye, por tanto, que la directiva del JEMAD 04/23 establece un requisito de interoperabilidad respecto a unos estándares que han implicado el desarrollo de herramientas tecnológicas solo en parte operacionalizadas en la OTAN, después de más de una década de desarrollo.

5.5 Estándares de interoperabilidad; impacto organización (normalidad)

¿Qué desafíos persisten desde la primera directiva de JEMAD sobre la implantación de esta capacidad en 2012? ¿Cuál es el impacto en los órganos de inteligencia de esta adaptación tecnológica?

Considero que a la hora de valorar los retos en la implantación de la capacidad JISR, se hace imprescindible analizar las estructuras objetivo de esta integración. En concreto, el concepto de operación para las FAS descrito por la directiva 02/23 de JEMAD, establece que la capacidad JISR se desarrolla tanto en la estructura operativa como en la orgánica y aclara que la organización «contempla actividades ISR dentro de la estructura orgánica fuera del marco del planeamiento y conducción de las operaciones». Este requisito implica, por consiguiente, que las herramientas a implantar, diseñadas preeminentemente para apoyo del ciclo de operaciones y *targeting*, deberán ser, asimismo, funcionales en apoyo de la etapa de elaboración del ciclo de inteligencia (fig. 2) para satisfacer las necesidades informativas contenidas en el PROGINT (Programa de Inteligencia).

Estimo que la adopción de nuevas herramientas bajo los estándares MAJIIC2 en la estructura orgánica (por tanto, al margen de la conducción de operaciones), supone un considerable desafío organizativo que requiere previamente de un detallado concepto de operación para desvelar el entendimiento de cuáles son las necesidades operativas reales que impulsarían el cambio organizativo. Este cambio se aplicaría a estructuras que en la actualidad ya realizan su función en el ciclo de inteligencia tradicional (dirigida por el nivel estratégico, IRs —necesidades de información del PROGINT—). Esta expansión del ámbito de aplicación de JISR más allá de estructuras operativas dificulta las estrategias de aplicación de nuevas tecnologías a esta comunidad, al utilizar unas herramientas consistentes con MAGIIC2 —sometidas, por tanto, a sus rigideces— diseñadas para que su *output* se traduzca en acciones efectivas en un marco operacional o táctico, que no sería el caso de la mencionada estructura orgánica.

No se puede ignorar que la implementación del proceso JISR en unas estructuras fuera del marco del planeamiento y conducción de las operaciones (tiempo de normalidad) complica las estrategias de aplicación de estos proyectos tecnológicos innovadores, asociados a unas herramientas diseñadas con unos estándares para facilitar la interoperabilidad de una constelación de sensores, centros PED y decisores en una red común, enfocados a apoyar acciones con tiempos críticos de decisión durante una operación.

Se recuerda que, desde la evolución de la capacidad ISR en sus orígenes, el cliente preeminente ha sido el ciclo de targeting, y más en concreto, el *targeting* dinámico y TST (Time Sensitive Target) y las herramientas son diversos desarrollos de esta perspectiva inicial. En el caso que nos ocupa, los sistemas deben ser manejados por personal implicado en el ciclo de inteligencia en situación de normalidad (cadena orgánica), personal cuyos menesteres habituales consisten en la producción de inteligencia en apoyo a la preparación de la fuerza y como contribución a las ATII (Áreas y temas de interés de Inteligencia) formulados por el nivel estratégico. Esto puede

suponer una barrera significativa a la adopción de estas herramientas, debido a la inevitable resistencia cultural a abandonar los métodos tradicionales del ciclo de inteligencia (de naturaleza preeminentemente predictiva, resultado de la fase de elaboración —para 5.2.—). Se hace necesario, en este caso, un paquete coherente de concepto de operación y doctrina que precise y propicie la mejor contribución de todo el potencial de la organización en beneficio del nuevo paradigma introducido por JISR.

5.6 Estándares de interoperabilidad; impacto en operaciones caso del MCC

En el caso de conducción de operaciones, en el MCC, los escoltas suelen ser plataformas multirol y portan sensores con capacidades como, por ejemplo, ACINT (Inteligencia Acústica) y SIGINT (Inteligencia de Señales), con sus consiguientes sistemas de explotación asociados en apoyo de la acción táctica en ámbitos de la guerra naval como ASW, ASUW, AAW, EW (Anti Submarine Warfare, Anti Surface Warfare, Anti Air Warfare, Electronic Warfare)... Estos sistemas embarcados llevan aparejados módulos de explotación de nivel 1 (información en NRT – Nearly Real Time). En el ámbito JISR (operaciones *joint*), los datos, una vez procesados, deben estar disponibles para su explotación, ya sea abordo (normalmente, el mismo sistema de obtención lleva integrada la capacidad de explotación de nivel 1) o desde otro centro PED en otra unidad/base en tierra. Esto lleva de nuevo a los estándares de interoperabilidad. Este requisito impone una capa más de complejidad y la realidad puede derivar en la imposibilidad en muchos casos contar con bases de datos y protocolos estandarizados, algo que se debe tener en cuenta a la hora de planear el procesamiento de datos y distribución de centros PED en una operación conjunta con unidades navales.

Por ello, debe planificarse con precaución qué conjunto de sensores se deben integrar para una misión en concreto según los estándares establecidos de interoperabilidad JISR, teniendo en cuenta que esta integración no tiene por qué traducirse fácilmente en una organización más eficiente dado el diseño de una fuerza naval tipo explicado en el punto 5.3.

Por otra parte, es necesaria una red soporte robusta y flexible en un ambiente, el marítimo, necesariamente minimalista por el escaso ancho de banda disponible; con la consiguiente limitación de los centros PED para procesar altos volúmenes de datos, ignorar este hecho puede abrir la puerta a vulnerabilidades que comprometan la efectividad de la arquitectura ISR de la fuerza naval.

6 Conclusiones

La integración de nuevas herramientas tecnológicas conlleva un notable desafío para las estructuras organizativas existentes objeto de su

implantación, debido fundamentalmente a dos factores. El primero es el requisito clave para la funcionalidad JISR: la interoperabilidad, por tanto, estandarización de modelos de datos, flujos de información y procedimientos. El segundo, el hecho de extender la implantación del concepto a todo el espectro del conflicto, no solo a la conducción de operaciones sino también a la situación de plena normalidad.

El ámbito operativo de una fuerza naval ofrece unas particularidades debido a su singular organización, con una descomposición vertical de mandos y unidades en niveles de delegación acordes a la necesaria descentralización y flexibilidad que requiere el entorno marítimo. Este diseño del MCC propicia una arquitectura de sensores, centros PED y órganos IRM & CM que requiere de una cuidadosa planificación a la hora de determinar el nivel de integración de estos en la red común ISR para lograr una organización realmente efectiva. Asimismo, se debe tener en cuenta que se considera un entorno de conectividad limitada (disponibilidad de ancho de banda) y, por consiguiente, centros PED con capacidad restringida de explotación de datos.

Bibliografía

Alberts, D. S., Garstka, J. J. y Stein, F. P. (2005). *Network Centric Warfare. Developing and leveraging Information Superiority*. CCRP.

Berkowitz, B. D. y Goodman, A.E. (2012). Best Truth: Intelligence in the Information Age.

DOP-MAJIIC2-115. (2015). *MAJIIC2 JISR Interoperable Capabilities Concept within a Coalition Environment*.

TCPED TACMEMO. (2013). *EE. UU. Fleet Intelligence TCPED*.

Inteligencia narrativa en la era de la IA: análisis de la desinformación antiucraniana de Rusia

Viktoriia Romaniuk
Yevhen Fedchenko
Traducido al castellano por Tara Zielinski

Resumen

La Inteligencia Narrativa (NARINT) es una herramienta crucial para comprender y contrarrestar la guerra de información, especialmente, en el contexto de guerra de Rusia contra Ucrania desde 2014. Este estudio explora enfoques interdisciplinarios hacia NARINT e integra la ciencia cognitiva, la psicología y las comunicaciones estratégicas para descifrar cómo las narrativas influyen en la toma de decisiones y el comportamiento. También examina cómo Rusia utiliza narrativas de desinformación, amplificadas por inteligencia artificial (IA), para distorsionar las percepciones de Ucrania entre sus ciudadanos y los aliados occidentales. Los temas clave incluyen retratar a Ucrania como un Estado fallido o fascista, desacreditar al Gobierno ucraniano, socavar el apoyo militar y humanitario y distorsionar los lazos históricos de Ucrania con Rusia, así como su relación con la Unión Europea. El estudio enfatiza el papel de la IA en la amplificación de la desinformación, desde la creación automatizada de contenido hasta operaciones de influencia sofisticadas, como Doppelganger, destinadas a disminuir el apoyo occidental a Ucrania. La investigación analiza casos de StopFake, una destacada organización ucraniana de verificación de datos, para ilustrar las narrativas en evolución y sus estrategias de diseminación.

Palabras clave

Inteligencia narrativa, Comunicación estratégica, Desinformación, Inteligencia artificial, Deepfake.

Narrative Intelligence in the AI Era: Analysis of Russia's Anti-Ukrainian Disinformation

Abstract

Narrative Intelligence (NARINT) is a crucial tool for understanding and countering information warfare, especially in the context of Russia's ongoing conflict with Ukraine since 2014. This study explores interdisciplinary approaches to NARINT, integrating cognitive science,

psychology, and strategic communications to decode how narratives influence decision-making and behavior. It also examines how Russia utilizes disinformation narratives, amplified by artificial intelligence (AI), to distort perceptions of Ukraine among its citizens and Western allies. Key themes include portraying Ukraine as a failed or fascist state, discrediting the Ukrainian government, undermining military and humanitarian support, and distorting Ukraine's historical ties with Russia as well as its relationship with the European Union.The study emphasizes AI's role in amplifying disinformation, from automated content creation to sophisticated influence operations, such as Doppelganger, aimed at diminishing Western support for Ukraine. The research analyzes cases from StopFake, a leading Ukrainian fact-checking organization, to illustrate the evolving narratives and their dissemination strategies.

Keywords

Narrative intelligence, Strategic communication, Disinformation, Artificial intelligence, Deepfake.

1 Introducción

Los actores de la amenaza extranjera integran la Manipulación e Interferencia de Información Extranjera (FIMI[1], por sus siglas en inglés) dentro de un conjunto más amplio de herramientas de guerra híbrida, en gran medida por motivos geopolíticos y económicos (European External Action Service, 2025).

El tercer informe del Servicio Europeo de Acción Exterior (SEAS) sobre las amenazas del FIMI desvela la amplia infraestructura en línea utilizada por Rusia y China en sus actividades FIMI (European External Action Service, 2025). Esta infraestructura abarca múltiples plataformas y regiones geográficas, lo que enfatiza la escala y la complejidad de la amenaza FIMI hacia las democracias a nivel mundial.

La visión estratégica de Rusia para remodelar el sistema internacional promueve un nuevo orden global, en el que autoridad y la toma de decisiones pasan de la esfera euroatlántica a las fuerzas no occidentales en ascenso (y con una evidente naturaleza autocrática o dictatorial). Esa perspectiva procura posicionar a Rusia como un actor central en el mundo multipolar emergente, afirmar su influencia sobre la región Eurasia y realzar su posición global (Arroyo *et al*., 2023).

Al inmiscuirse en las crisis locales y regionales, el Kremlin pretende influir en la opinión pública y socavar la confianza en las instituciones estatales. En España, por ejemplo, como se ha mencionado en el Informe Anual de Seguridad Nacional elaborado por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, el Kremlin se valió de la dana para sembrar desconfianza en las instituciones democráticas españolas, deslegitimar el apoyo del país a Ucrania y transmitir una imagen internacional de caos (González, 2025).

Rusia ha empleado de forma estratégica operaciones de información a fin de aprovechar y ahondar las divisiones entre los Estados miembros de la OTAN (Stradinger, 2024).

Es imprescindible identificar los patrones clave —tal como los actores, las plataformas y las narrativas— a fin de detectar las vulnerabilidades, así como fortalecer la integridad del contexto de la información.

La Inteligencia de Narrativas (NARINT) es una herramienta poderosa en el ámbito de la guerra de la información. Las narrativas influyen considerablemente en los procesos decisorios al orientar las percepciones, explotar los sesgos cognitivos y activar los mecanismos psicológicos (Newby, 2024;

[1] *Foreign Information Manipulation and Interference* (FIMI).

Stradinger, 2024). Esto resulta particularmente evidente en el contexto de la guerra que opone Rusia a Ucrania.

La guerra entre Rusia y Ucrania, en curso desde 2014, ha marcado una nueva fase de confrontación híbrida compleja, en la que el armamento moderno se combina con el uso activo de las tecnologías de información. Los intentos de Rusia de influir en las relaciones de Ucrania con la Unión Europea (UE) mediante estrategias manipuladoras y destructivas es uno de los objetivos principales de esa lucha informativa (Churanova y Romaniuk, 2023: 39).

Según el tercer informe del SEAS sobre amenazas del FIMI, Ucrania sigue siendo el blanco principal: casi la mitad de los incidentes registrados (257) están relacionados con este país. Al mismo tiempo, las operaciones FIMI rusas se dirigen también al público occidental (incluso EE. UU., la OTAN, el G7 y los países de la UE, sobre todo, Alemania y Polonia) con el fin de debilitar el apoyo a Ucrania, tanto como elaborar una narrativa de la guerra en favor del Kremlin (European External Action Service, 2025).

Desde hace más de una década, Rusia ha desarrollado una serie de temas clave y ha divulgado de manera sistemática narrativas adaptadas a diversos acontecimientos políticos y militares. Pretenden distorsionar las percepciones de Ucrania, tanto entre sus ciudadanos como entre sus socios occidentales. Rusia modela la opinión pública e influye en las decisiones de sus líderes, de modo que emplea métodos de control reflexivos (Fedchenko, 2016: 141). En los últimos años, la desinformación rusa se ha adaptado rápido a las capacidades tecnológicas de vanguardia y ha explotado la IA para las operaciones de información. Esto permite una escalación más rápida de las campañas de desinformación, así como una manipulación más efectiva de la opinión pública a diferentes niveles.

A fin de contrarrestar eficazmente los fuertes ataques de desinformación por parte de la Federación de Rusia dirigidas a los países miembros de la OTAN, en especial a España, es primordial estudiar e implementar métodos modernos para detectar los formatos digitales de desinformación, analizar la lógica de su diseminación y entender las estrategias narrativas subyacentes a la influencia de la información.

Este estudio profundiza en los conceptos de narrativa y de la Inteligencia de Narrativas y se centra en su utilidad en la guerra de la información. Se presta especial atención a analizar las narrativas desinformativas rusas respecto a Ucrania y a identificar sus temas principales, sus estrategias de diseminación y sus impactos en diversas audiencias.

Esta investigación también examina las principales operaciones de información realizadas por Rusia, utiliza la IA y analiza cómo los algoritmos y los sistemas automatizados crean, transforman y amplifican las narrativas

desinformativas. Además, no se debe olvidar las tecnologías de *deepfake* emergentes y su papel en la producción masiva de contenido manipulador destinado a crear realidades distorsionadas, desacreditar a los ucranianos y las instituciones internacionales, y socavar la confianza en las fuentes de información fiables. Los casos analizados se basan en materiales de desacreditación de StopFake, una importante organización ucraniana de verificación de datos fundada en 2014.

2 Inteligencia de Narrativas: perspectivas interdisciplinarias y definiciones

El análisis de los temas y las narrativas perjudiciales que circulan en el espacio de información es un componente crucial de la lucha contra la desinformación y ha cobrado relevancia dentro del estudio del contenido, de la estructura y de sus efectos en las audiencias en diferentes contextos. Una perspectiva interdisciplinaria sobre la Inteligencia de Narrativas permite explorar cómo las estructuras narrativas conforman el pensamiento, la comunicación y la toma de decisiones en distintos campos. Dado que los desarrolladores de los sistemas avanzados de divulgación de información adoptan métodos multidisciplinarios para detectar y analizar las narrativas, entender sus principales fundamentos constituye una necesidad.

Rastreando el origen del concepto, el análisis de narrativas comenzó en los estudios literarios, centrándose en sus propiedades y su estructura. Por ejemplo, el trabajo de Vladimir Propp sobre la estructura del cuento folclórico (Propp, 1969) y estudios posteriores (Bruner, 1991) sentaron las bases para futuras investigaciones sobre la inteligencia artificial (Mateas y Sengers, 1998).

La psicología narrativa examina la conexión profunda entre la narrativa y la mente humana y enfatiza su papel central en conformar las emociones, las percepciones del mundo y el desarrollo personal. El psicólogo Jerome Bruner (1991) fomentó el avance en este campo argumentando que la narrativa es fundamental para el entendimiento del comportamiento intencional humano, puesto que los individuos interpretan acciones deliberadas a través de estructuras narrativas (Mateas y Sengers, 1998).

La influencia estructural de las narrativas sobre las audiencias es un elemento clave que se usa en la comunicación estratégica. Aquí, aparece el concepto de narrativa estratégica, una narrativa creada para influenciar un público, en la que se modifican, de forma deliberada, las percepciones de los acontecimientos y de las posiciones. Lawrence Freedman define a la narrativa estratégica como algo «creado o sostenido para estructurar las respuestas de los demás a acontecimientos en desarrollo»; estas narrativas son estratégicas en el sentido de que están elaboradas o reforzadas intencionalmente a partir de ideas y visiones ya existentes, en vez de surgir de manera espontánea (Blas, 2023).

En un contexto global, las narrativas estratégicas sirven como herramientas a través de las cuales los actores políticos tratan de forjar un conocimiento común del pasado, del presente y del futuro de la política internacional e influyen en el comportamiento de los actores nacionales e internacionales (Miskimmon *et al*., 2013). Dependiendo de la intención y del objetivo, las narrativas estratégicas pueden brindar apoyo a la democracia o bien convertirse en instrumentos de manipulación y de guerra híbrida.

Trabajar con narrativas en el contexto de lucha contra las amenazas informativas permite identificar los peligros que surgen de las campañas de desinformación, anticipar las potenciales consecuencias e implementar medidas para mitigar las pérdidas relacionadas con los ataques selectivos de la manipulación de información.

La Inteligencia de Narrativas se aplica para entender en detalle e interpretar los relatos específicos —narrativas— que circulan en el espacio de la información. En un sentido extenso, implica el reconocimiento de patrones básicos, temas y emociones fundamentales de las cuestiones clave vinculadas a procesos, personajes y fenómenos políticos e históricos (Baruchin, 2024). Permite detectar las tendencias inquietantes y estimar los riesgos potenciales. El concepto incorpora conocimientos de la ciencia cognitiva, de la lingüística, de la psicología social y de la comunicación estratégica para comprender cómo las narrativas influyen en las percepciones de la realidad, de la identidad y del comportamiento del público.

Una narrativa eficaz comprende: contar historias que interpreten situaciones a través de un tema específico, iniciar acciones que refuercen la narrativa y comunicar sobre esas acciones (Waldman y Havel, 2022). Los efectos narrativos principales, como descrito en *The Military Interest in Narrative* de Mark A. Finlayson y Steven R. Corman, incluyen varios aspectos fundamentales (Finlayson y Corman, 2013):

— Comprensión mejorada: las narrativas no solo mejoran la comprensión de informaciones específicas, sino que también fomentan la capacidad de los lectores y de los auditores con menos formación a absorber mejor las informaciones, lo que crea una conexión emocional con personajes que potencian el recuerdo a través de fuertes asociaciones emocionales (Griffey *et al*., 1988).

— Pensamiento narrativo específico: las narrativas poseen una racionalidad única, en la que la justificación de las acciones está determinada por la validez narrativa, de modo que incluye la coherencia (cómo la historia está articulada) y la fidelidad (cómo se alinea con otras historias conocidas), como mencionado por Fisher (1984).

— Generación de interpretación: las narrativas tienen un papel crucial en las relaciones sociales y aportan un marco que ayuda a entender

cómo los sujetos y los objetos interactúan y conectan en ciertas situaciones (Finlayson y Corman, 2013).

Marc A. Finlayson y Steven R. Corman (2013) identifican cuatro componentes básicos de la narrativa, abreviados PAIV[2] por sus siglas en inglés:

— Trama (ubicando la fase narrativa y anticipando su dirección).

— Arquetipos (predecibles, personajes estructuralmente opuestos implicados en la acción).

— Imágenes (creando situaciones tangibles para la audiencia).

— Significados (ideas realmente reforzadas o defendidas) (Finlayson y Corman, 2013).

Gregg Newby, al contrario, nota que las narrativas tienen poder, puesto que aportan una estructura coherente que permite a las personas asimilar informaciones complejas. Esta coherencia influencia la manera en la que los individuos interpretan informaciones y toman decisiones (Newby, 2024). Newby identifica varias razones por las que las narrativas afectan las tomas de decisiones:

— Marco: la forma en que se presenta la información puede influir mucho en las decisiones, ya que se pueden resaltar ciertos aspectos y minimizar otros, lo que lleva a conclusiones concretas.

— Anclaje: la exposición inicial a una narrativa marca un punto de referencia que orienta opiniones y decisiones posteriores. Esto es particularmente fundamental en la guerra de la información, donde el control de la narrativa inicial puede definir las percepciones.

— Repetición: una exposición repetida a la narrativa incrementa su credibilidad y su influencia, lo que refuerza el mensaje deseado e implanta creencias duraderas en la guerra de la información (Newby, 2024).

Los investigadores que estudian los mecanismos emocional-psicológicos de las narrativas procuran explicar por qué son eficaces.

Según Gregg Newby, los mecanismos psicológicos influencian de forma considerable la toma de decisiones más allá del análisis lógico. Entender estos mecanismos es esencial a fin de usar o contrarrestar de manera eficaz narrativas en la guerra de la información (Newby, 2024). Newby destaca:

— Compromiso emocional: los relatos que suscitan fuertes emociones (el miedo, el enfado, la empatía) pueden invalidar el pensamiento racional y son más memorables.

[2] *Plot, Archetypes, Imagery, Values* (PAIV).

— Identificación y empatía: relacionarse con personajes o situaciones aumenta la probabilidad de ser influenciado y refuerza la aceptación de los mensajes.

— Simplificación de la complejidad: las narraciones simplifican la información, lo que ayuda a la comprensión, pero puede orientar hacia generalizaciones o distorsiones mientras preserva el mensaje principal.

En el contexto de narrativas de desinformación, esto implica promover temas ideológicos tanto como manipular hechos, lo que amplifica las posiciones alineadas con los intereses de los que crean y difunden esa narrativa.

En los últimos años, con los avances en el campo de la IA, el análisis narrativo ha superado la narración tradicional, convirtiéndose en sustancial para los sistemas algorítmicos en la comunicación, los medios de comunicación masiva y la seguridad de la información. Waldman y Havel (2022) observan que las audiencias perciben las narraciones no mediante el análisis lógico de las afirmaciones, sino a través de una exposición repetida a relatos que las respaldan, como testimonios reales y personales (Waldman y Havel, 2022: 111-122). Este enfoque adquiere importancia a medida que las narraciones se transmiten a través de las redes sociales y otras plataformas, con un público que reacciona de manera más emocional que lógica. De este modo, no solo importan la estructura y el contenido de las narrativas, sino también el tipo de contenido, el género y el ecosistema de diseminación. Ciertos modelos narrativos tienen un papel clave en la creación de contenido capaz de influenciar las visiones del público. Crear contenido que transmite eficazmente un mensaje deseado a una audiencia objetivo es el aspecto más difícil de la comunicación narrativa.

En la era de la IA, estos ecosistemas son cada vez más complejos e integrados dado que los algoritmos pueden no solo proceder las narraciones, sino también predecir su eficacia en diferentes contextos, lo que altera fundamentalmente el paisaje de las campañas modernas de información.

3 Narrativas contra Ucrania

El análisis narrativo de la propaganda del Kremlin revela que las narrativas básicas y sus transformaciones estuvieron influenciadas por los acontecimientos y las necesidades del público meta. A partir de la base de datos de StopFake, una organización ucraniana de verificación de hechos, se realizó un análisis narrativo, en el que se identificaron variaciones en el enfoque del contenido, así como en las estrategias tecnológicas de diseminación.

En un artículo de 2016, *Kremlin Propaganda: Soviet Active Measures by Other*

Means, Yevhen Fedchenko, apoyándose en las investigaciones de StopFake, identificó dieciocho narrativas desinformativas rusas (Fedchenko, 2016: 141). Algunas de ellas reivindican «un golpe de Estado y una junta respaldada por el Occidente», «Ucrania como un Estado fascista», «Ucrania como un Estado fallido» y «Rusia no forma parte de la ocupación/de la guerra». Otras desacreditan a las Fuerzas Armadas de Ucrania y les representan como una amenaza, desacreditan a las personas desplazadas internamente (PDI) y a los refugiados, «predicen» la desintegración territorial de Ucrania a causa de «las reivindicaciones territoriales de los países vecinos» y fortalecen una «falsa legitimización de las anexiones de Crimea y de la ocupación del Donbás por los gobiernos extranjeros, las organizaciones internacionales y la prensa». Otros de los temas principales incluyen: la guerra en Ucrania en realidad no está dirigida por las Fuerzas Armadas de Ucrania sino «por EE. UU., la OTAN o contratadores privados», el «declive del apoyo occidental a Ucrania», las declaraciones de las organizaciones internacionales y «las relaciones entre Ucrania y la Unión Europea» (Fedchenko, 2016: 159).

Las interpretaciones históricas también desempeñan un papel importante en las técnicas de desinformación, en particular, en las narrativas sobre el papel de Rusia en la Segunda Guerra Mundial y su victoria, el legado soviético, el origen de Kyiv Rus' y el papel de Ucrania en ello, el concepto de «pueblos hermanos» y la deslegitimación de la lengua ucraniana.

En 2023, el equipo de StopFake volvió a analizar su base de datos de desmitificación a fin de identificar las narrativas principales contra Europa y Ucrania, difundidas por la desinformación rusa antes y después de la invasión a gran escala de Ucrania por Rusia en febrero de 2022 (Churanova y Romaniuk, 2023: 40). La lista de temas permaneció casi inalterada y muchos de ellos constituyeron la base de los discursos de Vladímir Putin, usándolos para justificar la invasión a gran escala a su inicio. Las principales reivindicaciones desinformativas comprenden: «Ucrania como un Estado fallido», el «declive del apoyo occidental a Ucrania», la falsa «legalización de las anexiones de Crimea y de la ocupación del Donbás», «la UE como agresor», «Ucrania como un Estado fascista» y «el declive y el fracaso de la UE». Desde la invasión a gran escala, el paisaje de las narrativas ha evolucionado. Los temas prominentes ahora incluyen también: el apoyo militar a Ucrania, los refugiados, Ucrania como una fuente de crisis económicas y ecológicas, «No a Ucrania en la OTAN» y «Ucrania está perdiendo la guerra». Además, los esfuerzos para desacreditar el liderazgo de Ucrania, así como cuestionar la legitimidad del presidente Zelenski, se han multiplicado.

Asimismo, el análisis narrativo identificó cambios en las técnicas de manipulación, focalizadas en los países más sujetos a la desinformación, y en las formas de diseminación (Churanova y Romaniuk, 2023: 40), lo que permitió determinar los objetivos de propaganda, las estrategias y las posibles consecuencias de la amenaza.

4 La inteligencia artificial y la promoción de narrativas contra Ucrania en las campañas de desinformación del Kremlin

Las herramientas basadas en la IA han pasado a ser fundamentales en la guerra de la información (Murphy, 2023). Los investigadores de las tecnologías emergentes y las amenazas de la información han pasado de predicciones futurísticas a estudios reales, dado que las campañas de información se adaptan de manera dinámica al perfil psicológico de las personas. El mensaje se ajusta en tiempo real a partir de las reacciones de la audiencia y las narrativas elaboradas automáticamente poseen un nivel de detalle y unos matices previamente exclusivos a la mente humana (Kereopa-Yorke, 2023).

El informe del Centro de Excelencia de las Estrategias de Comunicaciones de la OTAN, *AI in Precision Persuasion: Unveiling Tactics and Risks on Social Media*, revela que los avances en el campo de la IA han ampliado significativamente las capacidades en *marketing* digital. No obstante, algunos actores malintencionados explotan activamente estas mismas tecnologías para comunicaciones hostiles en las redes sociales, lo que corrobora previos estudios. Resulta esencial detectar y neutralizar esas campañas a fin de mitigar las amenazas relativas a la IA (Bergmanis-Korāts *et al*., 2024).

Desde la invasión a gran escala de Ucrania, Rusia ha multiplicado sus campañas de desinformación contra Ucrania y sus socios occidentales y ha usado tanto métodos tradicionales como innovaciones impulsadas por la IA.

En 2022, los analistas del EU DisinfoLab identificaron la existencia de una red de operaciones de información rusa denominada *Doppelganger*. Su estrategia implica la creación de múltiples «clones» de medios de comunicación auténticos, la imitación de por lo menos diecisiete plataformas, incluso *Bild*, *20minutes*, *Ansa*, *The Guardian* y la agencia de noticias ucraniana *RBC-Ukraine*. El objetivo es redireccionar los usuarios hacia artículos y vídeos manipulados y encuestas. Los perpetradores adquirieron decenas de nombres de dominios similares a unos legítimos y replicaron sus diseños gráficos (Alaphilippe *et al*., 2022). Más de cincuenta dominios albergaron alrededor de ochenta artículos de desinformación durante ese periodo, algunos de los cuales posiblemente se usaron con anterioridad o se reservaron para futuras operaciones. La operación *Doppelganger* fue planeada con el propósito de esparcir noticias falsas (*fake news)* mediante diversos recursos, por ejemplo, un vídeo manipulado (*Deepfake*) dentro de un artículo inventado que cita una encuesta de un medio clon y promocionado por

cuentas falsas en Facebook (Alaphilippe *et al*., 2022). Los investigadores de EU DisinfoLab mencionan que las páginas de Facebook fueron creadas de manera masiva durante periodos específicos, activadas para una sola campaña Doppelganger y luego abandonadas.

En un informe de Meta, el jefe de Seguridad de la Información Guy Rosen destacó dos campañas significativas de información Spamouflage (relacionada con China) y Doppelganger (conectada con Rusia) (Rosen, 2023). Rosen notó que las acciones de Meta contra Rusia se dirigieron a campañas perjudiciales datadas de 2017, lo que insinúa que Doppelganger puede haber sido parte de los preparativos de guerra a largo plazo (Rosen, 2023).

La operación Doppelganger se centró en imitar los medios de comunicación líderes y las páginas web de los Gobiernos a fin de diseminar artículos inventados con el objetivo de minar el apoyo a Ucrania. En un inicio dirigida a Francia, Alemania y Ucrania, la operación se extendió después a EE. UU. e Israel. La generación de contenido y su diseminación se basaron, en gran parte, en las tecnologías de IA.

En su informe *AI and Covert Influence Operations: Latest Trends*, OpenAI detalló el bloqueo de cuatro grupos de cuentas vinculadas a actores que apoyan la operación de influencia rusa Doppelganger. Cada grupo utilizó distintas tácticas, técnicas y procedimientos (TTP), método típico de las operaciones en las que intervienen varios grupos funcionales.

- Primer grupo: se centraba en comentarios breves en inglés, francés, alemán, italiano y polaco, publicados en 9GAG y X con memes, vídeos y enlaces —algunos de los cuales eran contenidos preexistentes en Internet—. Las cuentas de 9GAG usaban avatares de gatos o de personas famosas y se focalizaban en canales como *random*, mascotas, humor y citas. Los enlaces en relación con Ucrania y EE. UU. estaban generados por la IA mediante los modelos de OpenIA, con vídeos creados a partir de clips de noticias. Las publicaciones obtenían, por lo general, entre tres y cinco reacciones generadas (por ejemplo, «lol») de cuentas recién creadas y señaladas como *bots*. En X, las cuentas de baja actividad publicaban enlaces *spam* (por ejemplo, solarpanelfor[.]sale) que conducían a las páginas web Doppelganger.
- Segundo grupo: traducía artículos del ruso al inglés y el francés, los publicaba en la página web vinculada a Doppelganger rrn[.]media y generaba comentarios en las redes sociales.
- Tercer grupo: editaba artículos franceses y los publicaba en francee-teu[.]today, también vinculado a Doppelganger.
- Cuarto grupo: trabajaba en contenido para grenzezank[.]com y creaba publicaciones breves para un grupo y una página Facebook (OpenIA, 2024).

Las metas principales de Rusia en sus operaciones de influencia occidental son minar el apoyo internacional a Ucrania —especialmente la ayuda militar— y presionar a Ucrania para que lleguen a un acuerdo de paz según los términos del Kremlin, a saber, una capitulación. Otros de los objetivos comprenden promocionar narrativas políticas prorrusas e instigar conflictos internos en los países occidentales para debilitar su resolución a apoyar a Ucrania y a contraatacar a Rusia.

Las narrativas de Doppelganger se dirigen a Ucrania y su Gobierno, lo que atiza sentimientos contra el Occidente, Europa, la OTAN y Estados Unidos de América (sobre todo, fuera de EE. UU.) y exagera las dificultades económicas y las tensiones sociales a fin de amplificar las percepciones del conflicto (Chawryło, 2024). Los analistas del EU DisinfoLab mencionan que las narrativas de Doppelganger entran en dos categorías (Alaphilippe *et al*., 2022):

— «Ucrania como un Estado fallido»: enfatiza la corrupción del Gobierno y el nazismo de la sociedad, de modo que sugiere que incluso los ucranianos preferirían vivir en Rusia y cuestiona las inversiones de Europa en Ucrania.

— «El invierno está llegando»: las declaraciones de apoyo a Ucrania y las sanciones contra Rusia causan crisis económicas en Europa —de las penurias de gasolina a los déficits en pan, mantequilla y cerveza—. Los analistas de StopFake interpretaron esa escalación de narrativas como una herramienta para pintar a Ucrania como el culpable de la energía global y de las crisis económicas (Churanova y Romaniuk, 2023; Romaniuk, 2023: 40).

La operación empezó con encuestas ficticias en medios de comunicación clónicos, después utilizadas para producir vídeos de propaganda y artículos que imitan los medios de comunicación alemanes para la credibilidad. A modo de ejemplo, una encuesta en una página web clónica ucraniana preguntaba: «¿En qué país te gustaría vivir? Polonia, Ucrania o Rusia». Poco después, un vídeo manipulado bild[.]pics reivindicó que el 68 % de los ucranianos preferirían vivir en Rusia y justificó la debilidad percibida de Ucrania (Alaphilippe *et al*., 2022).

Estos ejemplos destacan la coordinación entre todos los recursos de Doppelganger. En los últimos años, el ecosistema de desinformación ruso se ha desarrollado más allá de los medios tradicionales, de modo que ha aprovechado los *chatbots* basados en la IA para generar y diseminar contenido (Châtelet y Lesplingart, 2025). La desinformación alcanzó su punto máximo antes de las elecciones al Parlamento Europeo, con Ucrania como tema central. Las investigaciones de NewsGuard expusieron la red de desinformación rusa Pravda, que manipulaba los datos de los *chatbots* basados en la IA con falsas alegaciones y propaganda. Su meta no es influenciar directamente a los humanos sino modificar los modelos de respuesta de la IA sobre ciertos sucesos (Sadeghi y Blachez, 2025).

Los analistas señalan que la red inunda los resultados de búsqueda y los rastreadores *web* con impostores a favor del Kremlin, lo que altera los resultados del gran modelo lingüístico. Según NewsGuard, esta «infección» de los *chatbots* occidentales fue propuesta durante una charla que John Mark Dougan, fugitivo estadounidense convertido en propagandista radicado en Moscú, dio en la capital rusa en una conferencia de las autoridades rusas, donde afirmó, «Al propagar esas narrativas rusas desde la perspectiva rusa, podemos realmente cambiar la IA a nivel mundial» (Sadeghi y Blachez, 2025).

En 2024, 3,6 millones de artículos de propaganda infiltraron los sistemas IA occidentales e incorporaroon ahí falsedades, desinformación y propaganda (Sadeghi y Blachez, 2025). NewsGuard evaluó diez *chatbots* de IA —ChatGPT-4o, el asistente inteligente You.com, Grok de xAI, Inflection Pi, Le Chat de Mistral, Copilot de Microsoft, Meta AI, Claude de Anthropic, Gemini de Google y el motor de respuesta Perplexity— y usó quince narrativas de 150 páginas web pro-Kremlin de Pravda (entre abril de 2022 y febrero de 2025) (Sadeghi y Blachez, 2025).

Según Sadeghi y Blachez (2025), los diez *chatbots* repitieron las desinformaciones de la red *Pravda* y 7 de ellos aún citaron directamente artículos específicos de Pravda como sus fuentes.

Los resultados de NewsGuard confirman que «la red Pravda fue probablemente pensada para manipular los modelos IA más que generar tráfico humano». La organización no lucrativa definió la táctica que afecta los grandes modelos lingüísticos como «el cuidado de los grandes modelos lingüísticos» (Sadeghi y Blachez, 2025).

Pravda no crea contenido original, sino que «blanquea» la propaganda del Kremlin y junta los medios de comunicación estatales, las personas influyentes pro-Kremlin y las fuentes del Gobierno mediante páginas *web* de apariencia independientes. Conocido como Portal Kombat, se estrenó en abril de 2022 después de la invasión y fue identificado por primera vez por la agencia francesa Viginum en febrero de 2024. Desde entonces se ha desarrollado en 49 países y extendido a 150 dominios (Viginum, 2024) (Sadeghi y Blachez, 2025). Viginum conecta Pravda a TigerWeb, una empresa de tecnologías de la información (TI) basada en Crimea bajo ocupación rusa, perteneciente a Yevhen Shevchenko, un desarrollador *web* que trabajaba antes en Krymtechnologii, que crea páginas web para las autoridades ocupantes rusas en Crimea (Viginum, 2024; Sadeghi y Blachez, 2025). Desde 2022, Pravda desarrolló páginas web dirigidas a los ucranianos que dominan el ruso e imitó el diseño del ecosistema de Pravda y su línea editorial. Creados entre abril y diciembre de 2022, esas páginas *web* seguían el formato «nombre de la ciudad + -news[.]ru», enfocándose en ubicaciones estratégicas como Jersón y Mariúpol (Viginum, 2024).

5 El *deepfake* como una forma de diseminar narrativas desinformativas

Más allá de su red de noticias manipuladas en expansión, se debe prestar especial atención a los tipos de contenido empleados por Rusia durante su invasión a gran escala. El contenido generado por la IA abarca tanto textos como fotos, audios y vídeos manipulados. El término *deepfake* (en español, «ultrafalso») está derivado de *deep learning* (en español, «aprendizaje profundo») y «fake» (en español, «falso»), describiendo vídeos fotorrealistas o imágenes creadas con la ayuda del *deep learning* (DL) (Rana *et al*., 2022).

El gran problema con los *deepfakes* es que la mayoría de los usuarios pueden carecer de las competencias necesarias para identificarlos o reconocer el engaño. Ha *et al*. (2024) encontraron que poco más de la mitad —60 %— de los internautas pueden discernir imágenes generadas por la IA (Ha *et al*., 2024). Rössler *et al*. (2018) mostraron que los usuarios identifican de forma correcta vídeos falsos en solo el 50 % del tiempo, parecido al *random guessing* (Rössler *et al*., 2018).

Una encuesta de Kantar Ukraine (febrero de 2024) reveló que el 79 % de los encuestados saben qué es la IA, pero el 42 % duda de sus capacidades de reconocer contenido de GenIA (Kantar, 2024). En tiempos de guerra, esas cifras resultan alarmantes. Pues la instrumentalización de los *deepfakes* en tiempos de guerra puede no solo conducir a un engaño del público y una distorsión de la realidad, sino también tener una amenaza existencial tanto para los militares como para los civiles, dado que cuentan a menudo con personalidades influyentes como líderes militares o civiles que toman decisiones importantes o dan órdenes importantes.

Los *deepfakes* emergen, por lo general, durante las crisis extremas donde la verificación es limitada y su difusión supera su desmitificación. Los pueblos son, en estos momentos, particularmente vulnerables y buscan respuestas inmediatas sin fuentes fiables. Las redes sociales, especialmente los canales anónimos rusos como Telegram, así como las páginas *web* creadas específicamente para la ocasión impulsan su propagación. Con una moderación mínima y una comunicación electrónica instantánea, Telegram es ideal para la manipulación y para los *infodumps* que influencian la opinión pública e incluso la dinámica del campo de batalla.

Tal contenido maximiza la promoción de narrativas críticas sobre el enemigo. Las narrativas eficaces creadas por los actores de desinformación se valen rápido de la actualidad y elaboran narrativas claras y fácil de entender, que conectan eventos con ideas determinadas, con personas reales y dinámicas como figuras principales que atraen la atención del público.

Un ejemplo es la operación «Matryoshka», en la que Rusia produjo vídeos fabricados, lo que representaba negativamente a los refugiados

ucranianos. En particular, un caso relacionado con un informe manipulado acerca de una joven refugiada ucraniana que estaba estudiando en EE. UU. El vídeo combina imágenes de la entrevista con escenas fingidas de pasillos escolares repletos, imágenes de drogas y una voz en *off* generada por la IA que denuncia unas «horribles condiciones de aprendizaje» en las escuelas estadounidenses. Incluyó retóricas racistas a partir de estereotipos a fin de provocar un sentimiento de hostilidad hacia la joven y los ucranianos en general entre los telespectadores estadounidenses.

La entrevista original, sin embargo, la presentaba avalando su experiencia en una escuela privada de EE. UU. y calificando como muy buena la educación estadounidense. Los *bots* amplificaron su divulgación en las redes sociales y llegaron a una audiencia muy amplia, según los investigadores de *Voice of America* (Kupfer y Vorozhko, 2025).

Esto ejemplifica una estructura narrativa clásica:

— Protagonista: una adolescente dinámica como personaje central de la narración.

— Experiencia personal: su presunta experiencia transmitida por medio de comentarios negativos e imágenes estereotípicas de una escuela problemática y problemas de drogas.

— Idea básica: representando la ingratitud y la arrogancia de una ucraniana hacia su país anfitrión. Esas manipulaciones tienen como propósito de descreditar a los refugiados ucranianos, retratándolos como *ungrateful troublemakers* (en español, «alborotadores ingratos»), para fomentar negatividad en los países anfitriones y cuestionar la ayuda a Ucrania (Kupfer y Vorozhko, 2025).

A fin de analizar la eficacia de las narrativas de propaganda promocionados a través de la IA, se examinarán varios *deepfakes* diseminados por la propaganda rusa durante la guerra en Ucrania, evaluando el contenido y la estructura de la construcción narrativa, el contexto político y las características técnicas de su detección.

5.1 Caso 1: Comandante en Jefe de las Fuerzas Armadas de Ucrania, el general Valerii Zaluzhnyi (2021-2024)

Contexto

Desde 2024, la propaganda rusa ha redoblado los ataques informativos sobre el liderazgo militar y civil de Ucrania y ha usado tecnologías de *deepfake*. Una de las narrativas principales señala la ilegitimidad del presidente Volodimir Zelenski, destinada a minar la confianza del público, así como a instigar un pánico derrotista.

Descripción del caso

Un vídeo circuló en línea mostrando a un hombre parecido al general Valerii Zaluzhnyi, Comandante en Jefe de las Fuerzas Armadas de Ucrania, afirmando que Zelenski «eliminó» a su ayudante de campo y está planeando entregar el país (StopFake, 2023). Se afirma en el vídeo:

> «Zelenski es el enemigo de nuestro Estado. Por su culpa, hemos fracasado completamente en la contraofensiva. Hago un llamado a las plazas (Maidán) y a todos los defensores de Ucrania a desobedecer las órdenes criminales de sus comandantes. Deponed inmediatamente las armas (contra el liderazgo ucraniano) y marchad sobre Kiev».

Este *deepfake* de gran calidad, creado con la IA, superpone imágenes y audios manipulados sobre imágenes existentes y utiliza las redes generativas antagónicas (GAN[3] por sus siglas en inglés), lo que modifica tanto lo visual como la voz. Herramientas como *Deepware*, usado por los verificadores de información, detectaron signos de procesamiento artificial. Según los expertos del Centro para la Lucha contra la Desinformación (Ucrania), el vídeo se divulgó primariamente a través de canales anónimos en Telegram y de grupos pro-Rusia, publicado primero por Radio Trukha, un canal autodenominado como humorístico (StopFake, 2023).

Análisis narrativo

Este caso presenta elementos de la narrativa de propaganda narrativa:

- Comunicador fidedigno: el general Zaluzhnyi, quien servía de Comandante en Jefe de las Fuerzas Armadas de Ucrania (desde el 27 de julio de 2021 hasta el 8 de febrero de 2024), es muy fiable (al 70,9 % según *Active Group*, 2024), confiere credibilidad.
- Mensaje emocional: suscita el miedo, la traición y la desesperación y amplifica el pánico.
- Mensaje desacreditador: acusa a Zelenski de deslealtad y de rendición, lo que insinúa una fisura entre el liderazgo militar y estatal.
- Contexto político: la narrativa «Zelenski es un líder ilegitimo» impulsa los esfuerzos rusos a descreditar el Gobierno ucraniano y la confianza en sus instituciones. El Centro para la Lucha contra la Desinformación de Ucrania considera que tales falsedades forman parte de las operaciones psicológicas para incitar al pánico y a la división en la sociedad ucraniana (Center for Countering Disinformation, 2023). Los cinco años del mandato presidencial de Zelenski terminaron en mayo de 2024, pero las elecciones en Ucrania fueron aplazadas bajo la Ley Marcial según el Artículo 19 de la Ley Marcial, con su ejercicio extendido hasta su final. Un memorando de la Rada en noviembre de 2023 fijó que las

[3] *Generative Adversarial Networks* (GANs).

elecciones se celebrarán seis meses después de la finalización de la Ley Marcial, ya que la votación en tiempos de guerra es inviable.

5.2 Caso 2: Comandante en Jefe de las Fuerzas Armadas de Ucrania, Oleksandr Syrskyi

Descripción del vídeo manipulado

Un vídeo se divulgó en las redes sociales ucranianas y mostraba a una figura que parecía ser el coronel general Oleksandr Syrskyi, Comandante de las Fuerzas Terrestres en ese momento, que urgía a las tropas a rendirse, de modo que afirmaba que la situación en el frente favorecía a Rusia y que resistir era inútil:

> «Yo, el coronel general Oleksandr Syrskyi, quiero decir la verdad. Ha llegado el momento de admitirla. Nosotros, con Shoigu y Gerasimov [el Ministro de la Defensa rusa y el Jefe de Gabinete de la Fuerzas Armadas de Rusia en ese momento], estamos negociando con los rusos para acabar esta guerra fratricida. A los soldados y los oficiales: si los rusos ofrecen rendirse, rendíos. La palabra de un oficial ruso es fiable; son nuestro pueblo hermano».

Estructura narrativa

- Comunicador fidedigno: la gran confianza de Syrskyi como Comandante refuerza el peso del vídeo manipulado.
- Mensaje emocional: sugiere que la guerra está perdida, bajando el ánimo a resistir.
- Ideas ideológicas: promueve la rendición, la confianza en los rusos y la narrativa de «los pueblos hermanos».
- Arquetipo del «pueblo hermano»: vincula a los ucranianos con los rusos, basado en una ideología soviética imperial que niega la identidad nacional y la condición de nación de Ucrania. Según este enfoque, Ucrania no puede tener su propia independencia y forma parte del «mundo ruso». Esto refuerza la desinformación rusa y justifica la ocupación.

Análisis técnico

El vídeo presenta señales típicas de *deepfake* —movimientos oculares poco naturales y anomalidades en el mentón— que indican manipulación mediante IA.

Contexto

El concepto de «pueblos hermanos» justificó históricamente la dominación rusa y presentó a los ucranianos como «hermanos menores» dependientes. Niega la condición de nación de Ucrania y se alinea con la propaganda moderna de guerra (Ukrainian Institute of National Memory, 2023).

5.3 Caso 3: Michael O'Flaherty, Alto Comisionado de Derechos Humanos del Consejo de Europa

Descripción del caso

Un vídeo que circuló en las redes sociales ucranianas y en Telegram muestra, supuestamente, al Alto Comisionado del Consejo de Europa Michael O'Flaherty criticando a Ucrania por la «vigilancia lingüística» (medidas públicas para ejecutar leyes sobre el idioma en los servicios). El vídeo denuncia que esas «vigilancias» violan los derechos de las minorías, urgiendo a los líderes ucranianos a poner fin al «desorden» y lo presentaba como pruebas del aumento de las críticas de las instituciones de Europa hacia el «nazismo» ucraniano. Texto del supuesto discurso de Michael O'Flaherty:

> «Existen varias minorías lingüísticas en Ucrania, como las comunidades húngaras, romanas y búlgaras entre otras, y estamos recibiendo pruebas de la violación de los derechos humanos contra esas personas. El Consejo de Europa considera que se trata de uno de los problemas de derechos humanos más graves de nuestro continente. Esas presuntas vigilancias lingüísticas organizadas por el Gobierno ucraniano garantizan que no se hable otra lengua que la mayoritaria en el territorio ucraniano. Debemos colaborar mucho mejor con los lideres de Europa a fin de reducir este escandaloso nivel de desigualdad lingüística entre las minorías nacionales y la población de Ucrania en general, además de combatir el crecimiento del odio nacionalista. Hago un llamado a los funcionarios ucranianos y al presidente Zelenski para que detengan esta persecución por motivos políticos y respeten los principios de la Declaración Universal de los Derechos Humanos, la Carta Europea de las Lenguas Regionales o Minoritarias y la Constitución de Ucrania. Un país que intenta convertirse en un miembro igualitario de la comunidad europea no puede violar los derechos humanos fundamentales».

Análisis técnico

Los verificadores de hechos StopFake, después de un análisis profundo usando *Attestiv*, confirmaron la falsedad del vídeo. Las señales incluyen un fugaz «doble mentón» y movimientos faciales antinaturales —un parpadeo mínimo y una desincronización entre los labios y el discurso— lo que indica una manipulación por medio de la IA (StopFake, 2024).

Vídeo original

En realidad, la falsificación reutilizó un extracto vídeo del Consejo de Europa en el que el Alto Comisionado Michael O'Flaherty habla de mejorar la vida de las minorías en Europa, sin mencionar los problemas lingüísticos ni de las vigilancias lingüísticas en Ucrania. Los gestos y la ropa corresponden, pero el contenido difiere (StopFake, 2024).

Narrativas del problema lingüístico y la desinformación rusa

Rusia usa la lengua como una herramienta manipulativa, lo que alega que Ucrania oprime a las minorías mediante imposiciones lingüísticas, de modo que desacredita los esfuerzos de protección del ucraniano como lengua de Estado, y recurre a narrativas inventadas sobre violación de derechos.

Estructura narrativa

- Comunicador fidedigno: la posición internacional de O'Flaherty confiere credibilidad.
- Tonalidad emocional: enfatiza la violación de los derechos de las minorías, un tema delicado, representando a Ucrania como infractora de las normas.
- Narrativa básica: «Ucrania viola los derechos de las minorías por medio de vigilancias».

Contexto

La desinformación rusa incluye distorsiones históricas como negar la legitimidad de la lengua ucraniana y acusaciones de opresión a las minorías. Reivindicaron sus invasiones a la Crimea y el Donbás justificándose con el argumento de proteger los «derechos de los rusohablantes». La ley de 2019 sobre el idioma ucraniano, efectiva a partir del 16 de julio, ordenó el uso del ucraniano en la esfera pública, con cambios en el servicio (2021) y en la cultura/el turismo (julio de 2021), además de requisitos en la prensa escrita desde enero de 2022 (Law of Ukraine, 2019).

6 Conclusiones

La Inteligencia de Narrativas (NARINT) es un método interdisciplinario que integra la ciencia cognitiva, la lingüística, la psicología social, la comunicación estratégica y la tecnología moderna. Tiene un vasto potencial para el análisis de amenazas —especialmente militares— y para desarrollar estrategias de comunicación eficaces.

Trabajar con narrativas es primordial en la guerra de la información del Kremlin contra Ucrania, la OTAN y los países occidentales.

La desinformación rusa lleva mucho tiempo construyendo narrativas estructuradas con el fin de moldear las percepciones sobre los sucesos históricos, sociales y políticos ucranianos, reinterpretando la realidad, los hechos históricos, la presión psicológica y los procesos de autoidentificación —herramientas clave en la manipulación informativa global—.

Las campañas rusas se valen de la IA y de la tecnología para adaptar y propagar digitalmente narrativas contra Ucrania. Al usar *deepfake* y

contenido en masa, el Kremlin refina su propaganda para debilitar el apoyo global destinado a Ucrania y lograr victorias en la guerra híbrida. La IA permite una adaptación rápida a diversos contextos y públicos, amplica el temor local, la incertidumbre económica y la polarización, impone interpretaciones positivas y simula cambios en los sentimientos «orgánicos». Las operaciones impulsadas por la IA exigen nuevos métodos de detección y de lucha, como el análisis sistemático de las narrativas para rastrear la evolución de la propaganda y de sus canales de diseminación.

Luchar contra las amenazas de información sigue siendo una prioridad esencial en Europa y requiere una adaptación permanente y una cooperación global para proteger la democracia y un espacio de información libre y abierto (European External Action Service, 2025).

Las contramedidas activas deberían incluir:

— Desarrollo de la OSINT (Inteligencia de Fuentes Abiertas): crucial para entender la orientación del público con narrativas amenazadoras, que reflejen sus visiones del mundo, sus valores y sus aspiraciones. Implica identificar las personalidades influyentes que difunden falsedades y mapear las redes de diseminación.

— Análisis de la red de influencia: detecta los canales principales de desinformación y su vínculo con otros medios más débiles que introducen nuevo contenido desinformativo o bien que refuerza narrativas a través de personas u organizaciones confiables o con un cierto impacto mediático.

Este estudio revela una hábil integración de la estructura narrativa clásica en la propaganda por medio de herramientas impulsadas por la IA como los *deepfakes* y contenidos generados. Recurrir a los desarrolladores de IA es fundamental para comprender las formas y las escalas de influencia.

Bibliografía

Active Group. (2024). *Public and political moods of Ukrainians (December 2024)* [en línea]. [Consulta: 29 marzo 2025]. Disponible en: https://activegroup.com.ua/wp-content/uploads/2024/12/241210_december.pdf

Alaphilippe, A., Machado, G., Miguel, R. y Poldi, F. (2022). *Doppelganger: Media clones serving Russian propaganda* [en línea]. EU DisinfoLab. [Consulta: 29 marzo 2025]. Disponible en: https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf

Arroyo, D., Valencia, J. y Galán Cordero, C. (2023). From disinformation to cognitive warfare: Russian and Iranian techniques, tactics and procedures in the design and deployment of hybrid threats. En: Catalán

Matamoros, D. (eds.). *Disinformation and fact-checking in contemporary society* Madrid, Dykinson, pp. 79-101. [Consulta: 29 marzo 2025]. Disponible en: https://www.dykinson.com/libros/disinformation-and-fact-checking-in-contemporary-society/9788411707107/

Baruchin, R. (2024). Narrative Intelligence: The Number One Tool Against Disinformation. *Cyabra*. [Consulta: 29 marzo 2025]. Disponible en: https://cyabra.com/blog/what-is-narative-intelligence/

Bergmanis-Korāts, G., Haiduchyk, T. y Shevtsov, A. (2024). *AI in Precision Persuasion. Unveiling Tactics and Risks on Social Media* [en línea]. NATO Strategic Communications Centre of Excellence. [Consulta: 29 marzo 2025]. Disponible en: https://stratcomcoe.org/publications/ai-in-precision-persuasion-unveiling-tactics-and-risks-on-social-media/309

Blas, N. (2023). Beyond Storytelling: Strategic Narratives in Military Strategy. *Æther: A Journal of Strategic Airpower & Spacepower*. 2(1), pp. 46-57. [Consulta: 2025]. Disponible en: https://www.jstor.org/stable/48714686

Bruner, J. (1991). The Narrative Construction of Reality. *Critical Inquiry*. 18(1), pp. 1-21. [Consulta: 29 marzo 2025]. Disponible en: https://www.journals.uchicago.edu/doi/abs/10.1086/448619

Center for Countering Disinformation. (2023). *Why does Russian propaganda use a deepfake of V. Zaluzhny?* [en línea]. Center for Countering Disinformation under the National Security and Defense Council of Ukraine. [Consulta: 29 marzo 2025]. Disponible en: https://cpd.gov.ua/articles/dlya-chogo-rosijska-propaganda-vykorystovuye-dipfejk-v-zaluzhnogo/

Chawryło, K. (2024). Doppelgänger: The pattern of Russia's anti-Western influence operation. Centre for Eastern Studies (OSW). [Consulta: 29 marzo 2025]. Disponible en: https://www.osw.waw.pl/en/publikacje/analyses/2024-09-13/doppelganger-pattern-russias-anti-western-influence-operation

Churanova, O. y Romaniuk, V. (2023). Anti-EU narratives through the Russian-Ukrainian war in the light of StopFake.org's debunks. En: D. Catalán Matamoros, D. (ed.). *Disinformation and fact-checking in contemporary society*. Madrid, Dykinson, pp. 39-61. [Consulta: 29 marzo 2025]. Disponible en: https://www.dykinson.com/libros/disinformation-and-fact-checking-in-contemporary-society/9788411707107/

Châtelet, V. y Lesplingart, A. (2025). Russia's so-called «Pravda» network expands worldwide. DFRLab. [Consulta: 29

marzo 2025]. Disponible en: https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/

Fedchenko, Y. (2016). Kremlin propaganda: Soviet active measures by other means. *Sõjateadlane (Estonian Journal of Military Studies)*. 2, pp. 141-171. [Consulta: 29 marzo 2025]. Disponible en: https://ojs.utlib.ee/index.php/st/article/view/23975/18184

Finlayson, M. A. y Corman, S. R. (2013). The military interest in narrative. Sprache und Datenverarbeitung. *Sprache und Datenverarbeitung*. 37(2), pp. 173-191. [Consulta: 29 marzo 2025]. Disponible en: https://users.cs.fiu.edu/~markaf/doc/j2.finlayson.2013.sdv.37.173_archival.pdf

Fisher, W. R. (1984). Narration as a human communication paradigm: The case of public moral argument. *Communication Monographs*. 51, pp. 1-22. [Consulta: 29 marzo 2025]. Disponible en: https://doi.org/10.1080/03637758409390180

González, M. (2025). El informe de Seguridad Nacional atribuye a Rusia campañas desestabilizadoras de desinformación por la dana. El País. [Consulta: 29 marzo 2025]. Disponible en: https://elpais.com/espana/2025-05-22/el-informe-de-seguridad-nacional-atribuye-a-rusia-campanas-de-desinformacion-por-la-dana.html

Griffey, Q. L., Zigmond, N. y Leinhardt, G. (1988). The effects of self-questioning and story structure training on the reading comprehension of poor readers. *Learning Disabilities Research*. 4(1), pp. 45-51.

Ha, A. Y., Passananti, J., Bhaskar, R., Shan, S., Southen, R., Zheng, H. y Zhao, B. Y. (2024). Organic or diffused: Can we distinguish human art from AI-generated images? En: *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS 24')*. ACM. [Consulta: 29 marzo 2025]. Disponible en: https://doi.org/10.1145/3658644.3670306

Kantar. (2024). Art or entertainment: Ukrainians' attitude towards GenAI. Kantar. [Consulta: 29 marzo 2025]. Disponible en: https://www.kantar.com/ua/inspiration/advertising-media/ukrainians-about-genai

Kereopa-Yorke, B. (2023). ClausewitzGPT framework: A new frontier in theoretical large language model enhanced information operations. UNSW Canberra at the Australian Defence Force Academy. [Consulta: 29 marzo 2025]. Disponible en: https://arxiv.org/abs/2310.07099

Kupfer, M. y Vorozhko, T. (2025). Russia uses deepfakes against Ukrainian refugees. *Voice of America*. [Consulta: 29 marzo 2025].

Disponible en: https://www.golosameriki.com/a/russia-uses-deep-fakes-against-ukrainian-refugees/7953485.html

Ucrania. (2019). Law of Ukraine on ensuring the functioning of the Ukrainian language as the state language. *Verkhovna Rada of Ukraine* (VVR). N.º 21, Artículo 81. [Consulta: 29 marzo 2025]. Disponible en: https://zakon.rada.gov.ua/laws/show/2704-19#Text

Mateas, M. y Sengers, P. (1998). Narrative Intelligence. American Association for Artificial Intelligence. [Consulta: 29 marzo 2025]. Disponible en: https://www.cs.cmu.edu/~michaelm/nidocs/MateasSengers.pdf

Miskimmon, A., O'Loughlin, B. y Roselle, L. (2013). *Strategic Narratives: Communication Power and the New World Order*. London, Routledge.

Murphy, B. (2023). *Foreign disinformation in America and the U.S. government's ethical obligations to respond*. Cham, Springer Nature.

Newby, G. (2024). The Synergy of OSINT and Narrative Intelligence. Edgetheory. [Consulta: 29 marzo 2025]. Disponible en: https://edgetheory.com/resources/osint-and-narrative-intelligence

OpenIA. (2024). *AI and covert influence operations: Latest trends*. OpenIA. [Consulta: 29 marzo 2025]. Disponible en: https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf

Rana, M. S., Nobi, M. N., Murali, B. y Sung, A. H. (2022). Deepfake detection: A systematic literature review. *IEEE Access*.

¿Qué significa el crecimiento de la OSINT para los analistas de inteligencia militar?

Marcel Plichta
Edwin Dudley-Taylor
Traducido al castellano por Daniel Blanco

Resumen

La Inteligencia de Fuente Abierta (OSINT) está siendo adoptada por los profesionales de la inteligencia de todo el mundo y los analistas militares no son una excepción. Sin embargo, los analistas militares suelen responder a un conjunto distinto de requerimientos de información que sus homólogos en los servicios civiles y el sector privado. En consecuencia, las definiciones existentes de OSINT, así como sus ventajas y desventajas, pueden ser confusas y malinterpretadas en un contexto militar.

Este artículo definirá la OSINT en términos útiles para la inteligencia militar y analizará cómo las necesidades de los analistas y consumidores en contextos militares requieren conjuntos distintos de información. A continuación, se expondrán las ventajas y los desafíos de integrar significativamente la obtención de fuentes abiertas al proceso de inteligencia militar.

Además, se explorará como la OSINT ofrece a los analistas una forma adicional y, a menudo, más barata de responder a los requerimientos de los mandos, así como también facilita el intercambio de inteligencia con otros servicios de inteligencia y con el público en general. Pese a los beneficios, los analistas deberán evitar la dependencia excesiva de las fuentes abiertas en detrimento de los demás métodos de obtención y vigilar las posibles limitaciones legales y éticas en torno a la protección de datos.

Palabras clave

OSINT, Inteligencia militar, Analistas militares, Analistas de inteligencia, Fuentes abiertas.

What does OSINT growth mean for military intelligence analysts?

Abstract

Intelligence practitioners worldwide are embracing open-source intelligence (OSINT), and militaries are no exception. However, military analysts often answer a distinct set of questions compared to their counterparts in civilian intelligence and the private sector. Consequently, existing definitions of OSINT can be confusing, and the discipline's benefits and

tradeoffs are often misunderstood in a military context. In this article we will define OSINT in terms useful to military intelligence analysts and discuss how the needs of military analysts and consumers require a distinct set of information from OSINT. It will then draw out the benefits and challenges of adopting open-source collection more fully into the military intelligence process. Ultimately, OSINT collection offers an additional and frequently cheaper way for analysts to answer some kinds of intelligence questions and could make it easier to share intelligence with other services and the general public. At the same time, analysts should be wary of overreliance on OSINT to the exclusion of other collection disciplines, consumer bias towards or against information collected from OSINT, and the potential legal and ethical constraints for collecting personal information.

Keywords

OSINT, Intelligence analysis, Military intelligence, Intelligence training, Tradecraft.

1 Introducción

Durante los últimos años, las organizaciones de inteligencia han realizado un esfuerzo concertado para adoptar e integrar la inteligencia de fuentes abiertas (OSINT) a su trabajo. Diversos académicos comentan que los países del hemisferio occidental —en particular— podrían beneficiarse de ello. Harper y Cross, por ejemplo, afirmaron en 2024 que la OTAN puede «adelantarse, disuadir y derrotar los esfuerzos de sus adversarios mediante la explotación de la inteligencia de fuentes abiertas» (Harper y Cross, 2024). La Oficina del Director de Inteligencia Nacional de Estados Unidos (ODNI) fue un poco más lejos y calificó a la OSINT como «la inteligencia de primer recurso» en su Estrategia OSINT 2024-2026 (ODNI, 2024).

Pese a que la adopción de OSINT promete mejoras, que van desde una mejor obtención de inteligencia hasta una reducción de costes operacionales, sus beneficios generan preguntas entre los analistas militares y sus respectivas instituciones. Este artículo busca analizar las ventajas y los desafíos de dar prioridad al OSINT en la obtención de información dentro de contextos militares. «¿Qué implica el crecimiento de la OSINT para los analistas de inteligencia militar?», comenzará con una visión general de la inteligencia de fuentes abiertas y de los elementos únicos que caracterizan a la inteligencia militar. Seguidamente, el artículo analizará las ventajas de la OSINT para los analistas militares y los posibles obstáculos a los que se enfrentarán a la hora de incorporar los métodos de fuente abierta a su trabajo.

La OSINT ofrece a las organizaciones con competencias de inteligencia militar una nueva vía para responder a sus requerimientos de información y coordinarse con otras instituciones, pero también plantea retos que van desde garantizar que los consumidores de inteligencia y tomadores de decisiones comprendan los límites de la disciplina, hasta asegurar que los procesos de obtención sean realizados dentro de los límites legales. Cualquier grado de utilidad que los analistas militares puedan sacar de esta disciplina, será determinado por la forma en que las organizaciones afronten los desafíos planteados por las fuentes abiertas.

2 ¿Qué es OSINT?

Aunque el debate sobre OSINT está creciendo astronómicamente en los círculos de inteligencia, tanto las agencias gubernamentales como los expertos académicos utilizan el término para referirse a conceptos diferentes, a menudo con definiciones intercambiables. Por ejemplo, las empresas privadas y las organizaciones no gubernamentales pueden utilizar OSINT para referirse a cualquier trabajo del sector privado relacionado con la inteligencia, como las auditorías externas, las investigaciones privadas, la seguridad personal, los asuntos públicos o el periodismo de

investigación. Otros conceptos más estrictos la emplean como una abreviatura de la inteligencia derivada, en concreto, de las plataformas de medios sociales, mientras que la definición más laxa recae en los agregadores de contenido en redes sociales, que califican tareas sencillas de cotejo de información como «OSINT».

Para complicar las cosas, la OSINT también es un término que engloba diferentes actividades de obtención de información, algunas de las cuales se solapan con disciplinas ya establecidas. Por ejemplo, el uso de imágenes de satélites comerciales para observar la actividad en una base militar es GEOINT por definición, pero también es considerado OSINT si las imágenes recaen en el ámbito de la información disponible públicamente. Desde el punto de vista organizativo, esto significa que un analista de GEOINT podría ser también un analista de OSINT aunque esté aplicando el mismo conjunto de conocimientos en disciplinas diferentes.

Asimismo, los funcionarios gubernamentales también utilizan definiciones diferentes, refiriéndose en ocasiones a la OSINT como productos de inteligencia elaborados con información disponible públicamente. La OSINT suele ser definida a nivel de Gobierno como una disciplina de obtención, como la HUMINT y la SIGINT. El Centro Nacional de Inteligencia de España describe OSINT como «información procedente de fuentes abiertas». La Oficina del Director de Inteligencia Nacional de Estados Unidos, por su parte, publicó una definición actualizada de OSINT en diciembre de 2024 que la definía como una disciplina «derivada exclusivamente de información pública o comercialmente disponible» (ODNI, 2024: 6). Esto contrasta con su descripción de los productos de inteligencia OSINT, que son «derivados exclusivamente de PAI, CAI o OSINT» (ODNI, 2024: 7).

Durante el resto de este artículo se entenderá la OSINT como una *actividad de obtención*. Esto no significa que la OSINT carezca de relevancia para los analistas, sino todo lo contrario. Como se verá más adelante, la recopilación de información de fuentes abiertas alimenta de forma natural el procesamiento y el análisis de los productos de inteligencia.

3 Prioridades de la inteligencia militar y civil

Buena parte de los debates académicos sobre OSINT se centran en su utilidad en contextos civiles, ya sea en el sector privado o en una agencia de inteligencia de carácter civil. No obstante, los consumidores de inteligencia militar y los consumidores de inteligencia civil tienen diferencias importantes. Ambos tienen requerimientos de información y preferencias analíticas distintas, así como funciones que apoyan actividades conjuntas con propósitos diferentes, incluso si ambos consumidores forman parte del mismo Gobierno.

La inteligencia militar incluye entre sus consumidores a los responsables de tomar decisiones en las fuerzas armadas, como los comandantes de los ejércitos, los responsables políticos civiles que dirigen o asesoran sobre la política de defensa o los líderes nacionales que dirigen a las instituciones militares, mientras que los servicios de información civiles suelen abarcar una amplia gama de cuestiones de inteligencia, que van desde la estabilidad económica hasta la seguridad cibernética, la inteligencia militar suele ser más restrictiva. Dado que el comercio, la diplomacia o la delincuencia no forman parte del núcleo fundamental de la inteligencia militar —a menos que representen una amenaza para la defensa nacional— los analistas de inteligencia en instituciones armadas suelen centrar sus esfuerzos en las intenciones de adversarios, la lucha antiterrorista y las operaciones militares.

El uso principal de la inteligencia militar en un contexto estratégico es la planificación operacional o la prospectiva de defensa. Aunque en algunas ocasiones —como en la seguridad nacional— se produce un solapamiento entre la inteligencia militar y los servicios civiles, los analistas, normalmente, suelen adoptar enfoques adaptados a las diferentes necesidades de sus consumidores. Al igual que los servicios de información civiles, las organizaciones de inteligencia militar realizan diversas actividades de obtención. Además de la Inteligencia de Fuentes Abiertas, suelen incluir disciplinas de recopilación más antiguas, como la Inteligencia de Señales, la Inteligencia Humana y la Inteligencia Geoespacial. Dependiendo de cómo estén estructuradas las comunidades de inteligencia en los organigramas nacionales, las agencias civiles también pueden estar bajo el mismo paraguas general que las instituciones militares, como es el caso de la Agencia de Seguridad Nacional de Estados Unidos.

Pese a que los organismos militares y servicios civiles comparten el mismo acervo de información, los analistas de inteligencia de los ejércitos destinan el proceso de obtención a fines diferentes. Los productos de inteligencia militar se centran en «apoyar a los mandos en su toma de decisiones, ayudándoles a aumentar su comprensión», lo que puede abarcar desde las evaluaciones de amenazas a corto plazo hasta necesidades a más largo plazo como la previsión estratégica (*Ministry of Defence*, 2023: 8-9). La inteligencia militar suele evaluar temas como las capacidades de las fuerzas contrarias, la probabilidad de un conflicto y los retos para las operaciones planificadas o en curso.

La inteligencia militar a largo plazo también se utiliza en la política de defensa, el desarrollo de armamento y el análisis geopolítico para anticiparse a las amenazas emergentes y mantener o alcanzar la superioridad militar de una nación. Las necesidades de los consumidores de inteligencia militar requieren un conjunto único de productos de los analistas de inteligencia. Por ejemplo, los analistas militares suelen elaborar análisis del

orden de batalla, evaluaciones de daños en batalla y reportes de selección de objetivos que responden a las necesidades específicas de los comandantes del campo de batalla y los responsables de la toma de decisiones (USMC, 2016). Mientras que algunos beneficios del OSINT son intercambiables entre el ámbito civil y el entorno militar, los desafíos que se presenten en este último serán determinados por la medida en la cual la obtención de información de fuente abierta facilite o dificulte la elaboración de análisis para consumidores de defensa.

4 Ventajas de la OSINT para los analistas militares

Aunque los analistas militares se enfrentan a una serie de requisitos y expectativas diferentes a los de sus homólogos civiles, la OSINT ofrece formas de mejorar sus análisis y facilitar su difusión. Por ejemplo, los analistas podrían aprovechar la OSINT para subsanar vacíos de información y verificar fuentes de otras disciplinas, así como evaluar distintos medios de obtención y facilitar el intercambio de inteligencia con otras organizaciones.

Sobre el proceso de obtención, cabe destacar que su función principal es recolectar información destinada a producir inteligencia que pueda responder las preguntas de los consumidores finales. Durante la aplicación de este proceso pueden surgir lagunas o vacíos que dejen a los analistas militares y tomadores de decisiones con una imagen incompleta del asunto a evaluar. La OSINT podría llenar algunas de las brechas mencionadas con anterioridad.

Para ilustrar el argumento, se puede mencionar que la estrategia de propaganda y reclutamiento de un grupo extremista podría ser difícil de entender sin un esfuerzo coherente por recopilar sus declaraciones públicas y mensajes oficiales en las redes sociales. Adicionalmente, estudiar las métricas de interacción que obtienen estos mensajes podría ayudar a determinar su grado de eficacia.

Por otra parte, la recopilación de información en las redes sociales, como imágenes de combate, puede ayudar a los analistas a comprender dónde se están produciendo los combates con mayor precisión y rapidez que otros métodos de recopilación en las circunstancias adecuadas. Aunque la sobreabundancia informativa podría afectar de manera negativa a los analistas, un volumen mayor de fuentes abiertas puede ayudar a reforzar la evidencia en las cual basan sus conclusiones. Las Fuerzas Armadas de los Estados Unidos descubrieron a través de sus investigadores que la OSINT puede ayudar a los analistas a «identificar despliegues, movimientos, ejercicios, objetivos y disposiciones inusuales, seguimiento de objetivos de alto valor y patrones logísticos inusuales» (Sieting, 2024).

Como ejemplo reciente una base del Grupo Wagner fue geolocalizada y atacada por el Ejército de Ucrania después de que un periodista subiera una foto del sitio a sus redes sociales (Kirichenko, 2023). La OSINT también puede contribuir a la evaluación de daños y bajas (BDA) o al análisis del orden de batalla (ORBAT) en caso en que haya imágenes del combate o de sus consecuencias en las redes sociales; este tipo de análisis lo intentan a menudo las empresas de inteligencia que desarrollan sus actividades en el sector privado, lo que indica que los métodos de OSINT podrían aumentar la pluralidad de la información que el personal militar necesita para mantener y presentar el orden de batalla (ORBAT) actualizado que requieren sus consumidores (Jane, 2024). Aunque los analistas militares sigan dependiendo, en gran medida, de otras disciplinas de obtención para producir inteligencia, un flujo adicional de información procedente de los recopiladores OSINT mejorará la confianza de los analistas y añadirá redundancia si se pierde una fuente de información.

Centrarse más en la obtención de OSINT significa también que los analistas militares podrían operar mejor en entornos conflictivos o restrictivos donde otros métodos de obtención podrían no funcionar. La naturaleza descentralizada de la información de fuente abierta, que a menudo es compartida de forma voluntaria por muchas personas diferentes, la convierte en una fuente flexible en las circunstancias adecuadas. Ramsey (2024: 7) señala que, en lugares donde se dificulta a la obtención de información por parte de plataformas nacionales, «la OSINT probablemente estará disponible debido al gran número de sensores que proporcionan información y que probablemente también servirán como recurso principal para cubrir estas lagunas». Existen límites a la información que puede ser recopilada en un contexto de batalla, en especial, si un beligerante impone un apagón de comunicaciones u alguna otra medida para controlar la información en el área de operaciones. Aun así, el acceso a la OSINT podría ser un salvavidas para los analistas militares con fuentes limitadas de información.

Mediante la recopilación de publicaciones nacionales y prensa extranjera en redes sociales, la OSINT también puede ayudar a determinar las intenciones de los adversarios respecto a su percepción de la opinión pública. Por ejemplo, una nación adversaria podría amplificar la idea de que su tecnología de misiles puede vencer las defensas aéreas de un vecino. El Cuerpo de la Guardia Revolucionaria Iraní, de acuerdo con distintos reportes, invierte fuertemente en plataformas comunicacionales para «controlar parte del proceso de influencia en Irán, asegurando que su narrativa estratégica y su percepción de la realidad sigan siendo dominantes» (Gill, 2020: 113). Como segundo ejemplo, una organización extremista podría hacer públicas sus amenazas para causar pánico y ejercer presión a las autoridades locales. Los analistas pueden interpretar los mensajes estratégicos a través de

fuentes abiertas para conocer las intenciones o prioridades de un adversario, aunque, como se verá más adelante, deben ser de igual modo conscientes del engaño y la desinformación en las fuentes abiertas.

5 La utilización de la OSINT para mejorar y verificar la obtención

Se debe precisar que otros métodos de obtención suelen llenar las mismas lagunas de información que las fuentes abiertas. La HUMINT podría describir una estrategia de propaganda a través de una fuente clasificada y la GEOINT podría indicar con exactitud la región dónde se están produciendo los combates o ayudar con el análisis del orden de batalla. Ahora bien, los defensores de la OSINT sostienen que es una forma más rentable de responder a las mismas preguntas de los consumidores de inteligencia. Por ejemplo, los requerimientos de información de una agencia gubernamental pueden no necesitar una costosa plataforma satelital si existe un proveedor comercial con las mismas capacidades.

Conviene señalar, sin embargo, que el potencial ahorro de costes operativos no es percibido directamente por los analistas. Como mucho, podría significar que sus productos son diferentes, pero no necesariamente mejores si llegan a la misma conclusión analítica. Por supuesto, los responsables políticos o los directores de las instituciones pueden decidir que, de todos modos, merece la pena el esfuerzo de construir y mantener capacidades de obtención propias, sin importar su presupuesto. Incluso en esos casos, la OSINT podría ayudar a triangular y rellenar las lagunas dejadas por la información fragmentaria. Miguel Sánchez de Toca Alameda et al (2023: 21) señalan que la OSINT puede «apoyar a otras disciplinas de inteligencia para confirmar o desechar hipótesis» en un contexto militar.

Esto beneficia la confianza de los analistas en sus evaluaciones, así como su capacidad para ofrecer información a los operadores de las demás disciplinas. Gracias a la obtención de información de fuente abierta, los analistas pueden, por ejemplo, hacer un seguimiento de la información incompleta procedente de una fuente humana para confirmar la exactitud de la información. Esto, a su vez, mejora la capacidad de los analistas de HUMINT para evaluar la calidad o credibilidad de las fuentes empleadas en el proceso de obtención.

La OSINT también podría incrementar el alcance de las organizaciones con recursos limitados. En los últimos años, las herramientas de código abierto han permitido desde rastrear envíos internacionales hasta determinar interferencias en sistemas de posicionamiento satelital. Por ejemplo, Grey Dynamics ayudó al canal de televisión CBS News a rastrear las actividades ilícitas del Grupo Wagner en África Central mediante el empleo de métodos de fuentes abiertas. (Grey Dynamics, 2024)

Mientras que en la era pre-Internet resultaba difícil y costoso vigilar los acontecimientos mundiales, la información y las herramientas disponibles en la actualidad para los encargados de la obtención facilitan considerablemente el análisis a quienes carecen de herramientas de obtención más avanzadas, como aquellas disponibles en los servicios de información o agencias de inteligencia del sector público.

También se debe recordar que todas las organizaciones de inteligencia no siempre cuentan con los recursos y capacidades de agencias grandes como la CIA o la DGSE; las naciones más pequeñas pueden estar interesadas solo en obtener información sobre su región inmediata o pueden carecer del presupuesto para ejecutar operaciones clandestinas de obtención. Sin embargo, las amenazas para un país y sus ciudadanos no siempre son próximas. Como ejemplo, se presentan los buques comerciales de un actor estatal. Estos pueden atravesar o acercarse a una zona de conflicto situada a miles de kilómetros de sus fronteras. Incluso si el buque está fuera del alcance de los elementos operativos de los servicios de información, los responsables políticos pueden dar instrucciones a la inteligencia militar para que evalúe la seguridad de las embarcaciones. Para satisfacer rápidamente los requerimientos de información, los analistas militares podrían contratar los servicios de una empresa o la licencia de una herramienta que se especialice en la obtención de fuentes abiertas. Esto aumenta el rango de la información disponible para los analistas de inteligencia.

6 Uso de OSINT en transparencia e intercambio de inteligencia

La inteligencia militar también puede aprovechar la OSINT para mejorar la transparencia de sus procesos. Aunque el trabajo de los servicios de información suele ser clasificado y opaco por motivos de seguridad nacional, las instituciones gubernamentales pueden aumentar la confianza de la ciudadanía en su trabajo mediante la publicación de sus productos de inteligencia y conclusiones analíticas, siempre que sea posible. La OSINT juega un papel fundamental en dicha estrategia, ya que la información abierta puede desclasificarse con un riesgo menor en cuanto a la revelación de material sensible o métodos clasificados. La Agencia de Inteligencia de Defensa de Estados Unidos publicó en 2023 un informe con información de fuentes abiertas para demostrar que Rusia estaba utilizando drones diseñados por Irán en Ucrania (DIA, 2023).

Asimismo, los productos provenientes de OSINT también pueden facilitar el intercambio de inteligencia con aliados y socios debido a su naturaleza de fuente abierta. El proceso de desclasificar información o hacerla accesible a un Gobierno aliado suele ser laborioso, sobre todo, si el producto de inteligencia utiliza diversas fuentes para sustentar análisis. Mientras que un servicio o departamento de inteligencia militar puede guardar celosamente

sus métodos de obtención más sensibles, un producto que se base en su mayor parte o en su totalidad en OSINT sería más fácil de compartir con un socio en el que la agencia no confíe plenamente con la seguridad operacional de sus fuentes. Una filtración o filtración de productos de inteligencia basados en información abierta, sin dejar de ser una amenaza para la seguridad nacional, es más segura y menos comprometedora que la filtración de la identidad de una fuente humana o los detalles técnicos de una plataforma de señales.

7 Retos para los analistas militares

La OSINT puede ofrecer oportunidades para rellenar vacíos en los requerimientos de información o triangular información de fuentes provenientes de métodos de obtención distintos, pero también presenta límites y desafíos. Entre los retos a los cuales podrían enfrentarse los analistas militares se encuentran cantidades abrumadoras de información y operaciones de engaño por parte de los adversarios, así como los prejuicios del consumidor, el aumento de la privatización y las restricciones legales en las plataformas abiertas.

Romanow señala que «los mismos sesgos analíticos que han alimentado los fallos de inteligencia en el pasado seguirán estando presentes e incluso podrían acentuarse por las muchas nuevas fuentes y los nuevos actores en el campo de la inteligencia militar» (2025). Asegurarse de que se abordan estos inconvenientes es primordial para garantizar que los analistas militares puedan sacar el máximo provecho de las fuentes abiertas.

Quienes desempeñen labores analíticas, no deben asumir que la inteligencia de fuentes abiertas rellenará por sí misma los vacíos de *data*. Tampoco deben de sentirse presionados para recurrir a las fuentes abiertas a expensas de los demás métodos de obtención. La OSINT, como todas las disciplinas de inteligencia, puede no responder a los requerimientos de información más específicos de las instituciones militares Esto ocurre debido a que la inteligencia militar busca reunir información sobre las capacidades e intenciones de los ejércitos adversarios, información que no siempre está disponible en fuentes abiertas.

Por ejemplo, la localización de las bases aéreas de un país adversario puede ser información de dominio público, pero una lista de los recursos o activos militares presentes en esas localizaciones seguramente será clasificada. Del mismo modo, las fuentes abiertas no pueden reemplazar actividades de obtención en elementos restrictivos, como la intervención de las señales de una organización extremista para monitorear sus comunicaciones.

Otro de los mayores desafíos en la obtención de información de fuentes abiertas, es la incoherencia de los «sensores». Quienes agregan contenido

en redes sociales podrían indicar dónde se encuentra una unidad adversaria hoy, pero no mañana. Otras cuentas podrían, por confusión o impericia, etiquetar de forma errónea ubicaciones y acontecimientos o incluso afirmar que vídeos antiguos corresponden a acontecimientos recientes. Esto se agrava en un contexto militar, donde el público civil suele identificar incorrectamente el material militar, como ilustró el vídeo viral difundido por los rebeldes sudaneses el 21 de noviembre 2023, que mostraba una plataforma de defensa antiaérea Pantsir-S1 rusa y resultó ser falso (*Army Recognition*, 2023). La cuestión de la fiabilidad no es exclusiva de la OSINT, pero añade otro nivel de complicaciones para los analistas militares que deben asegurarse sin cesar de que utilizan información de calidad en sus productos.

Todos los métodos de obtención son susceptibles al engaño. La OSINT, sin embargo, presenta un problema considerable —en particular, con la información en redes sociales— para los servicios de inteligencia. Existen algunos factores que complican la situación ya descrita, en primer lugar, los usuarios de las redes sociales no suelen sentir la necesidad de comprobar o verificar el contenido o las afirmaciones que comparten. Esto significa que, aunque los usuarios no tengan intención de engañar, pueden hacerlo por falta de rigurosidad.

Todavía más complicado es el creciente problema de la desinformación difundida a propósito por agentes malignos o programas automatizados. Confiar en la recolección de datos de las redes sociales es, por tanto, complicado para los analistas, ya que los usuarios y las publicaciones pueden tener una relación endeble con la realidad objetiva. Para los analistas militares, el volumen de información y el alcance de los engaños pueden reducir la utilidad de las fuentes abiertas en el contexto de un campo de batalla.

Rasak (2021: 52) señala que «las consecuencias del bombardeo de eventos, las campañas de desinformación, el secuestro de tendencias y el engaño militar restarán fundamentalmente utilidad a la OSINT a nivel táctico». Puede que los mandos no deseen tomar una decisión importante en el campo de batalla basándose en un flujo de información comprometido, y que los analistas no difundan sus conclusiones hasta que haya una confirmación independiente de los datos obtenidos. Estos problemas pueden hacer que los productos de inteligencia basados en OSINT sean menos accionables y también socavan una de las ventajas pregonadas de la OSINT, que a menudo suele ser la velocidad en sus flujos de información.

Pese a los desafíos ya mencionados, la recopilación de información en las redes sociales es beneficiosa para las organizaciones militares que necesitan comprender y contrarrestar los efectos de la desinformación o la información errónea. Anticipar el impacto de la desinformación es vital porque, aunque algo no sea cierto, las personas pueden ajustar su comportamiento si catalogan la información falsa como un evento cierto.

Por ejemplo, las imágenes manipuladas de unas maniobras militares al otro lado de la frontera podrían incitar a un comandante a poner a sus fuerzas en alerta. Comprender los orígenes y las intenciones (si las hay) del engaño a través de las redes sociales es, por tanto, una poderosa forma de que los analistas informen a los responsables de la toma de decisiones. Comprender los orígenes y las intenciones (en caso de que las haya) de las operaciones de engaño a través de las redes sociales es, por tanto, una herramienta poderosa para que analistas informen a los responsables de la toma de decisiones.

Otro problema relacionado a la OSINT es que los consumidores de inteligencia pueden tener prejuicios en contra o a favor de las fuentes abiertas, debido a que suelen tener opiniones personales sobre qué métodos de obtención son más fiables. Como ejemplo, un general podría considerar que la información recopilada en redes sociales no es lo suficiente fiable como para llevar a autorizar una operación. Por otro lado, un consumidor de inteligencia podría dar prioridad a la OSINT sobre un asunto no necesariamente adecuado, solo porque cree que la obtención de fuentes abiertas es menos costosa en términos operativos.

Estos sesgos personales se agravan en los servicios de inteligencia si se agrega inteligencia artificial (IA) al procesamiento de datos. Juan Luis Sánchez Sánchez (2025: 19) sostiene que «el empleo creciente de la IA para analizar el entorno de la información mediante OSINT será fundamental para prevalecer y adelantar escenarios de inteligencia para el posterior empleo defensivo/ofensivo». Para los analistas militares, esto significa desarrollar nuevas habilidades para sacar el máximo partido de la inteligencia artificial y desarrollar una comprensión rudimentaria de cómo funcionan las IA y, en particular, los LLM (modelos de lenguaje de gran tamaño) para protegerse de problemas como las alucinaciones.

Sin embargo, no hay mucho que los analistas puedan hacer, ya que en gran medida estarán a merced de la organización de inteligencia más amplia que dicta dónde y cómo se utiliza la IA en el ciclo de inteligencia. Cualquiera de estas situaciones puede convertirse en un reto para los analistas militares, que tienen que asegurarse de que están caracterizando adecuadamente sus fuentes en los productos de inteligencia y en las sesiones informativas.

8 Restricciones legales y privatización de la obtención

Incluso en un contexto gubernamental, el debate sobre OSINT a menudo se solapa con la aparición de contratistas privados y empresas tecnológicas. La incorporación de contratistas de inteligencia podría representar una manera inicial de integrar a las entidades privadas a las instituciones

gubernamentales, debido a que los métodos de obtención de fuente abierta no suelen ser clasificados y los especialistas de la disciplina no necesitan necesariamente habilitaciones de seguridad tan elevadas como si trabajaran con otros métodos de obtención.

Si la empresa contratista ya cuenta con la capacidad y el personal necesarios, su incorporación a un servicio de inteligencia gubernamental podría resultar más rápido y asequible para los responsables políticos que crear una capacidad interna de características similares desde cero. Sin embargo, la privatización de la obtención plantea sus propios retos a los analistas. Williams y Blum (2018: 22-23) señalan que los productos comerciales tienen costes ocultos para los gobiernos, ya que deben adaptarse a sistemas clasificados.

Desde un punto de vista de seguridad, las naciones más pequeñas podrían tener que arriesgarse a contratar a una empresa extranjera o contratista multinacional para que les proporcione los servicios OSINT que desean en sus servicios de información. Ambas cuestiones pueden complicar el trabajo de los analistas militares y los funcionarios públicos, que podrían acabar lidiando con un proceso complicado de acceso a la información recopilada o perdiendo el acceso a las herramientas de obtención si la empresa pierde o no renueva su contrato con el Gobierno.

Por otro lado, el debate sobre la privatización de la OSINT también se solapa con otra consideración clave: las restricciones éticas o legales a la recopilación de información en el dominio público (Smith y Cook, 2023). Aunque un miembro del público ponga su información en Internet, las agencias de inteligencia pueden, sin que sea necesario, tener acceso a su obtención, debido a las leyes que regulan la recopilación y el almacenamiento de datos personales, sobre todo, en las naciones democráticas del hemisferio occidental.

Los analistas militares suelen centrarse en las amenazas externas más que en los asuntos internos, pero aun así tienen que asegurarse de que trabajan dentro de la legalidad en casos como el de un ciudadano que actúa en el extranjero o cuestiones como la contrainteligencia doméstica. Al igual que en el caso de la inteligencia artificial, los límites legales y las decisiones contractuales de la OSINT están en gran medida fuera del alcance de los propios analistas, pero siguen siendo un impedimento potencial para su trabajo si se aplican de forma ineficaz.

La privatización añade una capa más a los desafíos legales y éticos mencionados, ya que las empresas pueden enfrentarse a un complicado conjunto de normativas locales para ejecutar la obtención, especialmente si no tienen su sede en el mismo país que el servicio de inteligencia que los contrata. Proelium (2024), un bufete de abogados británico, señala que «la

posición jurídica general es que la [Ley de Inteligencia del Reino Unido] no se aplica a las actividades de una empresa privada, sin embargo, esa posición es diferente cuando una empresa privada es contratada por una entidad gubernamental para llevar a cabo una actividad equivalente a actividades de vigilancia». Debido a ello, los analistas que trabajan con empresas privadas para recopilar OSINT podrían acabar obteniendo menos información de la prevista para cumplir las leyes y acuerdos locales.

9 Conclusiones

Nuestro estudio analizó las ventajas y desafíos relacionados al empleo del OSINT en la inteligencia militar. La implicación principal es la necesidad de que los responsables políticos y tomadores de decisiones de las instituciones correspondientes comprendan las implicaciones de integrar fuentes abiertas a la inteligencia militar. Aunque, por lo general, se considera que la OSINT es una de las disciplinas de obtención con menor coste, desarrollar herramientas y capacidades supone una inversión significativa de recursos que luego podrían acabar infrautilizados y malgastados.

Para los propios analistas, es imperativo entender cómo integrar la OSINT a sus flujos de trabajo de manera efectiva. Dado que las herramientas y metodologías de OSINT pueden afectar a una amplia gama de actividades analíticas, los analistas deben asegurarse de que han recibido la formación adecuada para aprovechar las ventajas de las fuentes abiertas sin sucumbir a los inconvenientes ya conocidos de las fuentes abiertas, como la saturación de información.

También existen oportunidades para que los académicos y profesionales del sector de la inteligencia amplíen el debate sobre dónde puede la OSINT mejorar el análisis de inteligencia para las instituciones militares. Pese a que las fuentes abiertas suelen estudiarse de manera aislada, en los círculos de inteligencia y en los sectores de seguridad es necesario explorar más a fondo las formas en que las fuentes abiertas podrían mejorar la inteligencia militar y cubrir vacíos de información. Además, se podría ampliar el debate entre las fuentes abiertas y la inteligencia artificial.

Por último, la OSINT cambiará la forma de trabajar de los analistas militares a medida que se incrementa su empleo y dependencia, con contextualización adecuada y el apoyo institucional, por lo que puede convertirse en una herramienta poderosa para las fuerzas gubernamentales. Queda por ver hasta qué punto muchos de los conocimientos básicos que utilizan los analistas de inteligencia tienen menos relación con los métodos de obtención y más con el pensamiento crítico, la anticipación a las necesidades de los consumidores de inteligencia y la entrega rápida de sus conclusiones analíticas.

Pese a que no hay duda de que la OSINT podría ayudar a llenar vacíos de información y acelerar la llegada de inteligencia crítica, los analistas militares deben asegurarse de que la OSINT se trata con el mismo nivel de seriedad y escrutinio que otras disciplinas de obtención, sobre todo, por la importancia que supone la inteligencia militar para asuntos críticos relacionados con la seguridad nacional.

Bibliografía

Defense Intelligence Agency. (2023). *Iranian UAVs in Ukraine: A Visual Comparison*. Defense Intelligence Agency.

Gill, M. (2020). Capitalism, Communications, and the Corps: Iran's Revolutionary Guard and the Communications Economy. NATO Strategic Communications Centre of Excellence, p. 113.

Grey Dynamics. (2024). Case Studies [en línea]. Central Africa. [Consulta: 2025]. Disponible en: https://greydynamics.com/case-studies/

Harper, C. y Basset Cross, R. (2024). NATO Must Recognize the Potential of Open-Source Intelligence [en línea]. Atlantic Council. [Consulta: 2025]. Disponible en: https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-recognize-the-potential-of-open-source-intelligence/

Kirichenko, D. (2003). The Growing Use of Scamming Techniques and Social Media on the Battlefield [en línea]. Irregular Warfare Center. [Consulta: 2025]. Disponible en: https://irregularwarfarecenter.org/publications/perspectives/the-growing-use-of-scamming-techniques-and-social-media-on-the-battlefield/

Ministry of Defence (UK). (2023). Joint Doctrine Publication 2-00. Intelligence, Counter-Intelligence and Security Support to Joint Operations. Gov.uk, pp. 8-9. [Consulta: 2025]. Disponible en: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf

Office of the Director of National Intelligence. (2024). Citation and Reference for Publicly Available Information, Commercially Available Information and Open Source Intelligence. Office of the Director of National Intelligence.

Office of the Director of National Intelligence. (2024-2026). *The Intelligence Community OSINT Strategy*. United States Intelligence Community.

Proelium (2024). Compliance in OSINT: Legal Requirements for Data Protection and Privacy [en línea]. Proelium. [Consulta: 2025]. Disponible en: https://proeliumlaw.com/open-source-intelligence-and-privacy/

Ramsey, C. (2024). Ivy Intelligence (IVI) Large-Scale Combat Operations Targeting. *Military Review. The Professional Journal if the U.S. Army*, p. 7

Rasak, J. (2024). Event Barraging and the Death of Tactical Level Open-Source Intelligence [en línea]. Army University Press. [Consulta: 2025]. Disponible en: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Rasak-Open-Source-Intelligence-1.pdf?ver=OQwPyC0UYip2VkQsWIS7dQ%3D%3D

Romanow, N. (2025). The Transparency Trap: Risks of Deception in the Age of OSINT. *Proceedings*. U.S. Naval Institute. 151(1), p. 1463.

Sánchez Sánchez, J. L. (2025). Inteligencia artificial en apoyo a la inteligencia militar. Eje fundamental del éxito o fracaso en la competición estratégica entre grandes potencias. *Documento Analísis 09/2025*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, p. 19.

Sieting, L. (2024). Intelligence Discovery Experiment Open-Source Intelligence Support to Targeting. Military Intelligence.

Smith, A y Cook, S. (2023). Guide to Open-Source Intelligence [en línea]. Grey Dynamics. [Consulta: 2025]. Disponible en: https://greydynamics.com/a-guide-to-open-source-intelligence-osint-2/

Sánchez de Toca Alameda, M., Díaz, J., Martín, R. y Muñoz, A. (2023). El Subsistema De Inteligencia Del Ejército De Tierra: Presente Y Retos De Futuro. *Cuaderno de Inteligencia*. Madrid, Ministerio de Defensa, p. 21.

United States Marine Corps (2016) Doctrinal Publication 2, Intelligence, and Marine Corps Warfighting: Intelligence Operations Intelligence Production and Analysis. *MAGTF Intelligence Production and Analysis*. U.S. Marine Corps.

Williams, H. y Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. *Rand*. Santa Mónica, Rand Corporation, pp. 22-23.

Comité Científico y Consejo Editorial

Comité Científico

Arturo Esteban Ceballos
Teniente Coronel del Cuerpo de Infantería de Marina.
Doctor en Seguridad y Análisis de Riesgos y Conflictos.
Analista J2 STRIKEFORNATO.

Emilia José Peña Ruíz
Teniente Navío del Cuerpo de Especialistas de la Armada.
Doctora en Ciencias Sociales y Jurídicas.
Analista en J2 MOPS.

Julia Pulido Gragera
Doctora en Derecho Internacional Público y Relaciones Internacionales.
Jefa de Gabinete del consejero de Medioambiente, Agricultura e Interior.
Comunidad de Madrid.
Capitán (RV) Departamento de Inteligencia, ESFAS. CESEDEN.

Licesio J. Rodríguez Aragón
Doctor en Matemáticas.
Titular de Universidad del área de Estadística e Investigación Operativa.
Escuela de Ingeniería Industrial y Aeroespacial de Toledo. Universidad de Castilla-La Mancha.
Alférez (RV) Departamento Inteligencia, ESFAS. CESEDEN.

Adrián Nicolás Marchal González
Doctor en Derecho. Doctor del Grado de Criminología y Ciencias Forenses.
Director del Departamento de Seguridad y Defensa. Universidad Nebrija.

Álvaro Cremades Guisado
Doctor en Ciencias Políticas y de la Administración y Relaciones Internacionales.
Director del Máster Univresitario en Seguridad y Defensa. Universidad Nebrija.

Consejo Editorial

Presidente

José Antonio Fuentes de la Orden
General Subdirector/Jefe de Estudios de la ESFAS.

Vocales

Ángel Segundo Gómez González
Coronel ET (Reserva)

Carlos Alberto Ramírez Sánchez
Coronel ET. Director del Departamento de Inteligencia ESFAS

Normas de envío de artículos

Tema del Cuaderno de Inteligencia número 4

El próximo número del Cuaderno de Inteligencia tendrá como tema principal: «El papel de la Comunidad de Inteligencia Ampliada, presente y futuro». Si desea colaborar, los artículos propuestos deberán cumplir los siguientes requisitos:

1 Directrices para el envío de artículos

Los autores están obligados a comprobar que su envío cumple todas las directrices que se muestran a continuación.

- No haber sido publicado o sometido en consideración previamente por ninguna otra revista (o se ha proporcionado una explicación al respecto en los comentarios al editor/a).
- Se adapta a la finalidad y temática propuesta en el correspondiente Cuaderno de Inteligencia.
- Cumple con lo establecido en las «Normas de edición y publicación en el Ministerio de Defensa»[1] en formato (apartado 3), aspectos tipográficos (apartado 5), aspectos ortográficos (apartado 6), citas y bibliografía (apartado 7) e imágenes (apartado 8).
- Se adecua a la política de detección de plagio que asegura la originalidad de los manuscritos

2 Ficheros a entregar

Los autores deberán remitir los siguientes archivos al buzón del *Cuaderno de Inteligencia* (ESFAS_CuadernoInteligencia@mde.es) no más tarde del **treinta de marzo** de cada año:

- 1 documento de texto (formato compatible con Word Office), con el texto completo y paginado y sin imágenes incrustadas. Deberá tener una extensión entre 4.000 y 12.000 palabras. Si cuenta con imágenes, deberá marcarse la ubicación de estas en el texto, indicando el nombre que tenga el archivo de la imagen (tipo de fuente negrita y color).
- 1 documento Word que incluya un resumen de hasta un máximo de 200 palabras y 5 palabras clave, que no coincidan con el título. En castellano y su traducción al inglés.

[1] Disponible en https://publicaciones.defensa.gob.es/media/downloadable/files/links/n/o/normas_de_edici_n_y_publicaci_n_en_el_ministerio_de_defensa_1.pdf

- 1 documento Word con una breve biografía del autor de aproximadamente 150 palabras.
- 1 foto del autor en formato jpg o tiff.
- 1 carpeta que contenga todas las imágenes, en formato jpg o tiff, y una resolución mínima de 300 ppp que las haga aptas para su publicación.
- 1 documento Word con los correspondientes pies de foto.

3 Proceso de recepción y aprobación de originales

Una vez recibida la propuesta de artículo y comprobado el cumplimiento de las normas de publicación, se comunicará al autor la aceptación de su trabajo **para ser evaluado** por el Consejo de Redacción.

Entre los artículos recibidos se **seleccionarán** aquellos que destaquen por su originalidad, relevancia, interés y actualidad para su publicación en el Cuaderno de Inteligencia correspondiente.

En caso de haber sido **seleccionado**, el artículo se devolverá al autor con propuesta de correcciones (si fuera necesario). Al mismo tiempo se le remitirán los siguientes documentos que los autores deberán completar, para la cesión de derechos y el cobro por la colaboración (el Consejo los pondría a disposición de los autores):

- Cesión de derechos de explotación.
- Declaración responsable.
- Ficha de Datos

El **plazo de subsanación de errores** será de veinte días hábiles, tras los que deberán ser entregados al Consejo de Redacción las versiones definitivas de los artículos.

Para cualquier duda sobre la realización de este proceso, pueden enviar un correo al buzón del *Cuaderno de Inteligencia*.

UNIVERSIDAD NEBRIJA

CESEDEN

ESCUELA SUPERIOR DE LAS FUERZAS ARMADAS

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA

MINISTERIO DE DEFENSA

SUBSECRETARÍA DE DEFENSA

SECRETARÍA GENERAL TÉCNICA

SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL