Nuevas amenazas a la Seguridad Nacional

Cdi 2

CUADERNOS DE INTELIGENCIA

MINISTERIO DE DEFENSA

Nuevas amenazas a la Seguridad Nacional

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

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

NIPO 083-24-219-9 (edición impresa)
ISBN 978-84-9091-941-5 (edición impresa)

NIPO 083-24-220-1 (edición en línea)

Depósito legal M 15983-2024
Fecha de edición: octubre de 2024
Maqueta e imprime: Imprenta Ministerio de Defensa

Índice

Artículo cuarto

Artículo quinto

Artículo sexto

Artículo octavo

Artículo noveno

Artículo décimo

Presentación

En la década de los años noventa, el Ejército estadounidense acuñó el acrónimo VUCA para referirse al entorno Volatil (V), Incierto (U de *Uncertainty*), Complejo (C) y Ambiguo (A), en el que nos movemos en las últimas décadas. Estas características se han acentuado en los últimos años de la mano de la frecuente aparición de tecnologías disruptivas como la inteligencia artificial, las posibilidades de actuación en el ciberespacio, el manejo de grandes masas de datos, las redes 5G, etc. que favorecen el empleo de las estrategias híbridas para alcanzar objetivos geopolíticos, geoeconómicos o simplemente empresariales.

Vivimos en un mundo globalizado, altamente interconectado, que ya no se mueve solo en tres dimensiones: tierra, mar y aire; sino que ahora también se mueve en el ciberespacio, en el espacio profundo y ultraterrestre y en el espacio cognoscitivo, donde actúan las campañas de desinformación. Los riesgos y las amenazas son multidimensionales, cambiantes, difíciles de evaluar y de predecir. Esto da lugar a crisis mucho más frecuentes, más complejas, más difíciles de prever y de gestionar, que requieren actuaciones en el multidominio y donde disponer de buenos análisis de inteligencia es crítico.

La toma de decisiones es intrínseca a la gestión de crisis. Esas decisiones deben estar basadas en una correcta evaluación de la situación en todos sus aspectos, y en el conocimiento de las posibles líneas de acción y sus posibles consecuencias.

Para poder llevar a cabo el proceso de la toma de decisiones se requiere un buen análisis de inteligencia que cada vez es más complejo y más cambiante, por lo que es necesario que esté basado en datos multifacéticos tomados en tiempo real o casi real. Recordemos lo que decía Sun Tzu «Conoce a tu enemigo y conócete a ti mismo, y en cien batallas, nunca saldrás derrotado», sin embargo, hoy no basta con limitar ese conocimiento al ámbito militar, hoy necesitamos conocer la situación militar, económica, comercial, energética, agrícola, tecnológica, sanitaria, socio-política y el funcionamiento de las cadenas de suministros. Así como todos aquellos datos que nos permitan actuar sobre las estrategias híbridas propias y contra las del adversario.

Se requiere que los organismos que trabajan en inteligencia lo hagan con un enfoque integral, ágil, capaz de dibujar escenarios complejos, basados en múltiples indicadores que faciliten el seguimiento de los acontecimientos y la toma de decisiones, que ese es el fin último de la inteligencia.

La inteligencia es el principal instrumento con el que cuenta la Seguridad Nacional para hacer frente a las crisis que ponen en peligro los intereses nacionales.

La gestión de crisis debe estar basada en la inteligencia elaborada a partir de la integración de datos y en la capacidad de adaptación rápida a nuevos escenarios y todo esto requiere un sistema de Seguridad Nacional bien engrasado, suficientemente digitalizado para que la transmisión de datos pueda realizarse casi en tiempo real, lo que unido al conocimiento de las capacidades públicas y privadas disponibles, le permitirán al gobierno tomar las decisiones más acordes con la situación.

El analista de inteligencia debe trabajar imbuido del concepto *Just in time*. Un concepto muy aplicado en la fabricación, basado en la idea de que cada pieza llega al lugar donde se necesita en el momento que se necesita. Así deben de llegar los informes de inteligencia al decisor justo cuando los necesita y con la información que necesita ni más, ni menos, lo que no es fácil de conseguir, pero no por ello debemos renunciar a lograrlo.

Los acontecimientos de los últimos años que han activado el Comité de Situación, pieza clave en el Sistema de Seguridad Nacional para la gestión de crisis, han sido: los graves disturbios violentos promovidos en Cataluña por la plataforma independentista *Tsunami Democràtic* en 2019, la pandemia de COVID en 2020, la guerra derivada de la invasión rusa de Ucrania, en 2022, y la guerra en Gaza de Israel contra Hamas, en 2023, sin olvidar otras que han sido gestionadas por las comunidades autónomas, dentro del sistema de protección civil que también se integra en el sistema de Seguridad Nacional, como el volcán de la isla de La Palma, o la nevada de la borrasca Filomena en Madrid y Toledo.

En este ámbito, VUCA las crisis se solapan y hacen más complejas su gestión y requieren un mayor esfuerzo de los organismos que realizan inteligencia a los que necesariamente se les debe redoblar sus capacidades.

En el proceso de gestión de todas estas crisis se ha puesto de manifiesto la necesidad de disponer de datos fiables y análisis de inteligencia en tiempo oportuno para facilitar la toma de decisiones. En la actualidad se trabaja para que el Sistema de Seguridad Nacional disponga de datos en tiempo real, para que los análisis de inteligencia sean lo más precisos posibles.

Por todo lo expuesto las reflexiones que se presentan en este libro resultan más necesarias y oportunas que nunca. Se anima al lector interesado en estos temas a que se adentre en la lectura de este libro, donde, sin duda, encontrará muchas respuestas a sus dudas y nuevas rutas por explorar para aumentar su conocimiento sobre un tema tan complejo y de tanto interés como es la inteligencia.

GB. Miguel Ángel Ballesteros Martín
Exdirector de Seguridad Nacional (2018-2024)

Cuaderno de Inteligencia 2

Juan Ramón Sabaté Aragonés

En 2023, la Escuela Superior de las Fuerzas Armadas (ESFAS) del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) emprendió la iniciativa de realizar una publicación de periodicidad anual dedicada a la función inteligencia. El propósito de tal iniciativa era, y sigue siendo, doble: por un lado, servir de vehículo de intercambio de ideas entre los que constituyen la comunidad de inteligencia y, por otro, contribuir a la difusión de los desarrollos que se están produciendo en el ámbito de la inteligencia militar a un público cada vez más numeroso e interesado en estos temas. Gracias al impulso del departamento de Inteligencia de la ESFAS, y a sus estrechos vínculos con las organizaciones y expertos que componen la comunidad de inteligencia, el primer número del *Cuaderno de Inteligencia* contó con un significativo número de interesantes artículos dedicados al análisis de diversos aspectos de la inteligencia militar.

Dando un paso más hacia la consolidación de esta iniciativa, este año aparece el número dos de un cuaderno que, en esta ocasión, se dedica al análisis de la inteligencia, en relación con la Seguridad Nacional. Y, al igual que el pasado año, no han faltado expertos analistas que, de manera desinteresada, han aportado un total de catorce artículos que se recogen en este segundo cuaderno.

Este año se cuenta con con la colaboración especial del general Miguel Ángel Ballesteros, antiguo director del Instituto Español de Estudios Estratégicos y exdirector del Departamento de Seguridad Nacional, además de ser una persona muy querida y respetada en esta casa, quien ha tenido la gentileza de prologar este segundo cuaderno, y no cabe imaginar un mejor inicio.

En el primer cuarto del siglo XXI, la función de inteligencia está experimentado una profunda transformación, como consecuencia de la constante evolución de las amenazas a la seguridad y del rápido desarrollo de las tecnologías. En un mundo interconectado y dinámico, los desafíos a la Seguridad Nacional y global no solo han aumentado en número y complejidad, sino que también se han diversificado en formas inimaginables hace tan solo unas décadas. A las amenazas tradicionales, como el terrorismo y los conflictos armados, ahora se unen otras nuevas, como los ciberataques, la desinformación y el uso de tecnologías comerciales con fines bélicos.

En este escenario, la inteligencia se convierte en una herramienta esencial, no solo para la prevención y respuesta ante tales amenazas, sino también para la anticipación y adaptación a futuros desafíos. Esta capacidad de adaptación es crucial en un entorno donde la tecnología avanza a un ritmo acelerado y las tácticas empleadas por actores estatales y no estatales están en constante evolución.

En este cuaderno de inteligencia se presenta un conjunto de artículos que exploran diversos aspectos relevantes relacionados con la seguridad y la defensa. Desde el análisis de la amenaza emergente de los drones comerciales letalizados hasta la importancia de los sistemas tácticos de aeronaves no tripuladas, cada artículo ofrece una interesante perspectiva sobre cómo las fuerzas armadas, en coordinación con los demás instrumentos de poder del Estado, deben evolucionar para hacer frente con eficacia a los nuevos retos y amenazas.

La transformación de la función de inteligencia también implica un enfoque más colaborativo y multidisciplinar. La integración de datos masivos, la cooperación interdepartamental, intersectorial e internacional, y el desarrollo de nuevos conceptos, doctrinas y estrategias son elementos esenciales para enfrentar las complejidades de las amenazas modernas. Por otro lado, las cuestiones éticas y legales revisten, cada vez más, una relevancia que debe tomarse en consideración a la hora de desarrollar y emplear de tecnologías avanzadas, garantizando que la adopción de nuevas herramientas y procedimientos no comprometa los valores y derechos fundamentales.

Este cuaderno no solo pretende ofrecer un análisis profundo de las amenazas actuales y futuras, sino también inspirar a los profesionales de la inteligencia a adoptar una mentalidad innovadora y flexible. En un mundo donde la línea entre guerra y paz se difumina, y donde las acciones en la zona gris se vuelven cada vez más prevalentes, la capacidad de adaptarse y evolucionar es más crucial que nunca.

Esta reflexión pretende enmarcar los artículos que componen el cuaderno dentro de una narrativa coherente y relevante para el profesional de la inteligencia. Cada una de estas contribuciones ofrece un análisis detallado de un aspecto específico de la inteligencia al servicio de la seguridad. Espero que, al leer los diversos artículos, los lectores se enriquezcan con nuevos conocimientos, sino que también reflexionen sobre las implicaciones de la función de inteligencia en el siglo XXI.

El primer bloque presenta un numeroso grupo de artículos dedicados al análisis de las nuevas, y no tan nuevas, amenazas, bien de manera general, bien centrándose en alguna amenaza específica. Así, el artículo «Las amenazas en las Estrategias de Seguridad Nacional (ESN) de España y su equivalencia en la Unión Europea y la OTAN» proporciona un análisis

comparativo y evolutivo de las amenazas identificadas en las estrategias de Seguridad Nacional (ESN) de los años 2013, 2017 y 2021, y las compara con los documentos equivalentes aprobados por la Unión Europea UE y la Organización del Tratado del Atlántico Norte (OTAN).

Aunque existe un núcleo importante de amenazas que aparecen en las tres ESN analizadas, se observa que estas han ido evolucionando tanto en número como en naturaleza. Por otro lado, con el transcurso del tiempo las amenazas han aumentado en complejidad, desarrollándose simultáneamente en múltiples dominios y estando cada vez más interconectadas. Las estrategias híbridas y la revolución tecnológica han jugado un papel crucial en esta evolución, facilitando la aparición de nuevas formas de amenaza que aprovechan la interconexión global y las tecnologías avanzadas. El artículo afirma que las amenazas a la Seguridad Nacional de España están alineadas con las identificadas por la Unión Europea («Brújula Estratégica para la Seguridad y Defensa») y la OTAN (»Concepto Estratégico»), a la vez que defiende una cooperación internacional más estrecha y coordinada para enfrentar con eficacia estas amenazas complejas y multidimensionales.

Por su parte, el artículo que lleva por título «¿Regreso al futuro?: La función de inteligencia y las, no tan nuevas, amenazas a la Seguridad Nacional» analiza la evolución de la inteligencia en el contexto de la transición de la Guerra Global Contra el Terrorismo (GOTW) al desafío sistémico representado por China y Rusia. Describe cómo la política exterior de Estados Unidos ha desplazado su enfoque del terrorismo hacia la competencia estratégica entre grandes potencias. Este cambio de enfoque requiere adaptar las capacidades de inteligencia a un entorno donde la rivalidad interestatal es predominante. El artículo enfatiza la necesidad de una inteligencia estratégica, la cooperación internacional en inteligencia e integración de capacidades tecnológicas avanzadas. Es necesario, por tanto, la adaptación de la inteligencia a un entorno global complejo, reevaluando sus capacidades, métodos y objetivos para mantener una ventaja estratégica.

En el estudio de amenazas concretas, los siguientes artículos analizan diversos tipos: las ciberamenazas, las relacionadas con las emergencias, las asociadas al desarrollo e implantación de la inteligencia artificial o las derivadas del empleo generalizado de drones como instrumento militar.

El artículo «Evolución de las ciberamenazas: nuevos actores para nuevos escenarios» analiza cómo la diversificación y sofisticación de los actores en el ciberespacio han transformado el panorama de la ciberseguridad. Desde los ataques prorrusos en Estonia en 2007, los estados utilizan ahora grupos de cibercrimen y hacktivistas como proxies para realizar ciberataques, mientras que estos grupos también se han profesionalizado, ofreciendo servicios avanzados como Ransomware-as-a-Service y DDoS-for-hire. Los actores estatales, o Amenazas Persistentes Avanzadas (APTs), realizan

ciberespionaje, acciones ofensivas y operaciones de influencia. El cibercrimen ha crecido exponencialmente, y el hacktivismo se ha estructurado en grupos con ideologías políticas claras. El sector privado desarrolla y vende herramientas ofensivas avanzadas, y los actores internos representan una amenaza creciente. Una mayor cooperación entre los organismos implicados y un enfoque más amplio en el análisis de ciberamenazas son esenciales para enfrentar estas complejidades, requiriendo la colaboración entre fuerzas de seguridad, empresas especializadas y organizaciones académicas.

El siguiente artículo, «La necesidad de la Inteligencia en las operaciones del SOC», subraya la importancia de la inteligencia de amenazas en la ciberseguridad, destacando su papel esencial en los Centros de Operaciones de Seguridad (SOC). La inteligencia de amenazas facilita la identificación, análisis y mitigación de riesgos, mejorando la capacidad de respuesta ante incidentes. El artículo describe cómo la inteligencia de amenazas transforma datos en conocimiento útil para la toma de decisiones, detallando las funciones del SOC, como detección y respuesta a incidentes, caza de amenazas, gestión de vulnerabilidades y seguridad ofensiva. También resalta la importancia de un ecosistema tecnológico integrado con herramientas como SIEM y plataformas de inteligencia de amenazas (MISP, OpenCTI), y la cooperación en el intercambio de información. Concluye que es crucial entender y adaptar las necesidades de información del decisor y que la inteligencia debe ser oportuna, precisa, procesable, relevante y predictiva. Es vital seleccionar las técnicas de análisis adecuadas y comprender las amenazas específicas del sector y país del adversario. Es esencial tener un ecosistema tecnológico adecuado, desarrollar la madurez en procesos y capacidades técnicas, y automatizar procedimientos específicos de amenazas para mejorar el SOC.

El artículo «Cómo la inteligencia en emergencias se enfrenta a las nuevas amenazas» aborda la adaptación de este tipo de inteligencia ante el aumento de amenazas debido al cambio climático, globalización y abandono rural y otros factores. Estas amenazas incluyen riesgos naturales (inundaciones, incendios, fenómenos meteorológicos, terremotos) y tecnológicos (accidentales o intencionados). El artículo destaca la integración de tecnologías avanzadas como la inteligencia artificial (IA), aprendizaje profundo y *big data* para mejorar la anticipación y respuesta a emergencias. También se enfatiza la importancia de la colaboración para compartir información y mejorar la respuesta a emergencias. En conclusión, subraya la necesidad de un enfoque proactivo y colaborativo que aproveche las nuevas tecnologías para fortalecer la resiliencia y protección de las poblaciones frente a emergencias.

El artículo «¿Cómo la función inteligencia podría mitigar los riesgos de la introducción de inteligencia artificial en las operaciones militares?» analiza

las vulnerabilidades y riesgos asociados al empleo de la inteligencia artificial (IA) en el ámbito militar. Se destacan tres tipos principales de vulnerabilidades: datos, algoritmos e interacción hombre-máquina. Los datos pueden ser manipulados o incompletos, afectando la eficacia de la IA. Los algoritmos pueden ser atacados directamente o mediante envenenamiento de datos, mientras que la interacción hombre-máquina enfrenta desafíos de confianza. Por otro lado, el artículo aborda los riesgos de no implementar IA, sugiriendo que los adversarios podrían obtener ventajas significativas. Para gestionar estos riesgos, se recomienda la implementación de procedimientos robustos de prueba, evaluación y verificación (TEVV), y la protección de los ciclos de decisión mediante medidas de seguridad. La inteligencia y contrainteligencia son cruciales para identificar y mitigar estos riesgos, asegurando operaciones seguras y efectivas en un entorno dominado por la IA. En conclusión, la gestión cuidadosa de los riesgos de la IA es esencial para evitar amenazas operativas.

El artículo «Acotación de la amenaza presente y futura de los drones comerciales letalizados» analiza la evolución, capacidades y riesgos de los drones comerciales modificados para usos militares, particularmente en la guerra de Ucrania. Resalta la importancia de comprender esta amenaza, inicialmente subestimada debido a la percepción de los drones como juguetes. Los drones comerciales, como los de DJI, son fáciles de usar, pero difíciles de modificar, mientras que los drones FPV (*First Person View*) son altamente personalizables y requieren conocimientos técnicos avanzados. Estos drones han transformado el campo de batalla mediante la combinación de inteligencia, vigilancia y ataques precisos. La rápida evolución de los drones FPV se debe a la disponibilidad de componentes avanzados y económicos, y al soporte de comunidades de entusiastas. Simuladores y formación intensiva han sido cruciales para entrenar a operadores de drones, mientras que los avances en tecnología de radio y vídeo han mejorado de manera significativa el control y la operación de estos drones, permitiendo operaciones a larga distancia y en entornos complejos. La mayor amenaza no son los enjambres de drones, sino la masa distribuida de drones que permite un flujo constante de ataques y vigilancia. Los drones comerciales letalizados representan una disrupción significativa, siendo sistemas económicos y simples comparados con los costosos sistemas militares tradicionales. El documento subraya el papel crucial de las *war startups*, academias e iniciativas gubernamentales en Ucrania para fomentar la innovación en el uso de drones, concluyendo que estos sistemas han transformado la guerra moderna y plantean tanto desafíos como oportunidades para futuros conflictos armados.

El artículo «Enigmas o misterios: cuando la amenaza está en la interpretación» explora las amenazas en el Sahel, utilizando los conceptos de «enigmas» y «misterios» de Gregory Treverton. Los «enigmas» pueden

resolverse con suficiente información, mientras que los «misterios» son intrínsecamente complejos. El Sahel, con su inestabilidad política, demográfica y ambiental, es un ejemplo de esta dualidad. La región enfrenta conflictos, golpes de Estado, terrorismo y desafíos climáticos. Las fronteras coloniales y la falta de cohesión nacional complican la situación, mientras que el alto crecimiento demográfico intensifica los problemas. Las amenazas como el terrorismo y el cambio climático son difíciles de prever y controlar. Churchill señaló en 1939 la dualidad entre enigma y misterio, destacando que algunos problemas pueden ser ambos según el enfoque. En el Sahel, las amenazas requieren una inteligencia colaborativa, adaptativa y comprensiva, que vaya más allá de los datos hacia una comprensión profunda del entorno y sus relaciones complejas.

El bloque dedicado al análisis de las amenazas se cierra con el artículo «Contrainteligencia en el ámbito aeroespacial: amenazas a la libertad de acción del EA en el actual entorno de seguridad», que aborda cómo la complejidad del entorno de seguridad global ha transformado los conflictos, desarrollándose en una zona gris con acciones hostiles que buscan pasar desapercibidas y limitar la capacidad de respuesta. El autor afirma que el Ejército del Aire y del Espacio (EA) español es particularmente vulnerable a amenazas no convencionales como terrorismo, espionaje, sabotaje, subversión y crimen organizado (TESSCO). La subversión y el espionaje son especialmente peligrosos, degradando la confianza en las fuerzas militares y obteniendo información crítica. El sabotaje, tanto físico como cibernético, puede afectar de manera significativa las operaciones del EA. El terrorismo y el crimen organizado emplean tácticas no convencionales para dañar infraestructuras y desestabilizar a las fuerzas armadas. La cooperación y la concienciación del personal son esenciales para contrarrestar estas amenazas. En conclusión, el EA debe desarrollar una capacidad robusta de contrainteligencia para enfrentar eficazmente las amenazas no convencionales.

El siguiente bloque de artículos analiza el modo en el que diversos desarrollos tecnológicos pueden apoyar la evolución de la inteligencia. El artículo «Inteligencia de Datos en Apoyo a la Toma de Decisiones para la Seguridad Nacional» destaca cómo la inteligencia de datos es crucial para enfrentar amenazas híbridas y multidominio. Permite integrar múltiples fuentes de información para identificar, analizar y responder a diversas amenazas, abarcando ámbitos físicos y no físicos como el ciberespacio. La analítica avanzada, incluyendo el aprendizaje automático y el análisis predictivo, es esencial para procesar grandes volúmenes de datos y detectar patrones y anomalías. Estas técnicas mejoran la toma de decisiones estratégicas al prever escenarios futuros e identificar vulnerabilidades. El artículo enfatiza la necesidad de una arquitectura de sistemas de información escalable y distribuida, capaz de manejar el creciente volumen de datos. La colaboración y el intercambio de información son fundamentales

para enfrentar las amenazas híbridas, requiriendo una coordinación efectiva entre diferentes agencias y países. En resumen, la inteligencia de datos es vital para anticipar y responder proactivamente a amenazas complejas en la Seguridad Nacional.

El artículo presentado por los tenientes coroneles Touceda y Medina y por el comandante Rodríguez Torres analiza el papel de los satélites de observación de la Tierra (SEOT) con capacidades de inteligencia de imágenes (IMINT) en la Seguridad Nacional. Los SEOT son esenciales para la recopilación de información y la toma de decisiones estratégicas. En la actualidad, los SEOT presentan desarrollos significativos, como la capacidad de transmitir imágenes a través de satélites geoestacionarios para reducir la latencia. Los sistemas modernos combinan el uso dual (civil/militar) para distribuir costos y mejorar la soberanía y discreción en su uso. La emergente industria «NewSpace» impulsa la creación de constelaciones de mini satélites, proporcionando imágenes de alta resolución a costos relativamente bajos. El futuro de los SEOT se vislumbra con la miniaturización de componentes, propulsión eléctrica, mayor resolución espectral y el uso intensivo de inteligencia artificial para el análisis de imágenes. En el ámbito de la defensa, España ha participado en programas como Helios y PAZ, con el objetivo de desarrollar capacidades autónomas para la obtención de imágenes de inteligencia. La evolución de los SEOT y su integración con tecnologías emergentes son fundamentales para mantener la ventaja estratégica y la resiliencia operativa en un entorno espacial cada vez más competitivo y conflictivo.

El artículo «Necesidad de disponer de sistemas tácticos de aeronaves no tripuladas (TUAS) en las Fuerzas Terrestres» destaca la importancia de los UAS en operaciones militares modernas. Utilizados en conflictos como los de Ucrania y Siria, estos sistemas proporcionan vigilancia y reconocimiento en tiempo real, esenciales para la toma de decisiones tácticas. El Ejército de Tierra español ha adoptado varios UAS, desde el SIVA hasta el SIRTAP en desarrollo. Los TUAS de Clase II son particularmente importantes por su equilibrio entre capacidad y flexibilidad, apoyando funciones de inteligencia y reconocimiento (ISTAR). Conceptos emergentes como el MUM-T y Sensor to Shooter optimizan la integración y transmisión de datos entre UAS y aeronaves tripuladas. El SIRTAP mejorará estas capacidades con mayor autonomía y mejores sensores. En conclusión, los TUAS son imprescindibles para dotar a las Fuerzas Terrestres de herramientas versátiles y eficientes, mejorando la eficacia operativa en entornos complejos y multidominio.

El cuaderno se cierra con una interesante reflexión acerca de la evolución del concepto de seguridad interior. El artículo «La seguridad interior en un mundo cambiante» analiza la evolución del concepto de seguridad interior

en un entorno globalizado y lleno de amenazas complejas. Inicialmente centrada en la protección de activos dentro de las fronteras nacionales, la seguridad interior ahora abarca tanto amenazas internas como externas debido a la globalización y el cambio tecnológico. La seguridad se divide en aspectos subjetivos (percepción de seguridad) y objetivos (capacidad estatal para proporcionar seguridad). El artículo destaca la importancia de la colaboración nacional e internacional para enfrentar amenazas como el terrorismo, espionaje, crimen organizado y ciberataques. Subraya la necesidad de una infraestructura de seguridad flexible y adaptable, capaz de integrar tecnologías avanzadas y estrategias colaborativas. Las amenazas híbridas y multidimensionales requieren una revisión constante de las políticas de seguridad. En conclusión, el artículo aboga por un enfoque proactivo y adaptativo, integrando inteligencia, cooperación internacional y tecnología para asegurar la protección en un mundo cambiante.

Como se puede apreciar, este cuaderno de inteligencia intenta proporcionar una visión amplia y detallada de los desafíos contemporáneos en la Seguridad Nacional, destacando la necesidad de una inteligencia adaptativa y proactiva para enfrentar un entorno de amenazas cada vez más complejo y dinámico.

Tan solo me resta felicitar a los colaboradores cuyos trabajos aquí se publican y agradecerles el esfuerzo y tiempo para prepararlos; a la vez que aprovecho para animar a todos aquellos que forman parte de la comunidad de inteligencia o que sienten interés por este tema, que se planteen colaborar en futuros números de este cuaderno.

Artículo primero

Las amenazas en las estrategias de Seguridad Nacional (ESN) de España y su equivalencia en la Unión Europea y la OTAN

Gonzalo Escudero García

Resumen

Las amenazas a la Seguridad Nacional de España están recogidas en las tres Estrategias de Seguridad Nacional publicadas hasta ahora. Por un lado, hay una serie de amenazas que se mantienen constantes en los tres documentos y, por otro, aparecen nuevas amenazas en las ESN más recientes. Además, se mencionan una serie de aspectos que modulan y caracterizan las amenazas, así como un análisis del origen de las mismas. También, se explica cómo responder, de forma general, a las diferentes amenazas, donde el sistema de Seguridad Nacional es un mecanismo clave. Por último, se realiza un breve repaso de las amenazas en la Unión Europea y la OTAN.

Palabras clave

Amenaza, Seguridad Nacional, Estrategia, España.

The threats in Spain's National Security Strategies and their equivalence in the Euroopean Union and NATO

Abstract

Threats to Spain's National Security are included in the three National Security Strategies published to date. On one hand, there are a series of threats that remain constant in the three documents, and on the other hand, new threats appear in the most recent NSS's. In addition, there are a series of aspects that modulate and characterize the threats, as well as an analysis of their origin. It also explains how to deal with the different threats, in a general way, in which case the National Security System is a key mechanism. Finally, a brief review of the threats in the European Union and NATO is given.

Keywords

Threat, National Security, Strategy, Spain.

1 Introducción

La necesidad de conocer las amenazas a la Seguridad Nacional es la misma que la de conocer el enemigo en una guerra. Como reza la conocida frase: «Conoce a tu enemigo y conócete a ti mismo; en cien batallas, nunca estarás en peligro» (Sun Tzu, 2009). Sin embargo, este análisis es siempre complejo y no está carente de dificultades.

La primera consideración que hay que abordar al tratar las amenazas a la Seguridad Nacional es alcanzar un consenso respecto a una pregunta de fácil planteamiento, pero de difícil resolución: ¿qué es una amenaza? De acuerdo con el *Diccionario de la Real Academia Española*, en su primera acepción, amenaza «es la acción de amenazar», y amenazar es «dar a entender con actos o palabras que se quiere hacer algún mal a alguien». Por lo tanto, y por asimilación, se puede entender que amenaza a la Seguridad Nacional es todo aquello que, mediante actos o palabras, pretenda hacer mal a la Seguridad Nacional. Ahora bien, el concepto definido (Seguridad Nacional) no debería entrar en la definición. Se debe definir qué es la Seguridad Nacional.

Conforme a la Ley de Seguridad Nacional (*BOE*, 2015):

> «[...] la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos».

Así pues, una vez definidos estos dos términos, se puede concluir que se ha delimitado el concepto de amenaza a la Seguridad Nacional, que es:

> «[...] todo aquello que mediante actos o palabras pretenda hacer mal a la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos».

Si bien, en el presente estudio, se parte de la ESN 2013, se debe mencionar que este documento no fue el primero de estas características. De hecho, en su introducción, se reconoce que la ESN 2013:

> «[...] continúa y revisa la Estrategia Española de Seguridad aprobada en 2011, adaptando y actualizando su contenido a los cambios del escenario estratégico, configurando un nuevo Sistema de Seguridad Nacional e implicando a la sociedad civil en los ámbitos de interés prioritario de la Seguridad Nacional» (Gobierno de España, 2011).

Por lo tanto, para el estudio de estas amenazas, y como después se explicará con más detalle, se han utilizado las sucesivas Estrategias de Seguridad Nacional (ESN), publicadas en España. Se ha respondido a una cuestión primaria (amenaza a la Seguridad Nacional); a continuación, se debe enfrentar una segunda cuestión: el análisis de la evolución de estas amenazas en las Estrategias de Seguridad Nacional, porque en los distintos documentos estratégicos —cuya elaboración coordina el Departamento de Seguridad Nacional— se abordan, de forma indistinta, con diferentes denominaciones: «riesgos y amenazas» (ESN 2013; Gobierno de España, 2013), «amenazas y desafíos» (ESN 2017; Gobierno de España, 2017) y, de nuevo, los «riesgos y amenazas» (ESN 2021; Gobierno de España, 2021).

No es la intención de este análisis entrar en una discusión sobre el significado y las diferencias entre amenaza, desafío y riesgo, por lo que en este documento se ha decidido emplear todos los términos como iguales. De esta forma, se pretende facilitar el estudio, y se evita entrar en debates o malentendidos semánticos. Así pues, cuando este documento se refiera a «amenaza, desafío o riesgo», se empleará el término «amenaza», por economía del lenguaje y por simplificar la redacción.

Una vez aclarados estas dos cuestiones preliminares, este documento pretende analizar las amenazas a la Seguridad Nacional en España. Para ello, se hace un estudio de las tres Estrategias de Seguridad Nacional publicadas en España (2013, 2017 y 2021), así como su evolución. La ESN 2017, repite las amenazas contenidas en la ESN 2103 y se añadieron cuatro nuevas. Posteriormente, la ESN de 2021 —como única diferencia con su predecesora— recoge una nueva amenaza.

En ocasiones, las amenazas han cambiado ligeramente de denominación, pero se mantiene su sentido y fundamento, como se puede observar en el cuadro posterior. En este documento, se explica en qué consisten, además de aportar una visión global de su tratamiento en las tres estrategias, para finalmente exponer su significado actual.

Tras presentar cada una de las amenazas, se analizan otros aspectos que las rodean y afectan. Estos aspectos se citan como potenciadores (ESN 2013), como factores que afectan a las amenazas (ESN 2017) o como características de las mismas (ESN 2021). Es decir, son aspectos que las definen y condicionan de una forma general y, en ocasiones, tienen la capacidad de modularlas.

En el siguiente apartado, se abordará la procedencia de estas amenazas. En este sentido, no puede considerarse que haya habido una gran

evolución, pues los aspectos que afectan al origen de las amenazas son permanentes y, básicamente, se podrían fijar en tres diferenciados: el desarrollo tecnológico, la posición geográfica de España y su dimensión social y política.

Y en este contexto, la dimensión política de España aconseja realizar un somero repaso de las amenazas que identifica la Unión Europea y la OTAN. Sus consideraciones al respecto tendrán una importante repercusión para el desarrollo de los documentos estratégicos España, pues así obliga el compromiso internacional.

Finalmente, este capítulo concluye con una serie de reflexiones, fundamentadas en todo el análisis previo y que tratan de condensar la visión estratégica global sobre las amenazas a la Seguridad Nacional que enfrenta el mundo y, más en concreto, España.

2 Las amenazas en las estrategias de Seguridad Nacional españolas

En España, como se ha señalado, se han publicado tres Estrategias de Seguridad Nacional, los años 2013, 2017 y 2021, además de la predecesora Estrategia Española de Seguridad de 2011. Aunque existen diferencias en cuanto a los capítulos que las componen, su estructura general es muy similar, lo que permite hacer un análisis comparativo. Además, tienen un mismo objetivo: la articulación de la Seguridad Nacional como «acción del Estado».

Para analizar estas estrategias y la evolución de las amenazas, hay que atender a sus elementos comunes, que están relacionados con el estudio de aquellos elementos que socavan o ponen en peligro la Seguridad Nacional. En primer lugar, las tres estrategias contemplan los distintos aspectos de los que hay que proteger a la sociedad española para preservar la Seguridad Nacional. También comparten un capítulo que analiza las áreas del mundo de interés nacional y el papel de España en ellas. Por último, las tres ESN especifican el cómo se debe articular esta política de Estado.

Con estos parámetros, las estrategias responden a las tres cuestiones planteadas —¿de qué?, ¿dónde? y ¿cómo? — de forma diferente, que será motivo de análisis en este trabajo. Además, y aunque la respuesta a «de qué» se traduce en el listado de las amenazas, las contestaciones a las otras dos preguntas ayudarán a entender la evolución de cómo son percibidas dichas amenazas en la vida cotidiana de España y su población.

2.1 *Amenazas, riesgos y desafíos en las tres estrategias*

Tal como se ha señalado en la introducción, todas las Estrategias de Seguridad Nacional aprobadas en España establecen una serie de amenazas, pero también se consideran otros aspectos que, sin ser definidos como amenazas ni poder ser considerados como tales, se deben tener en cuenta para salvaguardar la seguridad.

Así, la Estrategia de Seguridad Nacional de 2013, en su capítulo 3, recoge los riesgos y amenazas, aunque sin establecer diferencia alguna o clasificación a la hora de presentarlos. Por otro lado, subraya la existencia de unos potenciadores que pueden «generar nuevos riesgos o amenazas, o multiplicar y agravar» las ya conocidas.

Por su parte, la Estrategia de Seguridad Nacional de 2017 plantea amenazas y desafíos y los define, aunque no cita ningún riesgo. Las amenazas «comprometen o pueden socavar la Seguridad Nacional»; mientras que los desafíos «sin tener entidad de amenaza, incrementan la vulnerabilidad, provocan situaciones de inestabilidad o pueden propiciar el surgimiento de otras amenazas, agravarlas o acelerar su materialización». Sin embargo, pese a definirlos y explicar sus diferencias, pertenecen al mismo capítulo y tienen un trato similar pues ambos, amenazas y desafíos, están interconectados. Por otro lado, la ESN 2017 recalca la importancia de los espacios comunes globales: estos «territorios» no están bajo la soberanía ni jurisdicción de un Estado, pero lo que sucede en ellos puede afectar de forma global y, por ende, a España. Finalmente, la ESN 2017 señala dos factores que afectan a las amenazas y desafíos: las acciones híbridas y la revolución tecnológica.

Por último, la ESN de 2021 recoge unos riesgos y amenazas, que son dinámicos e interdependientes, lo que puede provocar un efecto «cascada». Igualmente, en el contexto actual, las estrategias híbridas cobran un especial y creciente protagonismo. Además, la ESN destaca que todos los riesgos y amenazas planteados tienen cierta correspondencia con una dimensión tecnológica, al tiempo que pueden ser parte y componente de las estrategias híbridas.

En el siguiente cuadro, que servirá de guía para el análisis posterior, se recogen las amenazas, riesgos y desafíos planteados en las tres estrategias. Asimismo, se hace referencia a los aspectos que caracterizan, potencian o repercuten en estas amenazas, riesgos y desafíos.

ESN 2013	ESN 2017			ESN 2021
RIESGOS Y AMENAZAS	AMENAZAS Y DESAFÍOS			RIESGOS Y AMENAZAS
Conflictos armados	AMENAZAS	Conflictos armados		Tensión estratégica y regional
Terrorismo		Terrorismo		Terrorismo y radicalización violenta
Espionaje		Espionaje		Espionaje e injerencias desde el exterior
Prolif. de armas de destrucción masiva		Proliferación de armas de destrucción masiva		Proliferación de armas de destrucción masiva
Crimen organizado		Crimen organizado		Crimen organizado y delincuencia grave
Vulnerabilidad de las infraestructuras críticas y los servicios esenciales		Amenazas sobre las infraestructuras críticas		Amenazas a las infraestructuras críticas
Ciberamenazas	AMENAZAS Y DESAFÍOS ESPACIOS COMUNES GLOBALES	Vulnerabilidad del ciberespacio	Ciberamenazas	Vulnerabilidad del ciberespacio
			Uso ilegítimo del ciberespacio	
Vulnerabilidad del espacio marítimo		Vulnerabilidad del espacio marítimo	Actos intencionados y de naturaleza delictiva	Vulnerabilidad del espacio marítimo
			Accidentes naturales	
		Vulnerabilidad del espacio aéreo y ultraterrestre	Actores estatales	Vulnerabilidad aeroespacial
			Actores no estatales	
Inestabilidad económica y financiera	DESAFÍOS	Inestabilidad económica y financiera		Inestabilidad económica y financiera
Vulnerabilidad energética		Vulnerabilidad energética		Vulnerabilidad energética
Flujos migratorios irregulares		Flujos migratorios irregulares		Flujos migratorios irregulares
Emergencias y catástrofes		Emergencias y catástrofes		Emergencias y catástrofes
		Epidemias y pandemias		Epidemias y pandemias
		Efectos derivados del cambio climático		Efectos derivados del cambio climático y de la degradación del medio natural
				Campañas de desinformación
POTENCIADORES	AFECTAN			CARACTERÍSTICAS
				Interconexión
	Acciones híbridas			Estrategias híbridas
Cambio climático				
Desequilibrios demográficos				
Uso nocivo de las nuevas tecnologías	Revolución tecnológica			Dimensión tecnológica
Pobreza				
Desigualdad				
Extremos ideológicos				

A partir del cuadro anterior, se pueden comentar varios aspectos. En primer lugar, las amenazas han aumentado cuantitativamente y de forma sucesiva, sin que haya desaparecido ninguna de ellas. Esto muestra el incremento de su diversidad como realidad que afecta a la Seguridad Nacional. En la ESN de 2013 aparecen doce amenazas; en la ESN de 2017 se citan quince, cuatro más[1], y, por último, en la ESN de 2021 se plantean hasta dieciséis amenazas.

Respecto a la ESN de 2013, la de 2017 añade las siguientes amenazas: las relacionadas con la «vulnerabilidad del espacio aéreo y ultraterrestre» —que, a su vez, se dividen entre las provocadas por actores estatales y no estatales—, las «epidemias y pandemias», y los «efectos derivados del cambio climático». Por último, en la ESN de 2021 se incluye la amenaza que suponen las «campañas de desinformación».

En segundo lugar, y pese a su aumento numérico, existe un bloque de amenazas[2] que permanece constante y que, aunque se citen de forma diferente en cada estrategia, son persistentes y son producto del análisis de la seguridad, desde un punto de vista multidimensional.

2.2 *Estudio individualizado de las amenazas*

A continuación, se analizan cada una de las amenazas, riesgos o desafíos que aparecen en las ESN.

2.2.1 Conflictos armados / tensión estratégica y regional

En este caso, la evolución ha transitado desde contemplar los conflictos armados como aspecto nuclear de la amenaza a reconocer que la Seguridad Nacional ya está influida y afectada en los pasos previos al estallido de una crisis bélica. De ahí que la ESN 2021 haya cambiado la denominación «conflictos armados» por «tensión estratégica y regional».

En los ocho años que separan las tres ESN, la probabilidad de un conflicto armado, en su concepción de una confrontación clásica, ha aumentado. Su concurrencia ha pasado de ser una posibilidad remota, por efecto de la interdependencia de los estados y la globalización, a una cercana, dado el retroceso del multilateralismo, la asertividad de ciertos actores y el

[1] En este sentido, dentro de la vulnerabilidad del espacio aéreo y ultraterrestre se toma como dos amenazas diferentes las provocadas por los actores estatales y los no estatales.

[2] Son las siguientes: conflictos armados, terrorismo, espionaje, proliferación de armas de destrucción masiva, crimen organizado, amenazas a las infraestructuras críticas, vulnerabilidad del ciberespacio, del espacio marítimo y aeroespacial, inestabilidad económica y financiera, vulnerabilidad energética, flujos migratorios irregulares, y, por último, emergencias y catástrofes.

incremento de la competición entre las grandes potencias. La invasión de Ucrania por parte de Rusia ejemplifica este cambio de paradigma.

Además, al conflicto clásico se le unen nuevas amenazas, las que suponen las estrategias híbridas, donde convergen diferentes tipos de actos hostiles: operaciones de desinformación, presión económica, subversión... entre otras. Todas ellas son diversas acciones con el objetivo común de alcanzar una determinada influencia en el escenario político-estratégico mundial[3].

Otro cambio ha sido la extensión de sus ámbitos de actuación, pues de los tres dominios tradicionales —terrestre, aéreo y naval— se han pasado a seis, tras añadir el ciberespacio, el ultraterrestre y el cognitivo.

Ante la amenaza que suponen los conflictos armados (o la tensión estratégica y regional), se reitera la necesidad de que España tenga una capacidad de defensa propia autónoma y creíble, además de mostrarse como un socio fiable en las organizaciones internacionales a las que pertenece para dar respuesta, de forma conjunta, a estas amenazas.

2.2.2 Terrorismo y radicalización violenta

A lo largo del periodo que abarcan las ESN, esta amenaza también ha ampliado su concepción y alcance. Mientras la ESN de 2013 tan solo cita el terrorismo, en 2017 ya se reconoce que al extremismo violento es un paso previo, y, en 2021, se señala que el radicalismo violento es, en sí mismo, una parte implícita de la amenaza.

En este contexto, el yihadismo se convierte en la principal amenaza terrorista en España, un país especialmente preparado por la lucha contra el terrorismo de ETA. A su vez, el terrorismo de carácter yihadista ha ampliado, de forma progresiva, sus capacidades, gracias a las nuevas tecnologías y la actual sociedad global, lo que facilita la difusión de ideologías extremistas.

Por otro lado, la materialización de la amenaza puede llevarse a cabo por las tradicionales organizaciones o células terroristas, pero también por individuos radicalizados —en muy distintos ambientes: aislados en su hogar, en prisión o en otros ambientes— y que actúen de forma solitaria. Otra de los nuevos focos de atención es la radicalización de inmigrantes de segunda generación y el retorno de milicianos a Occidente desde lugares en conflicto.

[3] De acuerdo con la ESN 2021, las estrategias híbridas son «acciones coordinadas y multidimensionales, tratan de explotar las vulnerabilidades de los Estados y sus instituciones con un objetivo de desestabilización o coerción política, social o económica».

Además, el terrorismo y la radicalización violenta suponen una amenaza no solo por sus consecuencias directas, sino también por las tensiones sociales, la inestabilidad política o las reacciones violentas sobre minorías que pueden provocar.

En este contexto, la experiencia en la lucha contra ETA, así como la naturaleza actual del terrorismo, muestran que las políticas democráticas y la cooperación internacional son las principales herramientas para luchar contra esta amenaza global.

2.2.3 Espionaje e injerencias desde el exterior

El espionaje es una amenaza constante en las tres estrategias. Además de contemplarla en su vertiente más clásica, las nuevas tecnologías han ampliado sus posibilidades. Así, el ciberespionaje, surgido en los últimos años, cobra especial relevancia, al igual que la influencia de las nuevas tecnologías, pues estas facilitan el acceso a grandes volúmenes de información e, incluso, datos sensibles.

Actualmente, esta amenaza diversifica su autoría —ya no solo espían los Estados— y sus objetivos —que son públicos y privados—. Por lo tanto, los autores del espionaje no solo son los Estados, sino que otras organizaciones o individuos pueden utilizarlo para sus propios intereses y sus acciones pueden tener influencia en la Seguridad Nacional.

Además, la acción de espiar no se realiza exclusivamente sobre los Estados —ya sea para tratar de influir en sus decisiones u obtener información de importancia—, sino que también tiene objetivos en el espectro privado, como pueden ser la industria, las infraestructuras críticas o las investigaciones científicas. Todas estas actividades delictivas afectan al tejido empresarial y económico de los estados, y al bienestar de sus ciudadanos.

Con respecto a este asunto, la ESN 2021 presenta dos novedades, que implican ampliaciones de esta amenaza. Por un lado, además del espionaje en sí, señala que las «injerencias desde el exterior» son una amenaza de similar naturaleza. Por otro, además de los actos de espionaje contra intereses españoles (ya sean estatales o individuales), contempla la posibilidad de las acciones de actores extranjeros en España o, incluso, el uso del territorio español como base de operaciones de agencias extranjeras que operen en terceros países.

2.2.4 Proliferación de armas de destrucción masiva

La proliferación de las armas de destrucción masiva es otra de las amenazas que ha sido una constante en las tres ESN, que plantean sus cuatro variantes: armas nucleares, químicas, biológicas y radioactivas.

En clave de respuesta, las estrategias españolas resaltan los mecanismos internacionales como principal freno a esta proliferación. Principalmente, el Tratado de No Proliferación de las Armas Nucleares, las acciones de la Organización de la Energía Atómica y la Convención de Armas químicas y su sistema de verificación. Sin embargo, no existe una medida similar para las armas biológicas. Además, todos estos tratados y mecanismos, todavía vigentes son, cada vez, más precarios y de difícil aplicación. Así, el escenario de una carrera armamentística de armas de destrucción masiva está cada vez más cerca. Esto es, especialmente, por dos motivos: la creciente tensión regional y el enmascaramiento de la producción de este tipo de armas gracias al doble uso —civil y militar— de estas industrias.

Asimismo, la expansión de los potenciales usuarios de estas armas es otro motivo de preocupación. El número de estados que, presuntamente, están ampliando sus arsenales nucleares ha aumentado, como muestra el número de actores activos (Irán, Corea del Norte, China, India y Pakistán). De igual forma, la posibilidad de que otros actores no estatales —grupos terroristas, bandas criminales o individuos aislados— tengan en su poder armas de destrucción masiva crece a la par que la falta de control sobre su proliferación

Por último, el desarrollo tecnológico, que amplía las plataformas de lanzamiento a misiles más modernos y drones y facilita el trasvase de conocimiento, y la mejora de las comunicaciones, que favorece el movimiento mundial de mercancías, añaden un extra de dificultad en la contención de esta amenaza.

2.2.5 Crimen organizado / crimen organizado y delincuencia grave

Todas las estrategias españolas han contemplado el crimen organizado como amenaza permanente a la Seguridad Nacional, a la que, en la ESN 2021, se une la delincuencia grave. Las características principales de este fenómeno delictivo, son su naturaleza transnacional, su opacidad y su flexibilidad y adaptabilidad a las diferentes situaciones. Estas circunstancias hacen que sea especialmente difícil erradicar esta amenaza, tan persistente en la vida cotidiana y que muta para aprovechar cualquier circunstancia de la que conseguir beneficio, como los flujos migratorios o la crisis de refugiados.

Asimismo, esta amenaza se ha adaptado a las nuevas tecnologías digitales —como demuestra el uso de criptomonedas o la internet oscura para expandirse— y también al aumento de los flujos fronterizos para ampliar sus campos de actuación. Además, la descentralización de sus estructuras y la mejora de las comunicaciones facilita los vínculos entre grupos terroristas y otros delincuentes, así como su capacidad de catalizar otro tipo de amenazas.

A nivel mundial, el crimen organizado mina a la Estados y erosiona sus instituciones, desestabiliza a las sociedades y perturba la economía. En este contexto, España es especialmente vulnerable a esta amenaza por su importante sector servicios —al que tanto afecta el crimen organizado— y, sobre todo, por su posición geográfica, que la convierten en una puerta de entrada a Europa para América y África.

Por último, la ESN 2021 incluye la delincuencia grave que, sin llegar a la sofisticación del crimen organizado, tiene efectos similares, y atenta especialmente contra los derechos humanos, como demuestran los casos de explotación de menores y la trata de seres humanos.

2.2.6 Vulnerabilidad de las infraestructuras críticas y servicios esenciales / amenazas sobre las infraestructuras críticas

Las infraestructuras críticas y su buen funcionamiento son necesarias para asegurar el bienestar social y económico de los ciudadanos, los sectores productivos y el funcionamiento del Estado. En definitiva, son imprescindibles para todos los sectores estratégicos. Entre otras, estas infraestructuras críticas incluyen instalaciones, redes, equipos físicos tecnología de la información y de la comunicación, y su mal funcionamiento puede tener un impacto directo sobre la Seguridad Nacional al no existir alternativas y ser, por lo tanto, indispensables[4]. Además, el fallo en una de ellas puede provocar un efecto cascada que pueda afectar a otras tantas y, por ende, multiplicar los daños.

Asimismo, el buen funcionamiento y servicio de estas infraestructuras pueden verse afectado por incidencias de diversa índole —causas naturales, errores humanos o fallos tecnológicos—, pero lo más peligroso es que exista un ataque deliberado contra ellas. Estas acciones ofensivas y premeditadas pueden llevarse a cabo mediante actos físicos o cibernéticos —opción cada vez más probable debido a la progresiva digitalización y la implantación de las nuevas tecnologías—, pues el objetivo final de estas actividades es provocar el mayor daño posible.

Por otro lado, dado que buena parte de estas infraestructuras críticas son de carácter privado, es necesaria una estrecha colaboración público-privada para garantizar su protección.

[4] De acuerdo con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, los sectores estratégicos son: administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnología de la información y las comunicaciones, transporte, alimentación y sistema financiero y tributario.

2.2.7 Ciberamenazas y vulnerabilidad del ciberespacio

Las amenazas vinculadas al ciberespacio ya aparecían en la ESN de 2013, pero su transformación posterior fue consecuencia de la propia evolución del medio en el que se materializa. Así, las características propias del espacio cibernauta —acceso fácil y de bajo coste, dilución de las fronteras, ocultación sencilla de la autoría— hacen que estas amenazas sean difusas, más difíciles de detectar y de muy compleja atribución, al tiempo que aumenta su peligrosidad para la Seguridad Nacional.

Inicialmente, la ESN de 2013 solo contemplaba la ciberamenaza, y posteriormente, tanto en 2017 como en 2021, se diferencian ciberamenazas o ciberataques («todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos») y el uso ilegítimo del ciberespacio —es decir, la utilización del ciberespacio como medio para otras actividades ilícitas: campañas de desinformación, propagación y financiación del terrorismo o crimen organizado, entre otros—.

Otro aspecto a resaltar es la rápida evolución y amplificación de la amenaza cibernética. Al tiempo que ha aumentado el uso del ciberespacio, este se ha vuelto más vulnerable. Así, a través del ciberespacio se puede amenazar infraestructuras críticas, servicios públicos y privados, y este es uno de los motivos por los cuales las administraciones públicas y privadas se han sumergido en los procesos de transformación digital. Por otro lado, conforme se acrecienta la dependencia tecnológica, también lo hacen las vulnerabilidades en este ámbito. Además, es previsible que esta tendencia aumente en el futuro —entre otras causas, por el aumento del teletrabajo o la mayor capilaridad y uso de las redes—, especialmente por la aparición de la inteligencia artificial, el *big data* y la computación cuántica.

Finalmente, hay que reseñar que las causas de estas amenazas no tienen por qué ser provocadas por individuos, organizaciones o estados, también pueden existir causas naturales o fallos técnicos que traigan consecuencias negativas para la Seguridad Nacional, de las que, a pesar de no existir intencionalidad, también es necesario protegerse.

2.2.8 Vulnerabilidad del espacio marítimo

El espacio marítimo es uno de los espacios comunes globales más trascendentales para la seguridad global y nacional. Aproximadamente, ocupa dos terceras partes del planeta, es de fácil acceso y, en general, está poco regulado y controlado. Además, el mar es una importancia fuente de riqueza: la pesca, la extracción de bienes energéticos, la ubicación de infraestructuras críticas, tanto en la mar como en el litoral, son ejemplos claros. Asimismo, es un medio de otras tantas actividades de gran impacto, como el transporte marítimo de toda índole (bienes o recursos energéticos)

—la mayor parte de las importaciones y exportaciones de España se realizan por vía marítima— o el intercambio de información digital y el flujo energético a través de cables submarinos.

En este contexto general, se constata que las amenazas a la Seguridad Nacional relacionadas con el mar son de dos grandes tipos. Por un lado, están las actividades de naturaleza delictiva y, por otro, los accidentes y catástrofes naturales. Además de ello, la delimitación de los espacios marítimos entre estados puede provocar crisis o conflictos de gran repercusión internacional.

El uso del espacio marítimo en la actividad del ser humano ha ido en aumento, y también las vulnerabilidades que le son inherentes. En el caso de España, la importancia del mar se basa, sobre todo, en su singularidad geográfica: tiene una amplia costa, lo que le dota de una gran cantidad de espacio marítimo bajo su responsabilidad; controla el estrecho de Gibraltar, uno de los principales nodos del tráfico marítimo, y, por último, su economía depende, en gran medida, del transporte marítimo. Adicionalmente, los intereses marítimos del país alcanzan otras zonas, como el golfo de Adén y el golfo de Guinea, porque en ellas la flota pesquera española, junto con otras actividades comerciales, tiene una presencia destacada.

2.2.9 Vulnerabilidad del espacio aéreo y ultraterrestre/vulnerabilidad aeroespacial

La vulnerabilidad del espacio aéreo y ultraterrestre (o la vulnerabilidad aeroespacial) aparece por primera vez en la ESN de 2017 y, posteriormente, en la de 2021. Otro de los espacios globales que se ve amenazado por actores estatales y no estatales.

Por un lado, el espacio aéreo —cada vez más poblado (aviones comerciales y drones)— es vital para la comunicación y suministro internacional, y, por otro, el ultraterrestre se ha convertido en la última frontera de confrontación geopolítica, y registra una presencia estable de agentes no estatales. En este sentido, el uso de los satélites es cada vez más necesario para diferentes actores, cuyas actividades no están reguladas por una normativa de carácter universal.

Por todo ello, este ámbito tiene una importancia creciente para la actividad humana, y puede convertirse en el epicentro de futuras tensiones. La necesidad de proteger las actividades que en él se desarrollan, evitando posibles actos hostiles y la proliferación de los deshechos espaciales, así como la gestión del tráfico global, constituye un reto futuro que hay que enfrentar en el presente para minimizar o evitar problemas.

2.2.10 Inestabilidad económica y financiera

La inestabilidad económica y financiera también es una amenaza común a las tres estrategias. Además, ha tenido especial relevancia debido a las crisis financieras mundiales —la última provocada por los efectos de la pandemia de la COVID-19— y a la creciente globalización económica.

Sin duda, la inestabilidad económica y financiera tiene diversas causas, pero más preocupantes son sus múltiples consecuencias, que repercuten de manera transversal en diferentes sectores y en la ciudadanía. Por tanto, afectan directamente a la Seguridad Nacional. Entre otras muchas causas, se encuentran los desequilibrios macroeconómicos, las actividades ilegales (como el tráfico ilícito) o la corrupción y el uso indebido de los fondos públicos, estos últimos recogidos explícitamente en la ESN de 2021. Por su parte, las consecuencias más preocupantes es la desafección social por las instituciones públicas y el sector privado, y la naturaleza transversal de la economía hace que los efectos nocivos de estas crisis alcancen ámbitos muy diversos.

A las consecuencias ya citadas se le une la fragilidad en la cadena de suministros. La crisis provocada por el COVID-19 puso de manifiesto la importancia de las cadenas globales y las graves consecuencias que existen para la economía mundial si estas se ven interrumpidas.

Por último, la repercusión de esta amenaza puede sentirse no solo dentro de del territorio español, sino que también puede tener consecuencias indeseadas en compatriotas y empresas ubicadas en el extranjero. Por todo ello, y cómo avanzan la política de Seguridad Nacional, debe existir un marco legal y unas medidas flexibles que protejan y minimicen, en la medida de lo posible, las consecuencias de la inestabilidad económica y financiera.

2.2.11 Vulnerabilidad energética

La vulnerabilidad energética es una amenaza para por distintos motivos. En primer lugar, porque la energía es vital para el desarrollo de una sociedad y para mantener la soberanía del Estado, España depende excesivamente del suministro exterior de energía, y porque la baja interconexión con el resto de Europa intensifica la vulnerabilidad, que se acentúa en los territorios extra peninsulares, como las islas Canarias.

Por otro lado, el suministro energético depende de diversos aspectos, y en cada uno de ellos existen distintos peligros. Los aspectos más relevantes son: la existencia de una oferta suficiente en cantidad y precio —cuyo peligro es la inestabilidad en los países suministradores de energía—; la seguridad en las instalaciones y el transporte —esto obliga a mantener la

seguridad de las cadenas de suministro y buscar alternativas en caso necesario—, y, por último, la garantía de una industria energética respetuosa con el medio ambiente, lo que genera la necesidad de emprender una transición energética que evite que el mercado se vea afectado[5].

Se debe considerar el continuo crecimiento de la demanda energética en aquellas regiones del mundo que están en pleno desarrollo. Como consecuencia, los precios de la energía tienden a aumentar y esto puede provocar crisis y enfrentamientos entre países para garantizar su acceso a la energía. Por todos estos motivos, la vulnerabilidad energética de España es una realidad que no se puede ignorar pues, en gran medida, las amenazas que se ciernen sobre ella comprometen la Seguridad Nacional.

2.2.12 Flujos migratorios irregulares

La inmigración ha sido una constante en la historia del ser humano, pero las dinámicas de los últimos años —en especial, por la implicación del crimen organizado— hacen que los flujos migratorios irregulares deban también ser gestionados por su afectación a la Seguridad Nacional. En este sentido, los factores presentes en la inmigración que recibe España han estado presentes en el planeamiento estratégico desde 2013, y serán más importantes aun en los años venideros. Entre los parámetros más relevantes que subyacen en la inmigración, se encuentran la situación geográfica de España, frontera sur de la UE con África; la balanza demográfica, con un aumento de la población en los países africanos y disminución en los europeos; el desequilibrio económico entre la riqueza europea y la pobreza y el subdesarrollo de los países de origen, y, por último, los conflictos, la violencia y la inestabilidad social en dichos países de origen.

Por todo ello, es imprescindible planear y desarrollar una gestión completa e inclusiva de los flujos migratorios que pueda evitar problemas en los países receptores, como la falta de cohesión social; la creación de espacios que dificulten la integración; la frustración de los inmigrantes al no alcanzar sus expectativas laborales y vitales; el rechazo social de la población local; o la posibilidad de sucumbir ante el radicalismo extremista u

[5] En este sentido, la Estrategia Energética Nacional de 2015 identifica las siguientes amenazas para la integridad energética: una actualización insuficiente e inversiones inadecuadas en infraestructuras, actividades fraudulentas en el sector energético, inestabilidad política en los países productores, optimización de la diversificación de los recursos energéticos, amenazas a los países y rutas de aprovisionamiento, conflictos políticos entre países suministradores, consumidores y de tránsito, insuficientes interconexiones energéticas, riesgos percibidos de a generación eléctrica nuclear, accidentes industriales graves, catástrofes naturales, ciberamenazas y amenazas físicas a la infraestructuras energéticas.

otras actividades ilegales que puedan estar asociadas a la clandestinidad y a la exclusión.

En el espacio temporal de las estrategias españolas, desde 2013 a 2021, Europa vivió una de las mayores crisis migratorias desde la Segunda Guerra Mundial, lo que demostró las dramáticas consecuencias que pueden tener unos flujos migratorios descontrolados. Para evitarlo a futuro, y teniendo en cuenta que España y Europa seguirán siendo destino para los migrantes, así como la continua mejora de la movilidad internacional y de las comunicaciones, es necesario establecer respuestas —no solo españolas, sino también, y obligatoriamente, en el seno de la UE— para maximizar los efectos positivos en la sociedad de acogida de una inmigración regulada, que, al tiempo, exige trabajar para evitar su impacto negativo, tanto para las sociedades receptoras como para los propios migrantes.

2.2.13 Emergencias y catástrofes

Las emergencias y catástrofes, ya sean provocadas por fenómenos naturales, por la acción humana o por una combinación de ambas, son una amenaza tan antigua como constante. Sin embargo, hay una serie de condicionantes actuales que pueden potenciar su alcance y sus efectos nocivos que conviene destacar.

En primer lugar, la interconexión propia de la globalización hace que una emergencia o catástrofe lejana pueda tener consecuencias directas sobre España. Asimismo, en el mundo actual, un determinado suceso puede provocar mayores daños y perjuicios que en tiempos pretéritos. En este sentido, una catástrofe o una emergencia no perturbará exclusivamente a la vida, la salud y los bienes patrimoniales directamente afectados, sino que —como consecuencia— también afectará al ámbito económico, al medio ambiente, al suministro de bienes, ya sean energéticos o de otra índole, que pueden ser gravemente dañados.

Además, existen una serie de potenciadores —recogidos en la ESN de 2017— que multiplican los efectos de una catástrofe o emergencia. Estos son el aumento de la población en las zonas urbanas (en ocasiones en áreas más vulnerables) y el descenso en las rurales (que reducen la posibilidad de responder antes a incidentes o accidentes en las zonas más despobladas); la vulnerabilidad económica y tecnológica (ámbitos cada vez más interconectados y en los que la seguridad total es imposible de alcanzar); la degradación de los ecosistemas, que tienen como consecuencia un descenso de las defensas naturales, y, por último, el aumento de los fenómenos adversos, consecuencia del cambio climático.

Sin duda, España es un país con una eficiente red de seguridad ante este tipo de fenómenos, pero las actuales circunstancias y su evolución obligan

a una continua adaptación a las circunstancias que están presentes en las emergencias y catástrofes, y que son fundamentales para articular la mejor respuesta posible.

2.2.14 Epidemias y pandemias

A pesar de que las epidemias y pandemias han sido una constante en el devenir de la historia, en España no aparecen como amenaza hasta la ESN de 2017. Sin duda, esto no significa que este peligro no estuviese presente en la cotidianidad de las personas, pero sí es cierto que cobraron especial trascendencia internacional a partir de epidemias globales como la gripe A (2010) o el ébola (2014). Posteriormente, la pandemia provocada por el virus COVID-19 subrayó la urgencia permanente de prevenir, luchar y erradicar este tipo de amenaza tan dañina para la existencia humana.

Con todo, y aun considerando que las pandemias siempre han sido una amenaza existencial, la posibilidad actual de ocurrencia, expansión y daño sobre la población se eleva si se tienen en cuenta ciertas características del mundo actual. El incremento de la movilidad de la población, gracias a la mejora en el transporte, y el aumento de los grandes núcleos urbanos con alta densidad poblacional son los dos principales aspectos que, hoy en día, incrementan y aceleran la propagación de cualquier enfermedad infecciosa. El riesgo cero no existe ante una amenaza de esta índole, pero existen medidas que pueden reducir la vulnerabilidad de la sociedad, como son las medidas preventivas, la promoción de la salud, los controles e inspecciones sanitarias y, finalmente, las vacunas.

Por todo ello, conviene resaltar que de la crisis del COVID-19 se extrajeron una serie de lecciones aprendidas, con el objetivo de mejorar las futuras respuestas ante situaciones similares. Desde esta premisa, cualquier planeamiento y preparación ante una amenaza similar debe valorar la dificultad en la toma de decisiones y en la distribución de bienes sanitarios, la vulnerabilidad de las cadenas de suministros, la necesaria reducción de la dependencia exterior en algunos sectores estratégicos y las fricciones geopolíticas, además de la complicada cooperación internacional.

2.2.15 Efectos derivados del cambio climático y de la degradación del medio natural

Los efectos del cambio climático aparecen en la ESN de 2013 como un potenciador de los riesgos y amenazas a la Seguridad Nacional. Posteriormente, en 2017, y dada su importancia, los efectos del cambio climático fueron recogidos como una amenaza a la Seguridad Nacional. Entre ellos, el más nocivo probablemente sea la dificultad en el acceso a diferentes recursos —como los hídricos y energéticos—, lo que provoca el

aumento de la inmigración forzada y la tensión en ciertas áreas, que puede derivar incluso en conflictos armados. Otras consecuencias son el aumento de los fenómenos meteorológicos extremos (como las sequías), la inseguridad alimentaria o las hambrunas, así como el incremento de las inundaciones o incendios.

El cambio climático potencia otras amenazas y, por esta razón, se deben tomar todas las medidas para adaptarse al mismo. Además, estas medidas preventivas o reactivas deben implementarse mediante acuerdos internacionales, como corresponde a un fenómeno que tiene una afectación global sobre los seres humanos, más allá de donde habiten.

Por otro lado, y junto a los efectos del cambio climático, la ESN 2021 añadió la degradación del medio ambiente, diferenciando así a estos dos fenómenos. Esta degradación tiene una repercusión muy negativa sobre la biodiversidad, e incide en las mismas consecuencias que el cambio climático. En ambos casos es imprescindible encontrar respuestas que reduzcan la peligrosidad de esta para la Seguridad Nacional.

2.2.16 Campañas de desinformación

Esta amenaza, plenamente asumida en todo el mundo, es la más reciente de las que se recogen en las Estrategias de Seguridad Nacional de España, pues aparece, por primera vez, en la ESN de 2021. Las campañas de desinformación son un fenómeno diferente a las noticias falsas o *fake news*, y también de la información errónea o *misinformation*. En general, las campañas de desinformación distorsionan la realidad, con o sin noticias falsas, para manipular a la opinión pública en un determinado asunto, y siempre con la pretensión de desestabilizar el funcionamiento del Estado y sus instituciones. Además, cobran especial importancia en ciertos momentos, como son las campañas electorales.

La aparición de las campañas de desinformación como amenaza coincide con la contemplación del ámbito cognitivo como un nuevo ámbito, que se añade a los tradicionales (aéreo, marítimo y terrestre), además de los ya mencionados ultraterrestre y el ciberespacio. Asimismo, esta amenaza puede materializarla un agente estatal o no estatal —que puede buscar la polarización de la sociedad, lo que crea un país más débil y menos cohesionado, u opiniones generalizadas basadas en falsedades y de las que se beneficien los agentes— y tienen una difícil atribución, sobre todo cuando emplean medios cibernéticos para su propagación.

2.3 *Catalizadores de las amenazas*

En este epígrafe, se abordarán aspectos que afectan a las amenazas, los riesgos o los desafíos en las tres estrategias. En cada una de ellas han sido

nombrados de una forma diferente —potenciadores, «aspectos que afectan» o características—, pero todas tienen en común que se tratan como moduladores de las amenazas.

2.3.1 Potenciadores (ESN 2013)

En la ESN de 2013, aparecen varios «potenciadores» que pueden hacer que surjan nuevos riesgos y amenazas, o multiplicar los efectos de los ya existentes. El primero de ellos es el cambio climático —en las posteriores estrategias aparece ya como riesgo, amenaza o desafío—, que supone «el gran desafío ambiental y socioeconómico del siglo XXI» (Gobierno de España, 2013). Por otro lado, los cambios climáticos pueden contribuir al incremento de los flujos migratorios descontrolados, aumentar la tensión en diferentes zonas o perjudicar a la economía de las áreas afectadas.

Por su parte, los desequilibrios demográficos suponen otro factor determinante, principalmente por dos aspectos concretos. Por un lado, fomentan los flujos migratorios irregulares, por ejemplo, el desequilibrio demográfico entre África y Europa es un factor de empuje para la inmigración, y además es un potenciador de las amenazas vinculadas a este fenómeno. Y, por otro, la nueva distribución poblacional, más urbana y menos rural, influye en la aparición de diferentes amenazas, epidemias y pandemias o el acceso a los recursos, entre otros, así como la forma de enfrentarnos a ellas.

El uso nocivo de las nuevas tecnologías es otro de los potenciadores en la ESN 2013, que, además, se recoge en las estrategias siguientes, aunque con otras nomenclaturas. Sin duda, los avances tecnológicos brindan una oportunidad de mejora de la sociedad en muchos aspectos, pero no se puede obviar los riesgos que le son inherentes. Así, el desarrollo de las comunicaciones y el transporte, tan beneficios para el bienestar social, también puede ser utilizado por delincuentes o agentes que pretendan desestabilizar a el país o realizar actividades ilícitas. Además, estas nuevas formas de comunicación dificultan la atribución de los actos que en ellas se desarrollan y, al tiempo, son un vehículo eficaz para la transmisión de ideologías extremistas que pueden derivar, en el peor de los casos, en radicalismos violentos.

Otros dos potenciadores relacionados, aunque con importantes diferencias, son la pobreza y la desigualdad. Ambas circunstancias pueden favorecer la radicalización, el crecimiento del crimen organizado o la realización de actividades ilegales que afecten a la Seguridad Nacional.

Por último, la existencia de extremismos ideológicos, muy alejados de la pretendida cohesión social, potencia igualmente la aparición de los riesgos y amenazas ya analizados.

2.3.2 Factores que afectan (ESN 2017)

Además de lo anterior, la ESN 2017 presenta dos factores que, en la actualidad, incrementan y agravan las amenazas y los desafíos que enfrenta la Seguridad Nacional: las acciones híbridas y la revolución tecnológica.

En cuanto a las acciones híbridas, se reconocen como una serie de acciones diferentes con un objetivo común: desestabilizar o influir en una sociedad. Entre otras, la ESN destaca las siguientes acciones que tienen esta consideración «híbrida»: las actividades militares sin necesidad de superar el umbral del conflicto bélico, los ciberataques, la manipulación informativa, y la presión mediante actividades económicas. Todas ellas, aunque no se enmarquen en lo que tradicionalmente se califica como guerra, suponen un factor que puede favorecer la aparición de diferentes amenazas para la Seguridad Nacional española.

El otro factor determinante es la revolución tecnológica, ya mencionado en la ESN de 2013. La tecnología es una herramienta que facilita y mejora la comunicación y el desarrollo de múltiples actividades, pero también puede favorecer la aparición de amenazas. Tanto en 2017 como ahora, es difícil calibrar todos los aspectos de la revolución tecnológica, pero no cabe duda que debe ser un factor a controlar para evitar el mal uso y los efectos negativos de los avances tecnológicos.

2.3.3 Características (ESN 2021)

Los riesgos y amenazas que recoge la ESN 2021 tienen tres características comunes, que, de alguna forma, ya estaban recogidas en las estrategias anteriores. En primer lugar, está la interconexión; es decir, los riesgos y las amenazas no pueden ser tratados como realidades aisladas sin relación entre sí. En este mundo globalizado, la tendencia es el aumento de las conexiones, y la existencia de una amenaza beneficia la aparición de otras, al tiempo que potencia sus efectos.

En segundo lugar, las estrategias híbridas toman un protagonismo vital para entender, en toda su amplitud y de forma integral, las amenazas a la Seguridad Nacional. En este sentido, las acciones híbridas recogidas en la ESN 2013, hechos más aislados, sin necesaria relación, transitan hacia estrategias híbridas, que contemplan acciones combinadas y coordinadas para alcanzar objetivos determinados. Estas actividades orquestadas necesitan materializarse en diferentes acciones, que finalmente se convierten en amenazas como herramienta para lograr sus objetivos finales. Por lo tanto, existe una clara relación entre las estrategias híbridas y la interconexión de las amenazas.

En tercer lugar y, por último, aparece la dimensión tecnológica, que ha sido un factor constante en las tres estrategias. El avance tecnológico

influye más en unas amenazas que en otras, aunque está presente en todas ellas. No hay duda que cualquier avance tecnológico es un aspecto altamente positivo para cualquier sociedad, pero debe desarrollarse, minimizando las vulnerabilidades y garantizando la seguridad de los usuarios y de las actividades que estos desarrollan.

2.4 De dónde provienen las amenazas

En este apartado se analiza de dónde provienen, o pueden provenir, las amenazas. En este sentido, hay tres aspectos importantes: la revolución tecnológica, que ha borrado los límites territoriales y empequeñecido el mundo; la posición geográfica de España, una constante que sigue condicionando la seguridad, y la dimensión política y social, que es un claro objetivo de ciertas amenazas, pero que también provee aliados.

En primer lugar, hay que resaltar que en las tres estrategias se pone de manifiesto que la materialización de las amenazas a la Seguridad Nacional no tiene una delimitación fronteriza. Actualmente, los límites entre seguridad interna, dentro de las fronteras, y externa, más allá del territorio español, son cada vez más difusos.

Esta realidad se sustenta en el desarrollo de las comunicaciones y los transportes, gracias al avance tecnológico que ha hecho el mundo «más pequeño». En este contexto, aunque desde un prisma negativo, la rápida expansión del virus COVID-19 y sus consecuencias ejemplificaron que las distancias, también para las amenazas, son cada vez más cortas.

Otro efecto de la tecnología fue la aparición de internet, hace ya muchas décadas. Sin embargo, aun hoy se reconoce la revolución mundial que supuso el establecimiento del contacto entre dos puntos de forma instantánea. Con el trascurrir del tiempo, se han producido múltiples avances en el ámbito de la comunicación lo que ha acrecentado las posibilidades; pero esta potente herramienta también posibilita acciones ilícitas desde lugares lejanos que socavan la Seguridad Nacional. De esta forma, queda claro que ya no es necesario actuar en España para afectar a su seguridad.

Por último, el desarrollo tecnológico ha servido como multiplicador de ciertas actividades, tanto positivas para el desarrollo (la mayoría de ellas) como perjudiciales para la seguridad. De estas últimas, un claro ejemplo es la posibilidad de lanzar campañas de desinformación de forma más sencilla y con más alcance gracias al uso de internet. Además, otra característica es la difícil atribución de estos actos en la mayoría de los casos.

No obstante, y pese a que la tecnología realmente ha modificado los efectos de las distancias, la geografía sigue siendo vital para predecir las amenazas que más pueden influir a España. En este sentido, y por la

ubicación del país, España está directamente influenciada por todo lo que suceda en el Norte de África y Sahel. Por un lado, la península ibérica está separada por escasas millas de África, y España además es, por la ubicación de las ciudades de Ceuta y Melilla, el único país miembro de la UE que es bicontinental. Por otro, lo que sucede en el Sahel tiene una repercusión directa en las islas Canarias, en términos de flujos migratorios; además de ser un condicionante muy importante para la seguridad y el desarrollo a nivel nacional.

España también es un país mediterráneo y atlántico. Esta doble faceta brinda una oportunidad geoestratégica, pero también existe el peligro de amenazas que utilicen esta singularidad y puedan afectar a la seguridad. En este sentido, hay que resaltar, especialmente, los lazos históricos que unen a España con Iberoamérica, que facilitan el intercambio económico, social y cultural entre ambas regiones, pero también esa proximidad puede ser utilizada por agentes que socaven la Seguridad Nacional.

Un último aspecto que no se puede ignorar es la dimensión política de España: un país occidental, miembro de la OTAN y de la UE. Este hecho hace que comparta las amenazas con sus aliados, ya sea porque estas sean directas a la Seguridad Nacional o porque, conforme a los compromisos adquiridos, deba responder ante amenazas no directas. No obstante, también significa que el país cuenta con firmes aliados que cooperan para dar una respuesta ante estas amenazas, que afectan a más países además de a España.

2.5 *Cómo responder ante las amenazas*

Para completar el análisis de las amenazas contempladas en las tres Estrategias de Seguridad Nacional, estos documentos recogen cómo enfrentarse a cada una de ellas, ya sea de forma individual como colectiva. En las ESN se repite un mismo esquema: identificación de unos ámbitos —que aumentan conforme lo hacen las amenazas—, objetivos a alcanzar en cada uno de ellos y líneas de acción para alcanzarlos. Lógicamente, en todas ellas se nombra al Sistema de Seguridad Nacional como estructura en la que se apoya la gestión de las crisis relativas a la Seguridad Nacional, y en todas sus fases: prevención, detección, respuesta, retorno a la normalidad y evaluación, como recoge la Ley 36/2015.

Además del incremento de los ámbitos de la Seguridad Nacional, la ESN de 2017 recoge una serie de objetivos generales más trasversales: desarrollar el modelo integral de gestión de crisis, promover una cultura de Seguridad Nacional, favorecer el buen uso de los espacios comunes globales; impulsar la dimensión de seguridad en el desarrollo tecnológico y, por último, fortalecer la proyección internacional de España. Estos objetivos, de carácter

amplio, no se focalizan en amenazas concretas, sino que su plasmación e implementación estará presente, en mayor o menor medida, en la respuesta integral a todas ellas. De esta forma se avanza en un ámbito muy importante para garantizar la seguridad: la identificación de respuestas comunes, o al menos con factores comunes de actuación, a las diferentes amenazas.

En ese mismo sentido, la ESN de 2021 concreta una serie de líneas de acción, hasta 33, cuya materialización supondrá un gran avance para el sistema de Seguridad Nacional. Todas ellas están destinadas a alcanzar objetivos en diferentes ámbitos, con el objetivo compartido y general de responder a amenazas específicas en cada uno de ellos; pero, de forma paralela, también establece líneas de acción que pretenden generar una capacidad transversal para responder ante distintas amenazas. Estas líneas de acción son las destinadas a conseguir un «multilateralismo reforzado», la «autonomía estratégica europea» y el «mayor protagonismo en la OTAN». Esta dimensión internacional y cómo son concebidas las amenazas en la Unión Europea y la OTAN se abordará a continuación.

3 Las amenazas en la Unión Europea y en la Organización del Tratado del Atlántico Norte

3.1 Las amenazas en la Unión Europea

La Brújula Estratégica para la Seguridad y Defensa (Consejo de la Unión Europea, 2021) —el último gran documento estratégico de la UE, aprobado en el Consejo de la UE el 21 de marzo de 2022— recoge las distintas amenazas a las que se enfrenta la Unión y sus ciudadanos. En primer lugar, hay que destacar la consideración que atribuye a estas amenazas: «complejas, multidimensionales, transnacionales»; así como la especial relevancia que otorga a las amenazas híbridas y, ya en clave de respuesta, a la articulación de un sistema que permita su detección temprana. Para ello, no solo plantea una serie de medidas de carácter interno de la UE, sino que también contempla la cooperación con otros socios: OTAN, Naciones Unidas, Organización para la Seguridad y la Cooperación en Europa (OSCE), la Unión Africana y la Asociación de Naciones del Asia Sudoriental (ASEAN), además de acuerdos bilaterales con diferentes países. Asimismo, subraya que el cambio climático es un potenciador de todas las amenazas.

En cuanto a las amenazas, la primera que describe es el terrorismo y el extremismo violento. En concreto, se centra en el terrorismo de carácter yihadista, y destaca que esta amenaza se produce dentro y fuera de las fronteras de la Unión, por lo que también puede afectar a los europeos expatriados o a los intereses de la UE en otras regiones. Por otro lado, y respecto a su autoría, reconoce que la pueden materializar terroristas autóctonos o excombatientes retornados.

La proliferación de armas de destrucción masiva es otra de las amenazas recogidas en este documento estratégico de la UE. A este respecto, cita los programas nucleares de Corea del Norte y de Irán, y la proliferación en Rusia y China, y subraya que esta amenaza puede acrecentarse debido al debilitamiento de los sistemas internacionales de control de armamento.

Por otro lado, menciona una serie de amenazas —que pueden ejecutar agentes estatales y no estatales— que se agrupan y son parte de otras formas de influencia y de injerencias en procesos políticos y electorales: las estrategias híbridas, los ciberataques y las campañas de desinformación.

Asimismo, la Brújula Estratégica se refiere a los espacios globales comunes, y su vulnerabilidad, como un ámbito donde diferentes amenazas pueden socavar la seguridad y estabilidad de la UE. Estos son el ciberespacio, cuya vulnerabilidad se ve especialmente afectada debido a su propia naturaleza y a los avances tecnológicos; el espacio ultraterrestre, un nuevo punto de encuentro de los diferentes países y organizaciones y donde pueden surgir desencuentros; los espacios marítimos, que son vitales para la UE debido a la importancia del comercio marítimo y la cantidad de mares que rodean a la UE, y, finalmente, el espacio aéreo, testigo de acciones cada vez más agresivas.

Por último, el cambio climático, la degradación del medio ambiente y las catástrofes naturales también erosionan la seguridad europea. Estos tres aspectos provocan que la lucha por los recursos naturales —la tierra, el mar y los recursos energéticos— sea mayor y más compleja. Adicionalmente, aunque no se recoge como una amenaza en sí, la UE reconoce que las crisis sanitarias mundiales pueden repercutir en las tensiones regionales y erosionar la estabilidad económica.

Además de las amenazas que se mencionan expresamente en este documento estratégicos, hay otras que aparecen citadas de una forma u otra. Entre ellas, están la delincuencia organizada, la instrumentalización de la inmigración irregular, que también puede formar parte de una estrategia híbrida mayor, el revisionismo de Rusia y su entorno, los conflictos armados, la trata de seres humanos y la inestabilidad financiera, así como las diferencias sociales y económicas extremas.

3.2 *Las amenazas en la OTAN*

El Concepto Estratégico de 2022 (Alianza Atlántica, 2022), aprobado en la cumbre de Madrid de junio del mismo año, es el documento de la OTAN más actual donde analizar las amenazas que planean sobre la Alianza.

En primer lugar, el Concepto Estratégico de la OTAN clarifica que la alianza es una organización defensiva, y que su defensa colectiva debe estar preparada para cualquier tipo de amenaza. Por ello, aún de forma implícita, esta referencia estratégica amplía las amenazas más allá de las meramente convencionales. Además, reconoce que, en la actualidad, estas son globales y están interconectadas, lo que incrementa su complejidad. También señala que estas amenazas afectan a los diferentes dominios, con especial énfasis en el marítimo y el ciberespacio.

En cuanto a su autoría, subraya que las amenazas pueden provenir de actores estatales y no estatales, al tiempo que pueden tener una naturaleza militar o ser de carácter meramente civil. Asimismo, incide en la importancia de las amenazas híbridas.

Por otro lado, en el concepto estratégico cobra especial relevancia el terrorismo, que sitúa como principal amenaza asimétrica directa contra la paz y la estabilidad internacional. Además, el terrorismo hace uso de los avances tecnológicos para accionar de forma más compleja, lo que hace más difícil prevenirlas y enfrentarse a ellas.

Otro aspecto de especial trascendencia es que este documento cita expresamente a países que, a través de sus acciones, amenazan a la OTAN. Entre ellos destaca la Federación Rusa, la «amenaza más significativa», que centra sus esfuerzos de forma convencional, mediante estrategias híbridas y en el ciberespacio.

Al tiempo, este concepto estratégico señala que las armas de destrucción masiva son una amenaza global, que está encabezada por países como la Federación Rusa, Irán y Corea del Norte. Esta amenaza, en sus vertientes nuclear, biológica, química y radioactiva, gana protagonismo si se atiende a la erosión de los sistemas de control de armamento y el actual panorama de ausencia de acuerdos en esta materia.

Otro aspecto de gran trascendencia, nombrado en numerosas ocasiones en este documento estratégico, es el cambio climático. Este fenómeno tiene un gran impacto en la generación de crisis, además de ser un efecto multiplicador de las amenazas ya existentes. Por otro lado, el cambio climático fomenta la fragilidad de las instituciones, facilita las emergencias sanitarias y provoca inseguridad alimentaria.

Finalmente, y además de la necesidad de garantizar su capacidad autónoma de defensa colectiva, la Alianza establece que la cooperación internacional, especialmente con la Organización de Naciones Unidas y la Unión Europea, es una de las medidas más eficaces para hacer frente a todas estas amenazas.

4 Conclusión

Después de analizar, aún de forma somera, la plasmación de las amenazas, así como su evolución y trascendencia, tanto en las sucesivas Estrategias de Seguridad Nacional como en los documentos homólogos de la Unión Europa y la OTAN, se destacan las siguientes consideraciones:

— En las Estrategias de Seguridad Nacional de España no existe una diferenciación clara entre amenaza, desafío y riesgo. Tampoco se clarifican cada uno de esos conceptos (excepto en la ESN de 2017), y se tratan de forma similar. Por este motivo, este documento se refiere a todas ellas como «amenazas». Sin embargo, y aun considerando que tanto los desafíos como los riesgos pueden derivar en amenazas, se considera que, más allá de este documento, se les trate de forma diferenciada, lo que mejorará su análisis, así como la elección de la respuesta más idónea.

— Existe amenazas que se mantienen desde la primera Estrategia de Seguridad Nacional y aparecen otras cinco más en las ESN posteriores. Esto demuestra que la evolución de las amenazas significa su aumento y, rara vez, será la desaparición de alguna de ellas. Esta constatación evidencia la necesidad de hacer un continuo análisis del escenario estratégico mundial, que permita dilucidar la permanencia y evolución de las amenazas como «clásicas», así como aquellas nuevas que surgen con fuerza, y que se benefician de aspectos más novedosos como el multidominio o los avances tecnológicos.

— Las amenazas cada vez son más complejas, se desarrollan en varios dominios de forma simultánea, están más conectadas y se difuminan sus límites. Además, se amplían sus efectos que, como en el caso de la pandemia de la COVID 19, pueden afectar a ámbitos como la vulnerabilidad energética, la inestabilidad económica y financiera. Asimismo, ha surgido con más fuerza la amenaza que suponen las campañas de desinformación, capaces de desestabilizar a los regímenes democráticos y socavar el funcionamiento de las instituciones estatales.

  Asimismo, los límites de las amenazas son cada vez más difíciles de delimitar. Los causantes son actores estatales o no estatales, las amenazas lejanas a las fronteras afectan a España borrándose los límites entre lo externo e interno. Y, por último, se amplían continuamente. Así, se pasa de conflictos armados a tensión estratégica y regional, al terrorismo se le une la radicalización violenta y al crimen organizado la delincuencia grave.

— Existen elementos comunes que catalizan las amenazas. El principal es la dimensión o la revolución tecnológica que facilita las acciones que conllevan una amenaza. Además, la mejora de las comunicaciones y los transportes favorece la interconexión. Asimismo, la

preponderancia de las estrategias híbridas en los últimos años hace que puedan existir diferentes amenazas a la Seguridad Nacional con un objetivo común. Por otro lado, aspectos sociales como la desigualdad y la pobreza o los extremismos ideológicos pueden convertirse en potenciadores de numerosas amenazas.

— El origen de las amenazas es diverso y multifactorial. En España, existen tres factores —uno que afecta a todo el planeta y dos singulares— determinantes de su potencialidad: la revolución tecnológica, la situación geoestratégica de España —país mediterráneo y atlántico, frontera sur de la Unión Europea con África— y su dimensión política y social, como miembro de la OTAN, la UE y otras organizaciones internacionales.

— Todas las respuestas a las amenazas comparten una base común. Pese a que las amenazas son de diversa índole, las respuestas que se proponen en las ESN tienen aspectos comunes. La propia naturaleza de las amenazas actuales obliga a una respuesta integral: todas las capacidades del Estado coordinadas para articular y ejecutar la respuesta más firme frente a cualquier amenaza presente o futura. En este sentido el Sistema de Seguridad Nacional es clave en la respuesta, ya que permite una coordinación reforzada ante amenazas de naturaleza trasversal.

— Las amenazas contempladas en las ESN de España están en la misma línea que las de la Unión Europea y la OTAN. Esta constatación refuerza la idea de que es necesaria la mayor cooperación internacional posible para erradicar cualquier tipo de amenaza, más allá del lugar donde se origen y expande, desde el pleno convencimiento de que las amenazas globales obligan a respuestas conjuntas.

Bibliografía

Consejo de la Unión Europea. (2022). *Una Brújula Estratégica para la Seguridad y la Defensa*. Bruselas. [Consulta: 28 de febrero de 2024]. Disponible en: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf

España. (2015). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. *Boletín Oficial del Estado*. 29 de septiembre. N.º 233, p. 10389.

Gobierno de España. (2013). *Estrategia de Seguridad Nacional 2013.Un proyecto compartido*. IEEE. [Consulta: 28 de febrero de 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/Estrategia_Seguridad_Nacional_2013.pdf

—. (2017). *Estrategia de Seguridad Nacional 2017.Un proyecto compartido de todos y para todos*. Departamento de Seguridad Nacional.

[Consulta: 28 de febrero de 2024]. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2017

—. (2021). Estrategia de Seguridad Nacional 2021. Un proyecto compartido. Departamento de Seg uridad Nacional. [Consulta: 28 de febrero de 2024]. Disponible en: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

Ministerio de Defensa. (2022). Nuevo Concepto Estratégico de la OTAN. Madrid. [Consulta: 2024]. Disponible en: https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

Tzu, S. (2009). *El arte de la guerra*. Madrid, Ediciones Obelisco S. L. ISBN: 978-84-414-3815-6.

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

José María Gil Armario

Resumen

Las amenazas a la Seguridad Nacional constituyen una prioridad del Estado español. La comprensión de las amenazas supone uno de los cometidos de las unidades, centros y organismos de inteligencia e información del Estado, así como el asesoramiento al Sistema de Seguridad Nacional.

Con el presente artículo se pretende potenciar la comprensión de las amenazas como sistemas complejos sociales y proponer su estudio a través de la aplicación de técnicas analíticas estructuradas, modelado de sistemas y herramientas de inteligencia artificial.

Esta comprensión exige un cambio de paradigma en la elaboración de inteligencia: del ámbito cualitativo del juicio de experto, al ámbito mixto (computacional) de un grupo de expertos multidisciplinar. También implica la inclusión en los currículo de formación y especialización de las técnicas analíticas estructuradas y contenidos de ciencias de la computación.

Entre una propuesta eminentemente cualitativa dependiente del juicio de experto y la opción futurista de herramientas computacionales autónomas de inteligencia artificial se encuentra, en un estadio intermedio, el modelado lógico de las amenazas. El modelado lógico de las amenazas como problemas complejos sociales, generado a partir de grupo multidisciplinar de expertos mediante la aplicación de técnicas analíticas estructuradas, constituye el nivel más básico de comprensión. La integración de herramientas de inteligencia artificial en la consecución de un modelado físico de problemas complejos constituye, hoy por hoy, el camino a recorrer por las organizaciones de inteligencia.

Palabras clave

Complejidad, Computación, TAE, Dinámica de Sistemas, Pirámide invertida.

The understanding of threats to National Security as complex social systems. Application of structured analytical techniques, systems modeling and artifical intelligence

Abstract

Threats to National Security constitute a priority for the Spanish State. Understanding these threats is one of the missions of the intelligence and information units, centers, and agencies of the State, as well as advising the National Security System.

The purpose of this article is to enhance the understanding of threats as complex social systems and to propose their study through the application of structured analytical techniques, systems modeling, and artificial intelligence tools.

This understanding requires a paradigm shift in intelligence development: from the qualitative realm of expert judgment to the mixed (computational) realm of a multidisciplinary group of experts. It also entails the inclusion of structured analytical techniques and computer science content in training and specialization curricula.

Between an essentially qualitative proposal dependent on expert judgment and the futuristic option of autonomous computational tools of artificial intelligence lies, in an intermediate stage, the logical modeling of threats. Logical modeling of threats as complex social problems, generated from a multidisciplinary group of experts through the application of structured analytical techniques, constitutes the most basic level of understanding. The integration of artificial intelligence tools in achieving a physical modeling of complex problems is, at present, the path to be pursued by intelligence organizations.

Keywords

Complexity, Computing, Structured Analytic Techniques, Systems Dynamics, Inverted Pyramid.

1 Introducción

Las amenazas a la Seguridad Nacional constituyen una prioridad del Estado español. Esta se ve reflejada, entre otras evidencias, en la supremacía de la normativa que lo regula y en los recursos puestos al alcance de las Administraciones Públicas para conseguir la protección de los intereses nacionales. La comprensión de las amenazas constituye uno de los cometidos de las unidades, centros y organismos de inteligencia e información del Estado (en adelante UCO), así como su asesoramiento al Sistema de Seguridad Nacional.

La comprensión de las amenazas en el contexto actual y futuro de la sociedad occidental, y en el caso de España, se lleva a cabo mediante diferentes metodologías de investigación científica y técnicas de análisis. Esta diferente tipología de empleo dependerá, entre otros factores, de: las UCO que las pongan en práctica, el desarrollo e implementación tecnológica, el tiempo disponible para su comprensión y los datos que disponga sobre la amenaza.

Con el presente artículo se pretende potenciar la comprensión de las amenazas como sistemas complejos sociales y proponer su estudio a través de la aplicación de técnicas analíticas estructuradas (en adelante TAE), modelado de sistemas y herramientas de inteligencia artificial. Además, concienciar a los analistas y oficiales de inteligencia (y también a sus UCO) de la importancia de alcanzar competencias en pensamiento crítico, trabajo colaborativo y competencias digitales. Y finalmente, mostrar didácticamente las posibilidades de comunicación escrita de la argumentación en pirámide invertida.

Con ese propósito, se centra su estudio en si las UCO necesitan potenciar las competencias colaborativas en equipos multidisciplinares (aplicación de técnicas analíticas estructuradas), competencias analíticas y sistémicas (modelado lógico de sistemas) y competencias digitales en ciencias de la computación (modelado físico de sistemas con inteligencia artificial) para la comprensión de las amenazas a la Seguridad Nacional, así como de sus fenómenos emergentes.

El artículo ha sido elaborado con una metodología de investigación inductiva, mediante un análisis de fuentes documentales publicadas sin clasificación de seguridad y de acceso directo o por internet; así como aportaciones de taller de expertos. Se encuentra dividido en cuatro apartados, claramente diferenciados, y otro de conclusiones. La argumentación se ha centrado en la aplicación de la técnica de pirámide invertida, centrada su inferencia principal al inicio del argumento seguido de sus premisas que lo fundamentan.

Las amenazas a la Seguridad Nacional inician el contenido del documento. Se centra su exposición en la normativa española que las regula, elementos que la integran, tipologías y sus características. Finalmente, se abren las posibilidades de profundización de su comprensión por el estudio del problema de la situación actual, así como escenarios futuros.

A continuación, se analiza los sistemas complejos, en especial los sistemas complejos sociales. Tras establecer su definición y características, se infiere cognitivamente las amenazas como problemas sociales complejos, así como los problemas sociales complejos como representaciones gráficas de modelado de sistemas complejos. Se mencionan las metodologías investigación científica y las técnicas de apoyo a la decisión. Entre las técnicas cualitativas destacan las técnicas analíticas estructuradas, en las cuantitativas, el modelado de sistemas e integración de inteligencia artificial.

Continúa el texto con el estudio cualitativo de problemas complejos mediante las TAE. Se trata el objetivo, definición y tipología de las TAE, así como su aportación al pensamiento crítico. Para finalizar, se plantea la alternativa de profundizar en el análisis cuantitativo de los problemas complejos.

El siguiente apartado se centra en el estudio cuantitativo de los problemas complejos, a través del modelado de sistema y la aplicación de la inteligencia artificial (IA). Además, se expone las bases para el modelado lógico de sistemas complejos y las propuestas de mejora de los procesos de integración de la IA para el modelado físico de sistemas complejos.

Finaliza el artículo con unas conclusiones de los aspectos más relevantes tratados en los apartados precedentes.

Inevitablemente se presentan limitaciones en el artículo que tienen su origen en el autor y en la materia de estudio. Por el autor, en no constituir una autoridad en ciencias de la complejidad y de la computación; así como tener un perfil eminentemente docente en esta área del conocimiento. Por la materia de estudio, al circunscribirse a las amenazas nacionales a la Seguridad Nacional en España y con un contenido fuera de las materias de clasificación de la seguridad.

2 Amenazas a la Seguridad Nacional

Las amenazas a la Seguridad Nacional quedan definidas en la supremacía de la legislación española a través de la Ley de Seguridad Nacional (LSN), y en posteriores desarrollos reglamentarios. Esta ley afecta tanto a Administraciones Públicas como a personas físicas y jurídicas. Los servicios de inteligencia e información del Estado apoyarán de forma permanente al Sistema de Seguridad Nacional en lo concerniente a la prevención y detección de las amenazas y contribución a su neutralización.

En lo concerniente a las Fuerzas Armadas, y desde la perspectiva de la Defensa Nacional, cobra gran importancia la detección y valoración de las amenazas. Destacan los instrumentos y procedimientos para la comprensión de las amenazas (actuales y emergentes) y la generación de indicadores de alerta.

La comprensión de las amenazas queda supeditada principalmente a sus características principales, a los vectores de transformación que incidan en ellas y a los actores intervientes.

Se identifica una amenaza como toda circunstancia real que ponga en peligro la seguridad (PDC 01, 2018). A nivel nacional, el estudio de las amenazas se centra en aquellas que pongan en peligro la Seguridad Nacional. Según el artículo 3 de la Ley 36/2015 sobre la Seguridad Nacional (LSN) el objeto de protección de la Seguridad Nacional lo constituye **«**[…] la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos».

La LSN será de aplicación a las Administraciones Públicas y, según su desarrollo normativo, a las personas físicas o jurídicas (artículo 2 LSN). Los estados de alarma y excepción contemplan su propio desarrollo normativo. Los componentes fundamentales de la Seguridad Nacional son la Defensa Nacional (en adelante Defensa), Seguridad Pública (en adelante Seguridad) y la Acción Exterior (artículo 9.1 LSN).

Dentro de las unidades, centros y organismos de las Administraciones Públicas, los servicios de inteligencia e información del Estado tienen una especial participación en la prevención y detección de las amenazas y contribución a su neutralización. Estos servicios dentro de sus competencias «[…] apoyarán permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas […]» para los fines expuestos (artículo 9.2 LSN).

Desde la perspectiva de la gestión de crisis a la Seguridad Nacional, en el ámbito de la Defensa Nacional por parte de las Fuerzas Armadas, tiene gran relevancia la detección y valoración de las amenazas concretas mediante instrumentos de prevención y detección (PDC 01, 2018: 36). Entre los principales instrumentos destacan la comprensión de la amenaza y la generación de indicadores de alerta (PDC 01, 2018: 35).

Las amenazas que afectan a la seguridad de España se concretan en la Estrategia de Seguridad Nacional (ESN) en el artículo 4.3 de la LSN. La ESN contendrá, además, el análisis del entorno estratégico, la definición de las líneas de acción estratégicas y la promoción de la optimización de los recursos existentes. Los ámbitos de especial interés para la Seguridad Nacional, entre otros (artículo 10 LSN), en los que se lleva a cabo medidas

organizativas, vigilancia y protección son: la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente.

Las principales características que definen las amenazas a la Seguridad Nacional están reflejadas en el capítulo 3 del Real Decreto 1150/2021 de la Estrategia de Seguridad Nacional (ESN, 2021):

- Dinamismo. Se conciben de una manera dinámica, no estática.
- Interdependencia. Interconexiones entre distintas amenazas.
- Tecnológica. Papel primordial de la tecnología en su implementación.
- Efectos en cascada, como consecuencia de su interrelación.
- Prominencia de las estrategias híbridas.
- Autoría de composición compleja o de difícil identificación (PDC 01, 2018: 19).

Además, las amenazas pueden verse influenciadas por vectores de transformación (potenciadores de cambio) entre los que la ESN define: el contexto geopolítico, el entorno socio-económico, la transformación digital y la transición ecológica.

La ESN contempla un mapa de amenazas actuales[1], que se podría ampliar con la publicación doctrinal conjunta PDC-01 de las Fuerzas Armadas[2]. Los actores que materializan las amenazas tienen una especial importancia a la hora de diferenciarlas, entre los que se mencionan: los potenciales adversarios, terroristas transnacionales, organizaciones criminales, facciones y grupos paramilitares sin estado propio, apoyados o no por terceras potencias, y también adversarios de composición compleja o de difícil identificación (PDC 01, 2018: 19).

---

[1] En el capítulo 3 del Real Decreto 1150/2021, de 28 de diciembre, sobre la estrategia de Seguridad Nacional se describe un mapa de riesgos y amenazas a la Seguridad Nacional en el que se pone de relieve «[...] dinamismo e interdependencia, en un entorno de seguridad donde las estrategias híbridas ganan protagonismo [...]»: tensión estratégica y regional; terrorismo y radicalización violenta; epidemias y pandemias; amenazas a las infraestructuras críticas; emergencias y catástrofes; espionaje e injerencias desde el exterior; campañas de desinformación; vulnerabilidad del ciberespacio; vulnerabilidad del espacio marítimo; vulnerabilidad aeroespacial; inestabilidad económica y financiera; crimen organizado y delincuencia grave, y flujos migratorios irregulares.

[2] En la PDC 01, en la página 19, se describen los riesgos y amenazas entre los que se resaltan: el terrorismo y los ataques cibernéticos; la limitación de acceso a los recursos y la injerencia y apropiación de los espacios comunes globales; los efectos derivados de conflictos locales y regionales, como el tráfico ilegal de armas y personas, la dispersión de combatientes o los flujos migratorios; las catástrofes, naturales o no; la proliferación de armas de destrucción masiva; el crimen organizado; la inestabilidad económica y financiera; la manipulación de la información; la vulnerabilidad energética; las pandemias, y los efectos del cambio climático.

Desde la perspectiva de la Inteligencia Militar, **«**[…] la complejidad de las operaciones obliga a disponer de una Inteligencia que integre la información proporcionada por una gran variedad de fuentes y órganos, al objeto de alcanzar un perfecto conocimiento del entorno operativo» (PDC 02, 2020: 35). Se precisa una comprensión de la situación actual de las amenazas y de los actores que intervienen en su materialización (directa o indirecta), de las tendencias de cambio y de sus evoluciones a nuevos fenómenos (PDC 02, 2020: 36). El conocimiento de la situación actual se conoce metodológicamente como estudio del problema de la situación actual (estudio del problema)[3]. Las tendencias de cambio y evoluciones se denominan **«**escenarios de futuro probables y posibles**»**, que requieren de una comprensión y predicción del problema objeto de estudio (amenazas y actores). Una casuística especial son los escenarios de futuro imposibles o ciencia ficción, precisando integrar elementos de la situación actual que se desconocen.

La transición del estudio del problema de la amenaza actual a los escenarios futuros de las nuevas amenazas exige analizar las relaciones y los elementos que experimentan un cambio de tendencia o permanecen inalterables; los que evolucionan de forma drástica y aquellos que emergen, creando nuevo fenómeno (emergencia).

Las características principales de las amenazas a la Seguridad Nacional, objeto de tratamiento a lo largo del artículo, serán la composición compleja de elementos (actores, variables y relaciones), el dinamismo de su comportamiento, la interconexión e interdependencia de los elementos que conforman la amenaza y hacia otros ajenos, así como su emergencia a nuevas amenazas.

A continuación, con el estudio de los sistemas complejos por parte de las ciencias de la complejidad se podrán identificar sus principales características, tipologías de sistemas complejos y sus metodologías de estudio. Los sistemas complejos sociales se integran en el ámbito social de los sistemas complejos, entre los que se podría incluir las amenazas a la Seguridad Nacional por sus características definitorias.

Las amenazas a la Seguridad Nacional, para su comprensión cognitiva, se inferirán como problemas complejos sociales a través de la representación gráfica del modelado de sistemas.

[3] En la página 36 de la PDC 02 se define comprensión como «desarrollo de un profundo conocimiento de la situación». Además, la comprensión del entorno como «[…] percepción e interpretación de una situación particular, con la finalidad de definir el contexto, concretar la visión y su evolución previsible». Contexto, visión y evolución que resultarán elementos imprescindibles para la toma de decisiones.

3 Amenazas a la Seguridad Nacional como sistemas complejos sociales. Metodologías de investigación científica

Las amenazas a la Seguridad Nacional comparten las principales características de los sistemas complejos que se estudian en las ciencias sociales (sistemas complejos sociales). En este sentido, la comprensión de las amenazas precisa de una perspectiva metodológica ad-hoc de las investigaciones científicas. Estas se basan, entre otros aspectos, en la delimitación del "estudio del problema" y el establecimiento de cuestiones a responder del problema planteado. En este caso, el problema de estudio de las amenazas a la Seguridad Nacional se constituye cognitivamente como problema complejo social.

Las ciencias de la complejidad se interesan por los sistemas dinámicos no lineales de complejidad creciente. Entre estos, son de interés del presente artículo, aquellos sistemas que se modulan como problemas complejos por las ciencias sociales. Las características principales que destacan en los problemas complejos sociales serán la dinámica, complejidad y emergencia del sistema.

En el ámbito del pensamiento sistémico de las ciencias de la complejidad, cada problema complejo se compone de un sistema de (sub)problemas (complejos, complicados y simples) y así, sucesivamente. La comprensión de los problemas complejos sociales precisa del desarrollo de capacidades cognitivas de razonamiento del analista; la investigación científica desde diferentes disciplinas de conocimiento científico (ciencias naturales, sociales, de la complejidad y computacionales); y la aplicación de técnicas de análisis de apoyo a la decisión (cuantitativas y cualitativas).

La elección de las metodologías de investigación (multidisciplinar) y las técnicas de análisis de apoyo a la decisión dependerá del sistema complejo objeto de estudio, del tiempo y datos disponibles.

La definición de sistema se aproxima a un «complejo de elementos interactuantes», que dependerán del número y la tipología de elementos y sus relaciones (Bertalanffy, 1976: 54). Al hablar de sistemas complejos, estos presentan una complejidad intrínseca (tanto estructural como funcional) que generan dificultad en su comprensión, explicación y predicción (Galán, 2014: 7; Quintana y Alayón, 2022: 26).

Entre las principales características que definen los sistemas complejos destacan (Galán, 2014: 50):

— Configuración como un todo, compuesto por muchas entidades de una o varias tipologías que se interaccionan entre sí.

- Organización de las entidades en diferentes niveles o capas, donde cada nivel está compuesto por subsistemas que, a su vez, pueden estar compuestos por otros subsistemas, y así sucesivamente.
- Cambio del sistema con el tiempo y de forma constante (dinamismo).
- No linealidad del comportamiento del sistema bajo la expresión de la suma de los comportamientos de sus entidades.
- Emergencia del comportamiento, a través de las interacciones de las entidades del sistema. Emergencia como «[...] surgimiento de estructuras, patrones y propiedades nuevas y coherentes durante el proceso de autoorganización en los sistemas complejos» (Goldstein, 1999).
- Proceso espontáneo y autónomo de modificación de la estructura y su comportamiento, en busca de un orden (autorganización).
- Interdependencia entre las entidades del sistema. La interdependencia genera la emergencia en el comportamiento del sistema. Acciones en una entidad del sistema pueden provocar efectos en otras entidades sobre las que esta tiene influencia, propagándose el efecto y pudiendo tener consecuencias en diferentes áreas del sistema.
- Las entidades y sus interacciones marcan el comportamiento y evolución del sistema en cada instante, dependiendo del estadio temporal anterior y provocando cambios impredecibles futuros (complejidad).

La sociedad contemporánea occidental se enfrenta a una multitud y diversidad de cuestiones que debe de clarificar en su devenir en la protección y defensa de sus ideales. Estas cuestiones, denominados problemas sociales, son estudiadas por las diferentes áreas y disciplinas del conocimiento, a través de las metodologías de investigación social y técnicas análisis.

Un fenómeno social, y, por ende, un problema social, es único e irrepetible, en las mismas condiciones generales y particulares (Gordo y Serrano, 2008: 17). Las particularidades de los problemas sociales requieren una constante adaptación y creatividad en los métodos y técnicas de investigación para la consecución de objetos de investigación específicos en contextos concretos (Gordo y Serrano, 2008: 18).

La ciencia de la complejidad se interesa por fenómenos y comportamientos de sistemas dinámicos no lineales de complejidad creciente (Maldonado, 2008: 160), es decir, se interesa por los sistemas complejos que se modulan como problemas complejos. Como se mencionó anteriormente, los sistemas complejos se caracterizan, entre otras, por una dinámica global del sistema (que no se explica como la suma de las dinámicas locales de cada una de las partes), en la complejidad de sus elementos (variables, relaciones y actores) y por la emergencia de su comportamiento.

Se requiere, por tanto, de metodologías de investigación y técnicas de análisis capaces de estudiar la dinámica del sistema, tanto desde la perspectiva global del sistema como de cada una de las partes que las componen (Galán, 2014: 8). Su análisis y conocimiento será dinámico, incompleto e incierto (Somiedo, 2018: 169-170). Además, la complejidad de sus elementos y sus relaciones (Adamsen, 2000; Agüero, 2010; Quintana y Alayón, 2022) le confiere a su comportamiento un carácter de **«**[...] fenómeno emergente, y no ya causal» (Maldonado, 2008: 159).

Los procedimientos y recursos que se empleen para la resolución de problemas de sistemas complejos, así como las competencias del perfil profesional del analista y del oficial de inteligencia, constituyen los principales elementos diferenciadores de las organizaciones e instituciones (Adamsen, 2000).

Desde la perspectiva del pensamiento sistémico de las ciencias de la complejidad, **«**un problema complejo está integrado por un sistema de (sub) problemas, con un número indeterminado de (sub) problemas complejos, complicados y simples**»**. A su vez, cada (sub) problema contendrá su propio sistema de (sub) problema. Así, sucesivamente.

En este caso, los problemas complicados lo conformarían aquellos sistemas que **«**[...] la relación entre la causa y efecto no está clara, el grado de incertidumbre no es elevado y se pueden incorporar expertos que la reduzcan y naveguen por ella que alcancen con garantías una solución» (Quintana y Alayón, 2022). Son problemas con sistemas reducibles y, por tanto, predecibles.

Por otra parte, los problemas complejos son aquellos sistemas cuya resolución es imposible por las dimensiones y niveles de la realidad de estudio en constante transformación, y que requieren aproximaciones multidisciplinares para su comprensión (Gordo y Serrano, 2008).

El proceso de observación, razonamiento y conocimiento del ser humano sobre las regularidades del mundo ha sido evolutivo desde sus inicios, siendo el método científico el utilizado durante los últimos tres siglos en la civilización occidental (Checkand, 1993: 17). Las diferentes disciplinas del conocimiento de la investigación científica tienen elementos comunes y diferenciadores. Entre las diferencias destacan el objeto de estudio y la finalidad de la investigación (Cruz, 2016: 75-76). Las ciencias de la naturaleza buscan la explicación de su objeto de estudio, mientras que las ciencias sociales su compresión.

En las ciencias de la naturaleza, la investigación científica se basa en el método deductivo como proceso de descubrimiento de las leyes que determinan dicha realidad. Su objeto de estudio es la realidad material.

En las ciencias sociales, la investigación científica se basa en el método inductivo. La estrategia de investigación está condicionada por el propio objeto que se persigue comprender, el equipo investigador, el contexto y el momento en el que se desarrolla (Gordo y Serrano, 2008: 17). El objeto de investigación social es descubrir la realidad y desarrollar su comprensión abstracta.

Sin embargo, con la disrupción de los avances tecnológicos de las ciencias de la computación en la sociedad occidental, estos procesos de conocimiento se han fusionado en metodologías mixtas (inductivo-deductivo), orientándolos a ciclos de ensayo error más reducidos y basados en el principio de utilidad (Checkand, 1993: 17).

Según Whitten, «[...] no hay herramienta, técnica, proceso o metodología perfecta en todas las situaciones. Pero los conceptos y principios del pensamiento de sistemas siempre le ayudarán a adaptarse a situaciones nuevas y diferentes» (Whitten et *al*., 2008: 14). La comprensión de los sistemas complejos se puede alcanzar mediante las capacidades cognitivas de razonamiento del ser humano, así como mediante técnicas de análisis de apoyo a la decisión (figura n.º 1). Entre estas técnicas de análisis de apoyo se encuentran aproximaciones cualitativas, tales como las técnicas analíticas estructuradas (TAE); cuantitativas, en concreto los sistemas computacionales que integran *hardware*, *software* y datos en dichas tareas (Heuer y Pherson, 2015; Maldonado, 2008).

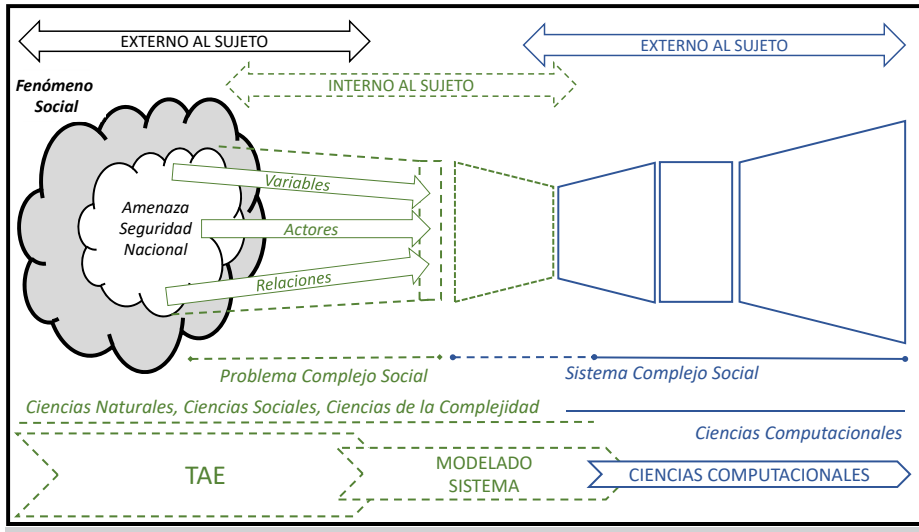

Figura 1. Ciencias del conocimiento y metodologías en sistemas complejos.
Fuente: elaboración propia

En el siguiente apartado se profundizará en la aplicación de las técnicas analíticas estructuradas a problemas complejos. Constituye una

metodología de investigación inductiva y deductiva que usa técnicas de análisis de información cualitativa procedente de juicio de expertos.

4 Estudio cualitativo de problemas complejos: técnicas analíticas estructuradas

Las técnicas analíticas estructuradas (TAE) proporcionan al analista o experto (equipo de analistas/expertos) un pensamiento crítico, independiente y alternativo en la elaboración de inteligencia para el asesoramiento en la toma de decisiones. Bajo metodologías de razonamiento deductivas e inductivas, se ponen en práctica procedimientos eminentemente cualitativos de análisis de información a partir de juicios de expertos. Especial interés tiene su aplicación en la comprensión de problemas complejos con la participación de un grupo de expertos, con un limitado tiempo de ejecución y dificultades de obtención datos cuantitativos.

Las técnicas analíticas estructuradas (TAE, en español) o *Structured Analytic Techiques* (SAT, en inglés) tienen su origen en amplia gama de prácticas de análisis en el ámbito de la inteligencia a partir de la década de los ochenta del siglo XX de la mano de Jack Davis, bajo la denominación de «Análisis Alternativo», y del director adjunto de la CIA Robert Gates. El análisis de los informes de los ataques terroristas del 11 de septiembre de 2001, la posesión de armas de destrucción masiva en Irak y la Ley de Reforma de las Inteligencia de EE. UU. del 2004 incentivaron el impulso de las técnicas analíticas estructuradas sobre la información y sus conclusiones en los análisis de inteligencia (Heuer y Pherson, 2015: 34).

Su objetivo principal es conseguir un pensamiento crítico e independiente del analista, o de su equipo, así como perspectivas alternativas de asesoramiento (proporcionando una visión más amplia de la situación) a la hora de respaldar la toma de decisiones (OTAN, 2024). Estas TAE posibilita que el pensamiento sea visible, observable, compartido, criticado y reformulado por otros analistas (Heuer y Pherson, 2015: 35).

Las TAE son un conjunto de técnicas de análisis de problemas complejos mediante metodologías razonamiento deductivas e inductivas. Estas técnicas utilizan principalmente procedimientos cualitativos de análisis información en actividades de colaboración de un equipo de trabajo (Heuer y Pherson, 2015: 48). Los procedimientos cuantitativos de análisis de datos se llevan a cabo en un nivel básico, sobre todo en tareas de visualización de datos y evaluación de la información obtenida (priorización y ponderación).

La elección de la secuencia de las TAE dependerá, en primera instancia, de la pregunta a responder por el analista a partir problema complejo de estudio.

Posteriormente, la finalidad del estudio, el equipo de trabajo, el tiempo disponible para su desarrollo y la información a emplear constituirán los principales condicionantes en la elección y empleo de las TAE. Entre las TAE que todo analista de inteligencia debería dominar se encuentra: tormenta de ideas estructurado, matriz de impacto cruzado, comprobación de asunciones claves, análisis de hipótesis competidoras (ACH), indicadores, análisis premorten, autocrítica estructurada y análisis *What if?* (Heuer y Pherson, 2015: 56-58).

En el 2000 Robert D. Folker publica en el *Joint Millitary Intelligence College* un artículo sobre **«**la mejora del análisis cualitativo en Inteligencia mediante metodologías estructuradas**»**, llevando a cabo un estudio experimental del uso de técnicas analísticas estructuradas y técnicas de análisis intuitivas (Folker, 2000: 15). A partir de este la investigación planteada se mencionan las diferentes aportaciones al análisis de inteligencia de las TAE (Folker, 2000: 32).

- Se requiere formación y capacitación del analista en la selección y combinación de las TAE para el problema complejo.
- Se genera mejores argumentos para la fundamentación de la pregunta de investigación planteada.
- Se garantiza que el análisis se realice y no se pase por alto (Folker, 2000: 32)[4].
- Se emplea el tiempo disponible de forma eficiente (Heuer y Pherson, 2015: 33)[5].
- Se lleva a cabo un análisis con los datos disponibles, aunque sean incompletos.
- Se aplican procedimientos definidos y abiertos a una revisión posterior con información nueva.
- Se mejora la claridad en el análisis de escenarios.

En la aplicación de este tipo de TAE destaca la importancia del rol del facilitador. El facilitador constituye un guía en la selección de los expertos, técnicas a aplicar, datos a utilizar y producto de difusión a emitir. La selección de expertos debe comprender la mayor amplitud posible de áreas de conocimiento (equipo multidisciplinar), atendiendo al problema complejo a tratar.

En la comprensión de problemas complejos sociales tiene especial interés la aplicación de las TAE en: la delimitación, profundidad y amplitud, del «estudio del problema»; la definición de la pregunta a responder en el asesoramiento; la identificación de los elementos del problema complejo

[4] Según Folker, el análisis es una función a la que la mayoría de los analistas no asignan un tiempo específico, puesto que creen que se produce automáticamente a partir de la recopilación de la información y preparación para la difusión.

[5] Según Heuer y Pherson, el empleo de las TAE ahorra tiempo al analista y al equipo de analistas en la coordinación de actividades, en la obtención e interpretación de evidencias, así como en la revisión y comunicación del producto de inteligencia a niveles superiores.

(variables, actores y relaciones) y en la búsqueda de fuentes de obtención de datos.

En opinión de Somiedo (2018: 162), la formación de metodologías de análisis de inteligencia estratégica en los cursos y postgrados universitarios españoles se ha centrado históricamente en las técnicas analíticas estructuradas y en la publicación de Heuer y Pherson. En el ámbito universitario y post universitario no se profundiza en los métodos de carácter cuantitativo (métodos cuantitativos, usando datos empíricos y métodos cuantitativos, utilizando datos generados por expertos (Heuer y Pherson, 2015: 33)).

Según Somiedo (2018: 163), se requiere una profundización en la metodología de investigación científica deductiva de análisis cuantitativo en Inteligencia, puesto que en la actualidad existen áreas del conocimiento y criterios para poder desarrollar el núcleo fundamental de las metodologías cuantitativas.

> «[...] en España nos hemos focalizado demasiado (y en gran medida muchos programas siguen haciéndolo) en las SAT, que, salvo excepciones como el ACH, están más orientadas al análisis cualitativo, olvidando la importancia y el peso que deberían tener en los programas formativos otras técnicas cuantitativas [...]. Esto es comprensible en una disciplina que apenas comenzaba a dar sus primeros pasos en nuestro país y cuyos programas estaban aún en desarrollo, pero no lo es ahora, cuando ya tiene el recorrido y el criterio suficientes para poder distinguir con claridad el núcleo fundamental de la metodología de análisis en inteligencia».

Una perspectiva intermedia entre las metodologías de investigación científicas inductivas con técnicas de análisis cualitativas de Heuer y Pherson y las deductivas con técnicas de análisis cuantitativos de Somiedo se encontraría en las metodologías de investigación de las ciencias de la complejidad, a través de la perspectiva del estudio de sistemas complejos. Los sistemas complejos se modelan como problemas complejos, con la aplicación de metodologías de investigación científicas mixtas (inductiva-deductivas), a través de ciencias de la computación.

5 Estudio computacional de problemas complejos: modelado de sistemas y aplicación de inteligencia artificial

5.1 *Ciencias de la computación y el modelado de sistemas en problemas complejos*

Las ciencias de la complejidad constituyen la perspectiva intermedia entre las metodologías científicas inductivas y deductivas, centrada en los sistemas complejos y bajo metodologías científicas mixtas de computación.

Las ciencias de la complejidad requieren de la aplicación de las ciencias de la computación en la comprensión de los sistemas complejos y, en el objetivo de este estudio, en los problemas complejos sociales. Las ciencias de la computación materializan su aportación en aplicaciones, herramientas y proyectos analíticos de estudio, de simulación, de representación gráfica, etc. Especial interés, el uso de la ciencia de datos e la inteligencia artificial.

El modelado del sistema constituye una de las primeras las actividades a desarrollar en una investigación científica de sistemas complejos. Actividad sensible y subjetiva, que dependerá (entre otras variables) de la pregunta a resolver en el problema planteado.

El modelado lógico proporciona el conocimiento esencial del sistema, sobre qué es o qué hace. Se puede llegar a generar, a un nivel básico, mediante la aplicación de TAE y herramientas básicas de computación (Excel de Microsoft) y representación (PowerPoint de Microsoft).

La imposibilidad de generar un modelo físico (implementación tecnológica y computacional que proporciona una simulación y validación del sistema) no debe restar el interés por comprender el sistema complejo de estudio mediante el modelo lógico u otras metodologías.

Como se mencionó anteriormente, la ciencia de la complejidad se interesa por los fenómenos y comportamientos de sistemas dinámicos no lineales de complejidad creciente; provocando una transformación en el desarrollo de la investigación científica (Maldonado, 2008: 159-160 y 163)[6], «[...] con el tránsito de la descripción a la explicación, y del modelamiento a la simulación [...]» (Maldonado, 2008: 160).

---

[6] Como ejemplos de fenómenos de complejidad creciente se encuentran geometría fractal (B. Mandelbrot), el caos y, en general, el trabajo con y el desarrollo de sistemas en perspectiva evolutiva. En este sentido, la matemática de la complejidad responde a la ecuación: «Matemáticas + Tiempo = Complejidad», que tienen que ver con iteración, evolución, aprendizaje, generalmente a través de procedimientos computacionales.
Como ejemplo la aplicación de la inteligencia artificial a fenómenos y comportamientos no lineales, gracias a una matemática con una lógica computacional basada en algoritmos genéticos en sistemas evolutivos.
Las matemáticas de la complejidad son matemáticas cualitativas. Se caracterizan por el estudio de problemas con:

— Amplio número de grados de libertad (a mayor grado de libertad, mayor complejidad).
— Sistemas abiertos, incompletos, inacabados y en evolución.
— Sistemas dinámicos, caracterizados por:

> «[...] no-linealidad, sinergias, bucles de retroalimentación positiva y negativa, transiciones de fase, bifurcaciones, autorganización y emergencias, en los que lo importante no son los elementos que componen un sistema determinado, sino las relaciones entre los componentes del sistema de que se trate, así como el hecho, fundamental, de que se trata de un sistema abierto, o sensible al entorno o medio ambiente».

El avance en el conocimiento de la complejidad se debe, entre otros factores, por el desarrollo de las ciencias de la computación (Maldonado, 2008: 159)[7], a través de la ciencia de datos e inteligencia artificial (IA), entre otras.

Las matemáticas de la complejidad son matemáticas centradas en el estudio de los sistemas termodinámicos (no linealidad, emergencia, autoorganización e irreversibilidad), no simplemente dinámicos, focalizado en el estudio de lo variable. Se materializa (Maldonado, 2008: 163-164)[8] en aplicaciones, herramientas y proyectos de las ciencias de la computación, ya sea en los métodos analíticos de estudio y de simulación; o bien, en la representación gráfica mediante simulaciones, grafos...

En el ámbito de los fundamentos y procedimientos (epistemología formal) de la investigación científica de los sistemas complejos se dan cuatro agrupaciones de actividades (figura n.º 2), que se suceden de forma secuencial (Galán, 2014: 3):

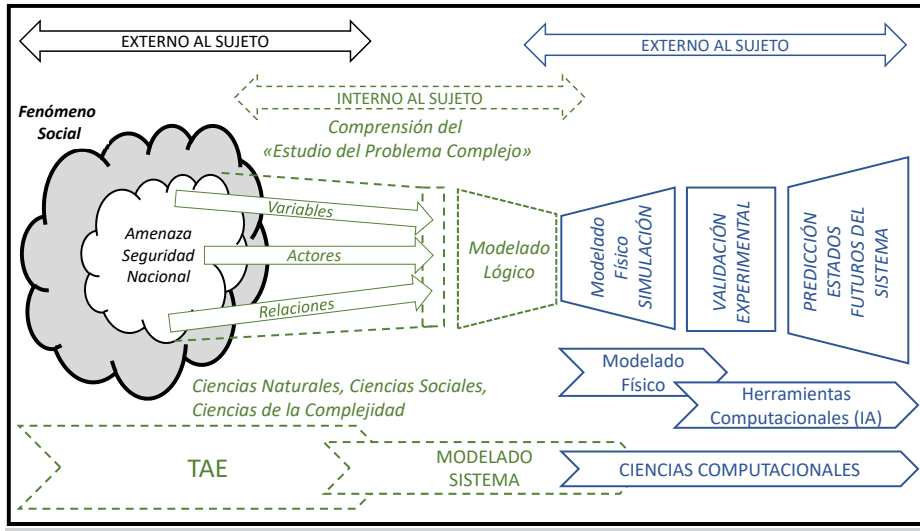

Figura 2. Investigación científica de los sistemas complejos y técnicas de análisis. Fuente: elaboración propia

[7] «[...] Las ciencias de la complejidad son al mismo tiempo posibles gracias al desarrollo de la computación y contribuyen, a su vez, para el desarrollo de lenguajes de programación, de cara a la heurística y metaheurística de los sistemas complejos no-lineales».

[8] Entre los métodos analíticos, cabe destacar las redes booleanas, mapas iterativos (lineales, no lineales y cuadráticos), la constante de Lotka-Volterra (estudio de sistema de la ecología), fractales, toros y actractores, actractores extraños, etc. La teoría de grafos como ciencia de conexiones, avanzando del enfoque matricial.

- Modelado del sistema, parte más sensible del estudio de sistemas. Constituye un método analítico de estudio del problema. «[...] Por un lado es necesario seleccionar los aspectos de la realidad más relevantes para estudiar el sistema, y por otro representarlos (modelarlos) de la forma más fiel posible a la realidad» (Galán, 2014: 239). Proceso subjetivo, que dependerá de qué se desea modelar y del enfoque de cómo se desea hacerlo.
- Simulación del sistema, a partir de las dinámicas de modelado, que permiten «[...] comprender su funcionamiento mediante, por ejemplo, la extracción de patrones o reglas de comportamiento. Estos patrones suelen ser reglas de comportamiento locales que permitirán simular el sistema a nivel global [...]» (Galán, 2014: 240).
- Validación experimental del comportamiento simulado con el comportamiento real del sistema (Galán, 2014: 240).
- Realización de predicciones sobre estados futuros del sistema (Galán, 2014: 240).

La ciencia de la complejidad requiere de la simplificación de los sistemas complejos, con la finalidad de centrar el estudio en aspectos concretos del sistema de forma aislada (Galán, 2014: 60). Un modelo o modelado es una representación conceptual (normalmente una simplificación) de algún fenómeno complejo de la realidad. La finalidad del modelado es estructurar y aislar aspectos relevantes, eliminar los irrelevantes y comprender el sistema objeto de estudio; así como documentar diseños técnicos. Se distinguen principalmente entre los modelos lógicos y físicos (Whitten *et al.*, 2008: 258; Galán, 2014: 61 y 239).

- Los modelos lógicos (o conceptual o de negocios o real) muestran qué es un sistema o qué hace; es decir, su esencia. Independientemente de su implementación técnica posterior, diseñan el sistema. Frecuentemente se designa como un diagrama de entidad relación (entity relationship diagram, ERD) basados en entidades y las relaciones descritas por las entidades (Whitten et al., 2008: 213). Se puede llegar a generar, en un nivel básico, mediante la aplicación de TAE y herramientas básicas de cálculo (Excel de Microsoft) y representación (PowerPoint de Microsoft). Destacar como ejemplo el modelo lógico del modelo lógico del fenómeno de la inmigración ilegal en el sur de España de la figura n.º 3 (Corrochano, 2023).
- Los modelos físicos (o de implementación o técnico) implementa el sistema física y técnicamente a partir del modelo lógico (figura n.º 4). Dependientes del desarrollo de la tecnología y sus limitaciones.

Existen diversas razones por las que las actividades de análisis de sistemas complejos se enfocan en modelos lógicos, entre las que se exponen:

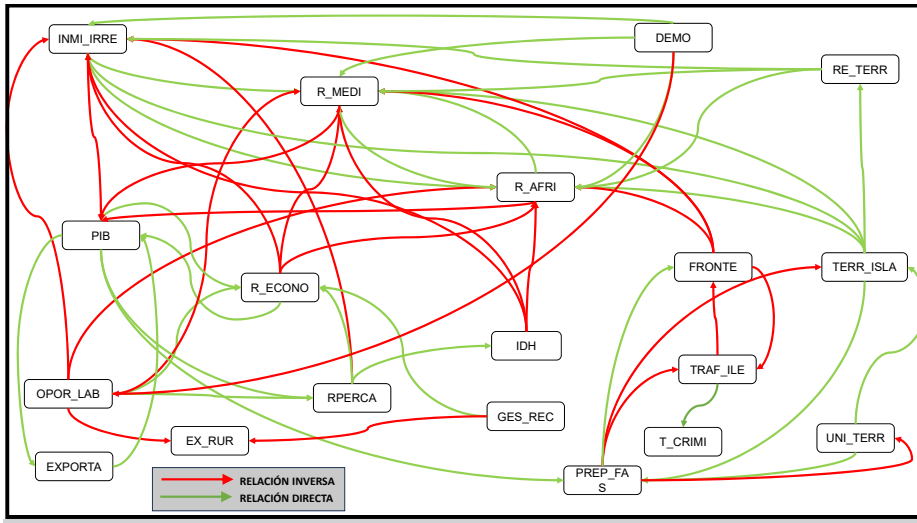

Figura 3. Modelo lógico del fenómeno de la inmigración ilegal en el sur de España (Corrochano, 2023)

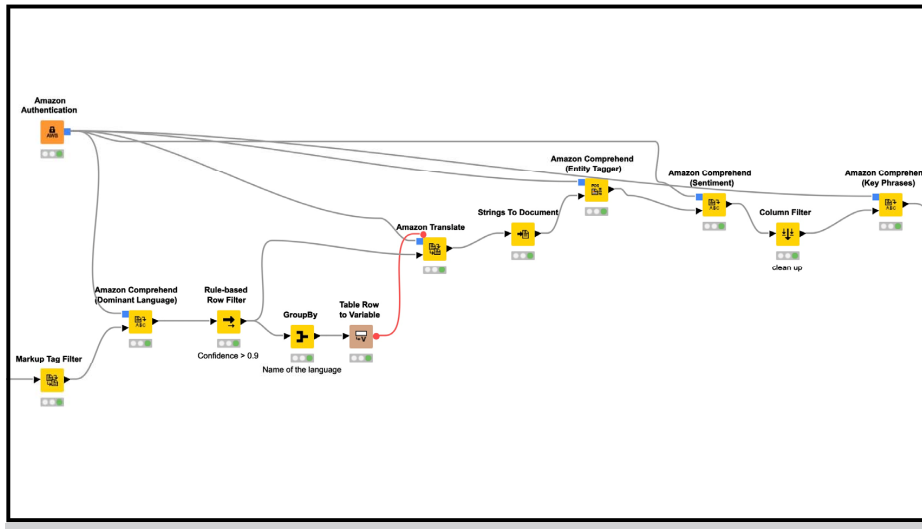

Figura 4. Modelo físico de estudio de gestión de riesgos en base a analítica de textos y fuentes de información en tiempo real. Fuente: elaboración Consultoría Analyticae

— Reducen los sesgos cognitivos al implementar el sistema, tanto del propio analista como de cualquier otro, puesto que motivan la creatividad (Whitten et al., 2008: 250).
— Reducen el riesgo de omitir los elementos o requisitos fundamentales del sistema por estar centrados en los detalles técnicos de desarrollo posterior (Whitten et al., 2008: 64). Generación

independiente de la representación de lo qué debe el sistema hacer y cómo lo hará.
- Permiten la comunicación sencilla y comprensible de los desarrolladores técnicos con los usuarios finales. Empleo de lenguaje menos técnico (Bertalanffy, 1976: 210; Echeverría, 1999: 44).
- Permite deducciones a partir de premisas; su posterior explicación y predicción. A veces, con resultados inesperados (Bertalanffy, 1976: 211).
- Excesiva simplificación, tanto mayor cuanto más complejo es el sistema. «Para hacerla conceptualmente controlable tenemos que reducir la realidad a un esqueleto conceptual, dejando en pie la pregunta de si al proceder así no habremos amputado partes vitales de la anatomía [...]» (Bertalanffy, 1976: 211).

Una aplicación de los modelos de sistemas complejos en los problemas sociales se puede visualizar en la Dinámica de Sistemas aunque, como modelos físicos, requieren ser simulados computacionalmente (Castilla, 2019: 12).

Los modelos físicos de sistemas complejos sociales son modelos que simplifican la realidad, aunque con limitaciones, puesto que **«**[...] será tanto mejor cuanto más acertada sea la elección de las variables que influyen sobre las variables en estudio y cuanto más fiel sea la función matemática o tabla de valores que representa dicha influencia [...]» (Castilla, 2019: 12). Sin embargo, la complejidad de los sistemas sociales y su dificultad de modelado recae en la riqueza y heterogeneidad del comportamiento social y humano. En el mismo sentido, las conclusiones del modelo serán menos probables cuanto mayor sea la proyección de su futuro (Castilla, 2019: 14).

En opinión de Castilla Varea (2019: 14), al constituirse los modelos de Dinámica de Sistemas como modelos de sistemas sociales físicos, no deberían mezclarse variables, actores y relaciones funcionales.

En la discusión de la aplicación de modelos lógicos o modelos físicos a los problemas complejos sociales deberá contemplarse las limitaciones con las que se cuenta a la hora de llevar a cabo estudio. Especial relevancia cobran los datos disponibles (información cualitativa de expertos o información cuantitativa de fuentes de datos); desarrollo tecnológico y computación como herramientas de análisis (TAE o inteligencia artificial); tiempo de ejecución (elaboración del asesoramiento o del tratamiento de los datos); etc.

De cualquier forma, se debe tener en cuenta que los problemas complejos sociales desde la perspectiva de la ciencia de complejidad constituyen un sistema de (sub) problemas que posibilitan su estudio multidisciplinar (ciencias naturales, sociales, de la complejidad y computacional) y la

aplicación de una amplia variedad de técnicas de análisis de datos (cualitativos (TAE) y cuantitativos (modelado y computación)).

5.2 *Integración de la inteligencia artificial en el estudio problemas sociales complejos*

El desarrollo de modelo físicos de problemas complejos (simulación y validación del sistema complejo) pasa por la integración de herramientas de las ciencias de la computación (en este caso, inteligencia artificial) en modelos lógicos.

En 2023 en la Escuela Superior de Fuerzas Armadas se celebraron unas jornadas de formación docente con el título "Construcción de modelos interpretativo-predictivos del entorno en Inteligencia. Las ontologías y la inteligencia artificial como catalizadores del trabajo interdisciplinar", cuyos talleres colaborativos contribuyeron a identificar propuestas de mejora en la integración de herramientas de computación de IA en proyectos de comprensión de problemas complejos. Entre las propuestas más significativas: la creación de equipos multidisciplinares en todas las fases del desarrollo del proyecto del IA, potenciación del rol de «analista técnico» perteneciente a la organización y formación cruzada multidisciplinar de alto nivel en la organización (área de inteligencia y área computacional).

La comprensión de los problemas complejos sociales mediante modelos lógicos constituye una actividad imprescindible para la implementación de modelos físicos con herramientas de ciencias de la computación; en este caso, inteligencia artificial (IA). Esta comprensión requiere un pensamiento sistémico que englobe los (sub) problemas complejos, complicados y simples que conforman el todo (problema social complejo).

Dependiendo de la tipología del problema y de su metodología de estudio (deductiva, inductiva y mixta) se identificará las técnicas analíticas a emplear. En el caso de la IA serán metodologías mixtas con técnicas analíticas cuantitativas, mediante matemáticas computacionales que integren aplicaciones, herramientas y proyectos de IA.

La Estrategia de Seguridad Nacional (ESN, 2021) potencia el empleo de aplicaciones, herramientas y proyectos de las ciencias de la computación a los problemas complejos sociales que les afecta. En varias líneas acción hace referencia, bajo sus diferentes enfoques[9], a: vectores de ventaja estra-

[9] La Estrategia de Seguridad Nacional (ESN, 2021) promulga, en su primer eje, la protección de la vida de las personas y sus derechos y libertades, así como el orden constitucional. En su línea de acción de Disuasión y Defensa se plantea «[...] reforzar las de defensa a través de la investigación, el desarrollo y la innovación tecnológica como vectores de ventaja estratégica».

tégica (investigación, desarrollo e innovación tecnológica); potenciación de la gestión y tratamiento del dato (IA, computación cuántica o la nube); instrumentos que mejoren la inteligencia y la detección; nuevas capacidades de ciberseguridad.

En la búsqueda de la potenciación de la gestión y tratamiento del dato de los problemas sociales complejos en el ámbito docente de la Inteligencia Militar se identificó la necesidad de establecer conexiones entre el mundo de la inteligencia y el mundo computacional. Con el tema de la «Construcción de modelos interpretativo-predictivos del entorno en Inteligencia. Las ontologías y la inteligencia artificial como catalizadores del trabajo interdisciplinar» se llevaron a cabo unas jornadas de formación en la Escuela Superior de las Fuerzas Armadas (ESFAS) durante los días 22, 23, 26 y 30 de junio de 2023.

Estas jornadas tuvieron la finalidad, entre otras, crear un marco ontológico e interdisciplinar de comunicación entre el científico computacional y el oficial de inteligencia e identificar nuevos perfiles de competencias profesionales. La ejecución de la jornada se dividió en módulos con una impartición mixta de conferencias y sesiones de trabajo en grupo con integrantes del marco nacional de Inteligencia, Fuerzas y Cuerpos de Seguridad del Estado y Departamento de Seguridad Nacional. Por parte de la consultora de analítica de datos ANALYTICAE S. L. y el profesorado del Departamento de Inteligencia (DINT) de la ESFAS se impartieron conferencias que, posteriormente, dieron paso a trabajos en grupo colaborativos entre asistentes y consultoría.

Con el módulo 2 sobre «Desarrollo de proyectos de inteligencia artificial en las organizaciones» se profundizó sobre la tipología de implantación de proyectos de inteligencia artificial en las organizaciones de Inteligencia. Los tipos de implantación de proyectos de IA en las UCO se diferencian según la capacidad de generación de las UCO de sus propias herramientas de IA (generación propia) o su externalización a empresas de desarrollo (externalización), no descartándose híbridos que combinan ambas tipologías.

Cualquiera de las tipologías expuestas (generación propia o externalización) requiere cumplir unas expectativas mínimas para el analista

---

En la línea de acción de Contrainteligencia, lucha contra las campañas de desinformación y acción frente a las injerencias del exterior se potencia «[...] sus capacidades humanas y tecnológicas, de manera que se sigan aprovechando las ventajas vinculadas a una adecuada gestión y tratamiento del dato, como la Inteligencia Artificial la computación cuántica o la nube [...]».

En la línea de acción Lucha contra el crimen organizado y la delincuencia grave se requieren «[...] instrumentos que mejoren la inteligencia y la detección, además de nuevas capacidades de ciberseguridad [...]».

(cliente, usuario, etc.), que conlleve un desarrollo continuo y escalable de la herramienta de IA y cuya necesidad profesional sea adaptada a los requerimientos de la organización. Otras características comunes de la implantación de proyectos (generación propia o externalización) se encuentran:

- Necesidad de explicar y difundir en todos los niveles de la organización de inteligencia los fundamentos, necesidades de uso, ventajas y limitaciones de las ciencias de la computación (ciencia de datos e inteligencia artificial).
- Visualización de las necesidades de uso de las herramientas de IA, así como su resolución, mediante desarrollos simples y caso de uso.
- Creación de equipos multidisciplinares en todas las fases del desarrollo del proyecto de IA.
- Identificación en la organización de Inteligencia del rol del business translator o analista técnico.

En los proyectos de IA se identifican en la UCO de inteligencia y de la empresa desarrolladora de herramientas de IA unos diferentes roles y procesos relevantes que aunan a ambas organizaciones en la consecución del proyecto. Destacan entre otros:

- Experto de producto IA. Personal ajeno a la organización de inteligencia, que puede pertenecer a empresa desarrolladora o agente comercial de productos IA. Facilita la labor del personal interno (analista) y es conocedor de los productos de inteligencia artificial del mercado.
- Analista Técnico. Traductor. Business translator. Personal de la UCO de inteligencia, o ajeno. En el caso ajeno, puede pertenecer a la empresa desarrolladora.
  Trabajo conjunto y colaborativo con el analista de inteligencia para proporcionar el apoyo técnico a sus cometidos y fines con las herramientas de IA. Define la información necesaria para responder a la necesidad de uso requerida por el oficial de Inteligencia (el problema). Analiza el dato y valora la calidad y cantidad necesaria para que el modelo de IA funcione.
- Oficial de inteligencia. Analista de inteligencia. Personal perteneciente a la organización de inteligencia.
- Define los casos de uso y las necesidades de la organización de inteligencia. Capaz de definir el modelado de la realidad, para la construcción de la ontología en el sistema. Evalúa y emite informe basado en los resultados aportados por el modelo de inteligencia artificial que previamente ha sido entrenado.

Otras propuestas de mejora de la integración de proyectos de IA en la resolución de problemas complejos, además de la existencia del rol de

analista técnico o analista traductor en las organizaciones de inteligencia, son las siguientes:

— Realización de talleres con otras organizaciones de IA que estén tratando de resolver problemas similares.
— Formación cruzada multidisciplinar (área inteligencia y área computacional) a científicos de datos y analistas, entendiendo como tal: formación técnica y tecnológica; formación sobre análisis de inteligencia, metodología y procedimientos.

Entre las buenas prácticas identificadas ante un proyecto de IA para la consecución de una aplicación de IA que alcance las expectativas de las UCO destacan:

— Aportación de la información necesaria a la empresa desarrolladora para el proyecto de la herramienta de IA. Esto incluye la metodología de trabajo, los casos de uso, el modelado del problema complejo, la información y fuentes disponibles.
— Implementación de una herramienta piloto de IA, principalmente con un caso real, con la finalidad de poner en valor la utilidad real de la herramienta, y convencer a escépticos.
— Fomento de la multidisciplinariedad de los equipos de proyecto, con la combinación de recursos humanos de diferentes perfiles. El clima de trabajo del equipo debe ser distendido, con libertad para aportar ideas y cometer errores.
— Instauración de un grupo permanente de apoyo al usuario en la organización, que debe estar formado por especialistas en la herramienta y oficiales de inteligencia. Generalmente provienen del equipo de proyecto que puso en marcha el sistema, por lo menos en su primera fase.

6 Discusión y conclusión

Las amenazas a la Seguridad Nacional constituyen una prioridad para el Estado español, que queda reflejado en el desarrollo normativo, en la implicación de Administraciones Públicas y otros sectores de la sociedad (personas físicas y jurídicas) y en la potenciación de los recursos para la prevención, la detección y su neutralización. Las Fuerzas Armadas y los servicios de inteligencia e información del Estado apoyaran al Sistema de Seguridad Nacional en la comprensión, detección y valoración de las amenazas, entre otros cometidos. La aplicación de las ciencias de la computación a los cometidos antes descritos conforman diferentes líneas de acción de la ESN.

Estas amenazas comparten las principales características de los sistemas complejos que se estudian en las ciencias sociales (sistemas complejos

sociales), entre otras, el dinamismo de sistema, su complejidad y la emergencia. La comprensión de las amenazas como sistemas complejos sociales requieren de una perspectiva metodológica de investigaciones científicas adaptadas al caso, en las que se planteen, entre otros aspectos, la delimitación de un *estudio del problema* y establecimiento de cuestiones a responder. El estudio del problema complejo social conformará la metodología de estudio de los sistemas complejos sociales.

Por parte de las UCO de inteligencia se precisa la comprensión de las amenazas y los actores que intervienen en su materialización (directa o indirecta). Esta comprensión implica un estudio del problema complejo de la situación actual, de las tendencias de cambio de los escenarios futuros y de sus fenómenos emergentes. La transición del estudio del problema complejo de la amenaza actual a los escenarios futuros de las nuevas amenazas precisa analizar las relaciones y los elementos del sistema que experimentarán un cambio de tendencia o permanecen inalterables; los que evolucionarán de forma drástica y aquellos que emergen, creando nuevo fenómeno.

La elección de las metodologías de investigación (multidisciplinar) y las técnicas de análisis de apoyo a la decisión dependerán del problema complejo objeto de estudio, del tiempo y datos disponibles.

Las ciencias de la complejidad constituyen la perspectiva intermedia entre las metodologías científicas inductivas y deductivas de estudio de problemas complejos. Se centra en los sistemas complejos y en metodologías científicas mixtas de las ciencias de la computación. Materializan su aportación en aplicaciones, herramientas y proyectos analíticos de estudio, de simulación, de representación gráfica, etc. Especial interés, el uso de la ciencia de datos e la inteligencia artificial.

En el ámbito del pensamiento sistémico de las ciencias de la complejidad, cada problema complejo se compone de un sistema de (sub) problemas (complejos, complicados y simples) y así, sucesivamente. La comprensión de los problemas complejos sociales requiere el desarrollo de capacidades cognitivas de razonamiento de analista; la investigación científica desde diferentes disciplinas de conocimiento científico (ciencias naturales, sociales y computacionales) y técnicas de análisis de apoyo a la decisión (cualitativas (TAE) y cuantitativas (modelado de sistemas e IA)).

La aplicación de las técnicas analíticas estructuradas en la comprensión de problemas complejos permite la elaboración de inteligencia para el asesoramiento en la toma de decisiones. Proporcionan al analista (o equipo de analistas) un pensamiento crítico, independiente y alternativo en problemas con un limitado tiempo de ejecución y dificultades de obtención de datos.

El modelado del sistema constituye una de las primeras las actividades a desarrollar en una investigación científica de sistemas complejos. Actividad sensible y subjetiva, que dependerá, entre otras variables, de la pregunta a resolver en el problema planteado.

El modelado lógico proporciona el conocimiento esencial del sistema, sobre qué es o qué hace. Se puede llegar a generar mediante la aplicación de TAE y herramientas básicas de cálculo (Excel de Microsoft) y representación (PowerPoint de Microsoft).

El desarrollo de modelo físicos de problemas complejos (simulación y validación del sistema complejo) pasa por la integración de herramientas de las ciencias de la computación (en este caso, inteligencia artificial) en modelos lógicos. Con este fin se necesita en las UCO de Inteligencia la creación de equipos multidisciplinares en todas las fases del desarrollo del proyecto del IA, potenciación del rol de *analista técnico* perteneciente a la organización y formación cruzada multidisciplinar (área de inteligencia y área computacional).

Como conclusión y respuesta a la pregunta inicial planteada, las organizaciones de inteligencia deben de potenciar la comprensión de las amenazas a la Seguridad Nacional desde la perspectiva de investigación científica mixta que proporciona las ciencias de la complejidad, entendiendo las amenazas como sistemas complejos sociales. La inclusión de las TAE y contenidos de ciencias de la computación (modelado y inteligencia artificial) en sus currículo de formación y especialización son la base de la mejora de la competencias colaborativas en la creación de equipos multidisciplinares que guíen los proyectos de implementación de modelos físicos con ciencia de datos e inteligencia artificial.

La comprensión por parte de las UCO de inteligencia de las amenazas a la Seguridad Nacional como sistemas complejos sociales exige un cambio de paradigma en la elaboración de inteligencia: del ámbito cualitativo del juicio de experto, al ámbito mixto (computacional) de un grupo de expertos multidisciplinar.

Concebir las amenazas como sistemas complejos sociales, así como abarcar su estudio como problemas complejos sociales, implica aceptar su dinamismo, complejidad y emergencia. ¿Realmente se comprenden las amenazas en su dinamismo, complejidad y emergencia? ¿Se disponen de herramientas computacionales que puedan acercarnos a su conocimiento y comprensión? Ante la negativa de las respuestas, la elaboración de inteligencia será subjetiva, irreproducible por otros analistas e incompleta al carecer de la amplitud de su multidisciplinariedad.

Entre una propuesta eminentemente cualitativa dependiente del juicio de experto y la futurista de herramientas computacionales autónomas de inteligencia artificial se encuentra el modelado lógico de amenazas (problemas

complejos sociales). El modelado lógico de problemas complejos sociales generado a partir de grupo multidisciplinar de expertos mediante la aplicación de técnicas analíticas estructuradas constituye el nivel más básico de comprensión. La integración de herramientas de IA en la consecución de un modelado físicos de problemas complejos constituye un camino a recorrer por las UCO. Algunos de los esfuerzos que se necesitan implantar han quedado reflejados en apartados anteriores.

«Parar, para darse cuenta dónde se encuentra; saber dónde se quiere ir, para marcar el rumbo; decidir ponerse en marcha, para alcanzar el objetivo. Estas pautas constituyen una lección de vida para el militar, para cualquier persona... También para las organizaciones».

Bibliografía

Agüero, J. (2010). Niklas Luhmann y los sistemas autopoiéticos. En: *VI Jornadas de Sociología de la UNLP*. La Plata, Universidad Nacional de La Plata, Facultad de Humanidades y Ciencias de la Educación, Departamento de Sociología. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.aacademica.org/000-027/38.pdf

Arnold, M. y Osorio, F. (1998). Introducción a los Conceptos Básicos de la Teoría General de Sistemas. *Cinta de Moebio*. Santiago de Chile, Universidad de Chile, Facultad de Ciencias Sociales, (3), pp. 40-49. [Consulta: 10 de febrero de 2024]. Disponible en: https://www.moebio.uchile.cl/03/frprinci.html

Bertalanffy, L. V. (1976). *Teoría General de los Sistemas*. México, Fondo de Cultura Económica. [Consulta: 10 de enero de 2024]. Disponible en: https://fad.unsa.edu.pe/bancayseguros/wp-content/uploads/sites/4/2019/03/Teoria-General-de-los-Sistemas.pdf

Cadenas, H. (2012). El sistema de la estructura. Estructuralismo y teoría de sistemas sociales. *Cinta de Moebio*. Santiago de Chile, Universidad de Chile, Facultad de Ciencias Sociales, (45), pp. 204-214. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.moebio.uchile.cl/45/cadenas.html

Castilla, A. (2019). Enfoque sistémico y planeamiento operativo: el emperador está desnudo. *Documento Marco 17/2019*. Madrid, Instituto Español de Estudios Estratégicos. Centro Superior de Estudios de la Defensa Nacional. [Consulta: 1 de febrero de 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_marco/2019/DIEEEM17_ 2019ALFCAS_operativa.pdf

Corrochano, A. (2023). *Dinámica de Sistemas aplicadas al fenómeno de la inmigración ilegal en el sur de España* [trabajo de finde

máster]. Director, José María Gil Armario. Aranjuez. Centro Universitario de la Guardia Civil. [Consulta: 10 de febrero de 2024]. Disponible en: https://www.cugc.es/investigacion/publicaciones/busqueda-avanzada/16-tecnologias-aplicadas-a-la-investigacion/1766-dinamica-de-sistemas-aplicada-al-fenomeno-de-la-inmigracion-ilegal-en-el-sur-de-espana.html%0A

Cruz Villalón, J. (2016). La metodología de la investigación en el derecho del trabajo. Sevilla, Universidad de Sevilla. *Temas Laborales*. 132, pp. 73-121. [Consulta: 10 de febrero de 2024]. Disponible en: https://idus.us.es/handle/11441/96142

España. (2015). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. *Boletín Oficial del Estado*. 29 de septiembre, n.º 233.

—. (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, n.º 314, pp. 167795-167830.

Echeverría, J. (1999). *Introducción a la Metodología de la Ciencia. La filosofía de la ciencia en el siglo XX*. Madrid, Cátedra. IBSN: 8437617006.

Flórez, A. y Thomas, J. (1993). Teoría General de Sistemas. *Cuadernos de Geografía. Revista Colombiana de Geografía*. IV (1-2), pp. 111-134.

[Consulta: 10 de febrero de 2024]. Disponible en: https://revistas.unal.edu.co/index.php/rcg/article/view/70711/64920

Folker, R. D. (2000). *Intelligence Analysis In Theater Joint Intelligence Centers: An Experiment In Applying Structured Methods*. Washington, D.C., Joint Military Intelligence College. Center for Strategic Intelligence Research. [Consulta: 15 de diciembre de 2023]. Disponible en: https://apps.dtic.mil/sti/citations/ADA476722

Galán, J. (2014). *Aplicaciones de la racionalidad acotada al razonamiento cualitativo sobre sistemas* complejos [tesis]. Director, Juan Borrego Díaz. Sevilla, Universidad de Sevilla, Departamento de Ciencias de la Computación e Inteligencia Artificial. [Consulta: 10 de diciembre de 2023]. Disponible en: https://idus.us.es/handle/11441/23901

Goldstein, J. (1999). Emergence as a construct: history and issues. *Emergence: Complexity & Organization*. 1(1), pp. 49-72. [Consulta: 2024]. Disponible en: https://journal.emergentpublications.com/Article/49564b2c-44f6-4763-89bc-5166c818341f/jats

Heuer, R. J. y Pherson, R. H. (2015). *Técnicas Analíticas Estructuradas para el análisis de inteligencia*. Madrid, Plaza y Valdés. IBSN: 84-15271-67-3.

Luhmann, N. (1998). *Sistemas sociales: lineamientos para una teoría general*. Barcelona, Anthropos. ISBN: 84-7658-493-8.

Ministerio de Defensa. (2018). Publicación Doctrinal Conjunta n.º 1. Doctrina de Inteligencia para las Fuerzas Armadas. IBSN: 84-9091-318-5.

—. (2020). Publicación Doctrinal Conjunta n.º 2. Doctrina de Inteligencia para las Fuerzas Armadas.

OTAN. (2024a). *ALTA Handbook. Organización del Tratado del Atlántico Norte* [en línea]. [Consulta: 15 de febrero de 2024]. Disponible en: https://www.act.nato.int/wp-content/uploads/2023/05/alta-handbook.pdf

—. (2024b). Organización del Tratado del Atlántico Norte [en línea]. [Consulta: 15 de febrero de 2024]. Disponible en: https://www.act.nato.int/activities/alternative-analysis/

Somiedo, J. P. (2018). El análisis bayesiano como piedra angular de la inteligencia de alertas estratégicas. *Revista de Estudios en Seguridad Internacional*. 4(1), pp. 161-176. [Consulta: 1 de febrero de 2024]. Disponible en: https://seguridadinternacional.es/resi/html/el-analisis-bayesiano-como-piedra-angular-de-la-inteligencia-de-alertas-estrategicas/

Vivanco, M. (2014). Emergencia: Concepto y método. *Cinta de Moebio*. Santiago de Chile, Universidad de Chile, Facultad de Ciencias Sociales, (49), pp. 31-38. [Consulta: 10 de diciembre de 2023]. Disponible en: https://www.moebio.uchile.cl/49/vivanco.html

Whitten, J. L. *et al*. (2008). *Análisis de sistemas: diseño y métodos*. 7.ª edición. McGraw-Hill/Interamericana. IBSN: 978-970-10-6614-0. [Consulta: 10 de octubre de 2023]. Disponible en: http://opac.unellez.edu.ve/doc_num.php?explnum_id=1815

La seguridad interior en un mundo cambiante

Antonio Alberto González

Resumen

La garantía de la seguridad se ha percibido como una necesidad humana desde los orígenes de la sociedad. Con el nacimiento del Estado Moderno, el tradicional concepto de seguridad ha evolucionado hacia un ámbito de aplicación más amplio que el simple ejercicio nacional del poder del Estado en la aplicación del Derecho interno. Este marco restringido se había limitado a proteger activos reconocidos y garantizados en las leyes en un contexto acotado, y que resultaron eficaces para afrontar una amenaza particular. Sin embargo, esta restricción espacial no es óbice para que se configuren, sin ser incompatibles, círculos concéntricos de seguridad por encima de las capacidades competenciales y contextos espaciales propios de un Estado y que atienden más al valor del activo, y al riesgo de amenaza, que al límite de las fronteras.

En este sentido, un concepto más amplio de la seguridad legitima a las autoridades nacionales a atribuirse una competencia acorde con un concepto más universal de la seguridad, por su importancia estratégica y afectación a la soberanía nacional, dotándose de recursos humanos, medidas objetivas y órganos de colaboración en entes supranacionales, que sean acordes a las necesidades y riesgos transversales que se derivan de una amenaza, en constante mutación, y adaptándola a las actuales necesidades de seguridad de una sociedad globalizada.

Palabras clave

Necesidad, Activos, Amenaza, Riesgo, Frontera.

Internal security in a changing world

Abstract

The security guarantee has been perceived as a human need since the origins of society. With the birth of the Modern State, the traditional concept of security has evolved into a wider field of application than the simple national exercise of the power of the State in the application of internal law. This restricted framework was limited to protecting assets recognized and guaranteed by law in a limited context, and which were effective in facing a particular threat. However, this spatial restriction is not an obstacle to the configuration, without being incompatible, of

concentric circles of security over the competitive capacities and spatial contexts of a State and which attend more to the value of the asset, and to the risk of threat, that at the limits of our borders.

In this sense, a broader concept of security legitimizes national authorities to grant themselves a competence in accordance with a more universal concept of security, due to its strategic importance and its impact on national sovereignty, providing themselves with human resources, objective measures and collaboration bodies in supranational entities, in accordance with the needs and cross-cutting risks arising from a constantly changing threat, and adapting it to the current security needs of a globalized society.

Keywords

Need, Assets, Threat, Risk, Frontier.

1. Introducción

La seguridad es un concepto poliédrico y plagado de aristas, que afecta a bienes jurídicos insertos en la esfera más próxima al ciudadano y se bifurca en dos aspectos: uno subjetivo, como es la propia seguridad, la tranquilidad y, en último término, la paz de las personas, en definitiva una sensación, y otro objetivo que vincula al Estado, como proveedor público y finalista de seguridad, y que debe monitorizar así como calibrar en abstracto esta variable, concretizándola posteriormente.

Más allá de ello, la seguridad, indefectiblemente unida a la amenaza y a los activos que debe proteger, si se adjetiva como interior, alude al ámbito espacial donde confluyen y se asientan estos tres elementos, que no es otro que el territorio soberano del Estado.

2 El origen fue la libertad

No genera duda ni debate la manida expresión que aduce que la libertad sin seguridad no tiene razón de ser. Son dos bienes jurídicos protegidos de primer orden, reconocidos como tales, tanto en la normativa española como en la internacional, gozando de una protección jurídica reforzada: acceso privilegiado a jueces y tribunales especiales, persecución pública de los delitos y procedimiento ágil, preferente y sumario.

Yendo al origen: si el ser humano primigenio gozó en los primeros momentos de su vida de una cota inusitada de libertad, entendida esta como una ausencia de cualquier coerción externa, tanto de sus semejantes como de un ente paraestatal en ciernes (libertad en sentido negativo) o una ampliación máxima de sus capacidades físicas y mentales (libertad en sentido positivo), fue poco después cuando se dio cuenta que la primera sin la segunda no tenía sentido. Así, los seres humanos como agregados de individuos en aras a su progreso cooperativo, como salvaguarda frente a las inclemencias de la naturaleza, conformaron un ente diferente y abstracto, que trascendía a ellos, llamado sociedad, que, con el devenir histórico del liberalismo tardío, dio lugar a la creación de un Estado, que pasó de ser liberal a mutar en social, caracterizado por un, cada vez mayor, fuerte intervencionismo en ramas incluso en principio vedadas a aquél, como la economía. En este contexto de crecimiento del Estado, el concepto de seguridad va cobrando un papel de idea-fuerza, ya que una de las funciones principales de aquel, sino la central, es dotar de protección a los individuos que cobija bajo su seno.

La seguridad es ante todo una sensación subjetiva y elástica que debidamente parametrizada se puede objetivar. Resulta obvio que no todos los ciudadanos tienen un mismo concepto de ella —si así lo fuera, convendría en un absurdo humano o sería propio de dictaduras—, ya que la seguridad

variará según las personas y las circunstancias en las que opere. Por otra parte, determinadas profesiones y actividades se encuentran más vinculadas a esa noción, por lo que esa sensación será diferentemente percibida entre unas y otras. En todo caso, el Estado, compelido a la protección de sus ciudadanos, deberá aunar los mayores esfuerzos por conformar un espacio-tiempo confiable, por lo que el concepto abstracto de seguridad que maneje deberá contar con un sinfín de datos, traducidos en información y esta transformada en inteligencia, que en forma de metanálisis final debería repercutir en una mayor seguridad, lo más cercana posible al 100 %: para todos los individuos y en todas las situaciones imaginables.

3 Las variables de la seguridad

En todo caso resulta indiscutible que la seguridad es una función que depende de tres variables: la amenaza, los medios que se implementen —singularmente por parte del Estado— para afrontarla, y los activos, donde confluyen tanto la amenaza como el Estado. Asimismo, existe una cuarta variable más indefinida —la contextual— que opera presencialmente en la ecuación, y que en los modernos ejercicios de escenarios tiene una importancia capital, donde se mueven tanto la amenaza como los poderes públicos para neutralizarla, reducirla o traspasarla a un tercero (las tres posibilidades para enfrentarla).

En definitiva, el contexto es el marco físico y mental, el aire que se respira en la sociedad donde tiene lugar la amenaza, de tal manera, que no será el mismo entorno en cada uno de los Estados donde esta se materializa, ya que la percepción, la actitud o el clima existente —que incluirá un sinfín de derivadas, la mayoría difícilmente determinables— variará entre unos países y otros, a pesar de las semejanzas culturales, políticas o socioeconómicas, y por muy equivalente que sea la amenaza e incluso las posibilidades para afrontarla.

Durante muchos años, los expertos en inteligencia han tenido problemas para calibrar y monitorizar la variable contextual, hasta que se ha llegado al consenso, no sin polémica, que la misma puede ser debidamente parametrizada a través de técnicas de investigación social como las encuestas y los estudios de opinión. Así, por ejemplo, si en el problema del *procés* las principales variables que orbitan entorno al mismo se pueden agrupar en un tetraedro imperfecto: los activos (el principal, el orden territorial de España, pero también puede serlo un policía o un edificio gubernamental, por ejemplo); la amenaza, conformada por los actores (políticos, radicales, sociales e incluso digitales) que hagan frente a los activos; el Estado o factor institucional, obligado a perseguir la amenaza, y, en último lugar, opera la variable indicada, que sería el ambiente social sobre ese fenómeno, el cual puede ser debidamente referenciado a través de encuestas de opinión

que aborden, de la manera más objetiva posible, la materia. La pregunta central de un sociólogo en este ítem sería: ¿Hasta qué punto el *procés* le preocupa o afecta a su vida?

No obstante, lo anterior, si la seguridad subjetiva es materia reservada en exclusiva a los individuos, como sentimiento que al fin y al cabo es, la seguridad objetiva será responsabilidad del Estado. Este último debe ser quien, configurando la primera, de manera cualitativa, pero sobre todo cuantitativamente, debe calibrar el grado de seguridad existente, numerarlo, explicarlo, y finalmente implementar las medidas —públicas y privadas— para afrontar la amenaza. Como ejemplo de lo anterior, la amenaza descrita en el Plan de Prevención, Protección y Respuesta Antiterrorista, debidamente valorada, se somete al análisis y escrutinio de expertos que, de manera periódica en el tiempo, se reúnen para describirla, contextualizarla y discutirla, para, seguidamente e informado el cliente decisor (la Secretaría de Estado de Seguridad del Ministerio del Interior), cifrarla numéricamente, estipulándose a continuación las medidas a tomar para contrarrestarla y determinar su gradación, llamado nivel de alerta antiterrorista (NAA) que en España, en marzo de 2024, se sitúa en el puesto cuatro sobre cinco, conceptuado como nivel alto.

4 Los activos

Los activos representan el conjunto de elementos del Estado, animados e inanimados, materiales e inmateriales, que son considerados dignos de protección. La seguridad, pues, aparece indefectiblemente unida al activo, ya que el uno sin el otro no tiene razón de ser, de tal manera que la protección de los activos españoles se extiende espacialmente dentro y fuera del territorio español.

En este sentido, las embajadas y consulados, recursos físicos, o los españoles que viajan o residen fuera de España, capital humano, se convierten en activos en el extranjero. Ambas tipologías, por ubicarse fuera de las fronteras, se encuentran bajo el paraguas de la Acción Exterior del Estado, conformada por las actuaciones de los órganos, instituciones y entidades de la Administración Pública llevadas a cabo en el exterior, entre las que se encuentran las desarrolladas por los operadores de seguridad pública de ámbito estatal españoles en colaboración con sus homólogos de los países donde se materialice la amenaza sobre los activos españoles.

5 La seguridad interior

Por el contrario, la seguridad interior se vincula a activos, propios o ajenos, ubicados en el espacio de soberanía del Estado español. Esta seguridad, de la que algunos países de Europa como Alemania, Reino Unido,

Francia, Italia y sobre todo España, pueden impartir cátedras de conocimiento empírico, se proyecta como la seguridad clásica y por excelencia, que se ubica espacialmente en el territorio sobre el cual el Estado mantiene su autoridad.

En España, al igual que en otros países del territorio de la Unión Europea (UE)[1], la seguridad interior es una competencia estatal compartida espacialmente, de tal manera que son varios los organismos que ejercen sus competencias, por razón del territorio y con capacidades y atribuciones desiguales. Así, se entiende que en el nivel más próximo al ciudadano, el local, opera una Policía del mismo tipo, caracterizada por un nivel de recursos provisto, mayoritaria o exclusivamente, por la administración donde actúa. Sus competencias se centran en el mantenimiento del buen orden dentro de la comunidad, que incluye el tráfico y el comercio, fundamentalmente.

En un círculo espacial mayor, el regional, desempeña sus funciones una Policía con características asimétricas por decisión del legislador: así existen comunidades o regiones donde la policía tiene una vocación claramente integral, otras poseen una policía «cedida» por el Estado, con funciones limitadas, mientras que unas terceras ni siquiera cuentan con un cuerpo de seguridad al efecto.

Finalmente, en el círculo espacial superior, que abarca todo el Estado en su conjunto y sin perjuicio de la responsabilidad sobre toda la Seguridad Pública[2], opera una policía sobre asuntos más cercanos al núcleo duro de la seguridad estatal y con mayor impacto social y mediático, terrorismo, crimen organizado, inmigración ilegal, en un modelo similar al del FBI estadounidense: abarcaría los delitos graves, para los cuales la policía del territorio carece de los suficientes recursos, y los conexos a los cometidos en otras comunidades, sean o no limítrofes. En estos casos se aplicaría una policía con actividad transversal en todo el territorio *ratione materiae*.

Por lo tanto, una seguridad interior vinculada de forma directa a activos geolocalizados hace que los organismos encargados de velar por ella se vehiculen funcional y orgánicamente, adaptándose a las características de la amenaza en lo que a recursos humanos y materiales concierne, habiendo tenido lugar en las dos últimas décadas una evolución sustantiva en este terreno, ya que una vez mutada la amenaza terrorista autóctona en otra de orientación yihadista y radical han de variar no solamente los recursos implementados, sino el contenido de planes y programas, tanto operativos como estratégicos, de tal manera que incluso el *knowhow*, que opera en el

[1] Desde 2010, la UE tiene su propia estrategia de seguridad interior.
[2] La Ley 36/2015 de Seguridad Nacional identifica los componentes fundamentales de la Seguridad Nacional: Defensa Nacional, Seguridad Pública y Acción Exterior.

corazón de la organización, también debe mutar al compás del cambio en la amenaza.

En un sentido amplio, la seguridad interior abarcaría todo lo relativo a la seguridad dentro de las fronteras —desde la seguridad ciudadana hasta la lucha antiterrorista, pasando por el control de la inmigración o la lucha contra la delincuencia— y, en sentido restringido, englobaría las vulneraciones, alteraciones y procesos de desestabilización del sistema democrático que tienen por objeto subvertir el orden constitucional y el régimen de derechos y libertades fundamentales, alterando la convivencia.

6 Conclusión

La seguridad interior es una competencia básica del Estado que en la práctica se traduce en el mantenimiento de unos niveles elevados de paz y tranquilidad en las fronteras del mismo, configurándose como un ítem esencial para el desarrollo de las naciones. Vinculada al territorio, protectora de activos y siendo espada y escudo frente a la amenaza, su valor añade un plus de calidad y cantidad al resto de recursos del Estado, como son la economía, el imperio de la ley, la libre circulación o el desarrollo cultural, entre otros.

Las diferentes amenazas poliédricas, híbrida y multidimensionales que se ciernen sobre todos y cada uno de los distintos países de occidente que comparten un acervo cultural e histórico común, aconsejan una revisión constante y periódica de todos los elementos que inciden sobre la citada variable, esto es la seguridad interior, aconsejándose ejercicios de escenarios prospectivos lo más imaginativos posibles, en la medida que las nuevas amenazas provengan por esa vía.

¿Cómo la función inteligencia podría mitigar los riesgos de la introducción de inteligencia artificial en las operaciones militares?

Jose María Lorenzo Tenreiro

Resumen

La inteligencia artificial (IA) ha venido para quedarse y tienen el potencial de tranforma todas las actividades humanas, entre ellas la guerra. En un momento actual, en lo que parece el inicio de una nueva revolución, este artículo analiza los riesgos que se derivan de la implantación o no de la IA a las operaciones militares.

Para ello, se apoya en un escenario ficticio en el que combaten tres países con diferentes aproximaciones a la IA y estudia las vulnerabilidades que la IA lleva aparejadas. Dada la dependencia de los datos que las IA tienen, se identifica que la Función Inteligencia puede jugar un papel fundamental para mitigar los riesgos derivados de ellas e impedir que se materialicen. Inteligencia y Contrainteligencia están llamadas a desempeñar un rol fundamental para introducir a las Fuerzas Armadas a un inminente futuro que, indudablemente, estará permeado por la IA.

Palabras clave

Algoritmos, Datos, TEVV, Vulnerabilidades, Contrainteligencia.

How could the intelligence function mitigate the risks of the introduction of artificial intelligence into military operations?

Abstract

Artificial Intelligence (AI) has come to stay and has the potential to transform all human activities, including war. At a time when we are at what seems to be the beginning of a new revolution, this article analyzes the risks that arise from the introduction or not of AI to military operations.

To do this, this article relies on a fictitious scenario in which three countries with different approaches to AI fight and studies the vulnerabilities that AI entails. Given the dependence of the data that the IA's have, it is identified that the Intelligence Function can play a fundamental role

to mitigate the risks derived from them and prevent them from materializing. Intelligence and Counterintelligence are called upon to play a fundamental role in introducing our Armed Forces to an imminent future that will undoubtedly be permeated by AI.

Keywords

Algorithms, Data, TEVV, Vulnerabilities, Counterintelligence.

1 Ambientación

En el año 2033, en algún lugar del país Azul, el general García, COMFOC[1] de la xoalición, acaba de recibir la conferencia de adopción de la decisión y está meditando.

Hasta el momento, todas las predicciones de Blake, el programa de Inteligencia Artificial (IA) denominado Base Lógico-Algorítmica para Efectos Clave (*Key Effects* en inglés), han sido acertadas. Las plataformas de la coalición son superiores en el enfrentamiento a las fuerzas de Rojo. El programa de guerra cibernética, iniciado en 2025, ha dado frutos. Al haber podido envenenar las fuentes de datos que Rojo ha usado para entrenar a sus IA, las plataformas propias son erróneamente clasificadas como otros tipos de plataformas, lo que hace que las soluciones de tiro que se ofrecen a los operadores de Rojo sean subóptimas y extemporáneas, lo suficientemente malas como para ser inefectivas.

Además, el haber podido realizar ingeniería inversa a los algoritmos[2] de Rojo está permitiendo obtener superiores decisiones. Las acciones que Blake propone, aparentemente inconexas, producen efectos que se acumulan en cascada y ya se han alcanzado varias condiciones decisivas. Todo ello con un ritmo machacón y monótono, sin altibajos, que permite un flujo constante y predecible en las cadenas logísticas y su empleo al máximo de su capacidad.

El desánimo comienza a hacer mella en Rojo. Blake demuestra con sus análisis de OSINT[3] y SOCMINT[4] que la idea de que «da igual lo que hagamos, la Coalición siempre va por delante» o «da igual lo que hagamos, la Coalición siempre tiene un plan B», está calando en las audiencias objetivo.

La única preocupación del general es el flanco oeste, cubierto por las Fuerzas Armadas de Verde que, centradas en las personas y desdeñando la IA, han mostrado dificultades para integrarse en la maniobra conjunta. De hecho, Blake ya ha planeado una rama para cubrir el posible colapso de Verde.

Aun así, García no se decide a firmar la JCO 002[5]. Hasta ahora la campaña está siendo impecable, pero algo dentro de él se resiste a firmar papeles que ni él ni su Estado Mayor entienden completamente, ¿debería fiarse de Blake o hacer caso a esa voz interior y repensar todo?

---

[1] Comandante de la Fuerza Operativa Conjunta.
[2] También denominados modelo, algoritmo y modelo se emplearán indistintamente en este texto.
[3] Inteligencia de Fuentes Abiertas.
[4] Inteligencia de Redes Sociales.
[5] Una *Joint Coordination Order*, o JCO, es la directiva del COMFOC que ordena el cambio de fase en una operación.

Figura 1. Alegoría de la IA asistiendo al planeamiento (fuente: techslang.com)

Este relato corto no es más que una hipotética situación que aspira a hacer al lector pensar sobre el impacto y riesgos asociados a la adopción o no adopción de la IA en las operaciones militares. Los riesgos asociados a la IA se materializan en amenazas tanto para la fuerza como para el conjunto de la nación, lo que justifica todo esfuerzo que se haga en mitigarlos.

La guerra es una empresa eminentemente humana que se caracteriza por ser un choque de voluntades y una prueba de fuerza (Smith, 2005). También se puede entender, desde la óptica de la Trinidad de Clausewitz,: una actividad política dominada por la razón, la pasión y el azar. Por lo tanto, la guerra refleja la sociedad en la que se produce. Y, si en el Neolítico y la Edad Antigua el combate se basaba en la fuerza animal, en la Era Industrial las máquinas tomaron el relevo y complementaron la acción humana. Inmersos en la Era de la Información, la consecuencia lógica es incorporar las herramientas propias de esta Era a la guerra, entre las que destaca la inteligencia artificial. Así, es necesario estudiar los riesgos que entrañan tanto la introducción como la no introducción de la IA en operaciones militares, sin perder de vista el papel que la mente humana juega en la guerra.

La IA tiene un marcado carácter transversal que hace que su aplicación e impacto se puedan asemejar al de la máquina de vapor o al de la electricidad (Ryan, 2022). Más aun, es previsible que una ventaja incluso marginal en el campo de las IA ofrezca beneficios desproporcionados (Scharre 2023, 2021). Por lo tanto, la IA tiene el potencial de afectar profundamente a todas las facetas de la Defensa Nacional. El concepto mismo de disuasión, las actividades de obtención y desarrollo de capacidades, diseño de la fuerza al planeamiento y conducción de operaciones militares desde el nivel estratégico al más bajo nivel táctico, todos estos aspectos se verán afectados por la IA, tanto si se dispone de esta tecnología como si se renuncia a disponer de ella. Además, existe una estrecha relación entre el dominio

cognitivo y la aplicación de la IA; las IA se alimentan de datos e información para su funcionamiento, de lo que se deduce importancia que el dominio cognitivo y la dimensión informativa adquieren.

El Ministerio de Defensa ha publicado su estrategia de adopción de la inteligencia artificial en la que establece una serie de casos iniciales de uso que tienden hacia un uso responsable de la IA, reducido a unos determinados casos de uso y con una fuerte supervisión humana (Ministerio de Defensa, 2023). Esto no es sino reflejo de los valores de España, alineada con el mundo occidental y coherente con los valores de la Unión Europea expresados en la Ley de IA, pendiente de ratificación (European Union, 2024). No obstante, otros países están demostrando tener muchos menos escrúpulos en la aplicación de la inteligencia artificial (Scharre, 2023), lo que apunta a un escenario de posibles desigualdades en el nivel de desarrollo y la profundidad de la aplicación de la IA en el que no es descartable que Occidente se halle en desventaja.

Por ello, resulta interesante analizar dos escenarios, hipotéticos, en los que un país disponga de la superioridad tecnológica que la temprana y extensiva aplicación de la IA brinda frente a otro que, aunque la ha aplicado, la ha aplicado tardía e imperfectamente. Estos dos extremos del espectro permitirán analizar muchos de los posibles riesgos y las maneras en las que se pueden mitigar.

Siendo conscientes de que existen muchas otras acciones posibles para mitigar los riesgos que abarcan desde el propio diseño de la fuerza, a cambios en la Instrucción y Adiestramiento, pasando por medidas enmarcadas en la Enseñanza Militar, este artículo se ceñirá al papel que, en este campo, juega la Función Conjunta Inteligencia.

La inteligencia gravita en torno a la obtención y negación de información sobre el entorno operativo (Estado Mayor de la Defensa, 2020) y, debido a la dependencia que las IA tienen de la dimensión informativa, da un marco doctrinal adecuado para mitigar algunos de los riesgos detectados. Además, enlaza con las actividades de Seguridad de Operaciones y Protección de la Fuerza.

Este artículo realizará un estudio de las vulnerabilidades y riesgos inherentes a la aplicación o a la renuncia de aplicación de la IA a las operaciones militares para, seguidamente, estudiar qué herramientas ofrece la Función Inteligencia para mitigarlos.

2 Las inteligencias artificiales

Actualmente, existe abundante literatura sobre la definición de la inteligencia artificial y cierto consenso en su clasificación. Esto es así porque,

contra lo que pudiera parecer, el concepto de IA lleva tiempo con nosotros al haberse acuñado en los años cincuenta del siglo pasado, dos años después de la muerte del científico inglés Alan Turing, y a consecuencia de los estudios y debates que suscitó el test que propuso.

Dicho test consistiría en situar a un operador humano frente a una máquina y que dialogue con ella para, a continuación, preguntarle si estaba hablando con una máquina o con una persona. El test se consideraría aprobado si el operador no era capaz de determinar si había hablado con una máquina o con una persona. La bondad de las respuestas queda excluida de esta definición y se pone el acento el comportamiento; una IA es un programa informático que se comporta como un humano.

Este test ha influido las definiciones que se han dado a continuación para las IA, lo que se puede apreciar en la definición de IA adoptada por el Ministerio de Defensa, que proviene de la Estrategia Nacional de IA y ha sido redactada por la Comisión Europea (Ministerio de Defensa, 2023) :

> «Sistemas de software, y posiblemente también de hardware, diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento al analizar cómo el medio ambiente se ve afectado por sus acciones previas».

Esta definición contiene los principales elementos que se derivan del test de Turing, ya que no se incide en la bondad del resultado y sí que se pone el énfasis en un proceso que emula al razonamiento humano; de hecho, se puede ver claramente el ciclo de decisión. Según esta definición, la IA observa el entorno, razona (es decir, se orienta y decide) y ejecuta una acción. No obstante, existen diferencias entre una IA y la inteligencia humana cuyo estudio permitirá una mejor apreciación de las vulnerabilidades de las IA y los riegos que estas vulnerabilidades entrañan.

Además, esta definición permite diferenciar entre sistemas automáticos y sistemas autónomos. En este sentido se consideran sistemas automáticos aquellos que se pueden basar en un conjunto de reglas lógicas del tipo «si A..., entonces B...»; son deterministas y predecibles ya que una entrada al sistema siempre producirá la misma salida. Por otra parte, los sistemas autónomos son aquellos que razonan probabilísticamente y, entonces, una entrada no produce siempre la misma salida (Cummings, 2018), solo estos sistemas caben en la definición de IA adoptada por el MDEF.

Para poder razonar, los sistemas de inteligencia artificial construyen un modelo del entorno a partir de los datos que reciben de los sensores y lo actualizan continuamente. La complejidad de este modelo, y, por lo tanto, la cantidad de datos que se necesiten para construirlo, dependerá de la misión del sistema autónomo. Un sistema de pilotaje autónomo de drones es mucho menos complejo que un sistema de conducción autónoma que requiere comprender un entorno más congestionado con otros vehículos, señales de tráfico… (Cummings, 2018).

Las inteligencias artificiales se pueden clasificar atendiendo a su rendimiento en relación con la mente humana (Balis y O'Neill, 2022):

— Inteligencia artificial débil, de capacidades inferiores a la mente humana.
— Inteligencia artificial general, de capacidades equivalentes a las de la mente humana.
— Súper inteligencia artificial, de capacidades superiores.

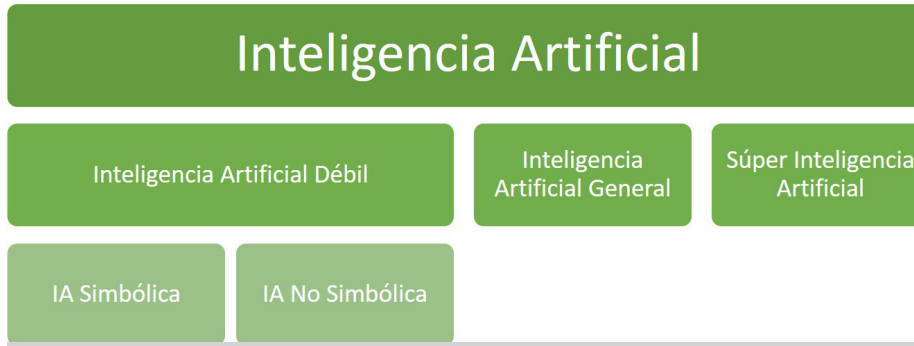

Figura 2. Clasificación de las IAs (elaboración propia)

El estado del arte actual permite asegurar que la IA general está a décadas de llegar, de modo que, en lo sucesivo, este artículo versará principalmente sobre las IA débiles. Estas, a su vez, se pueden clasificar en IA simbólica e inteligencia artificial no simbólica. La IA simbólica descansa sobre conjuntos amplios de reglas y, habitualmente, se denominan sistemas expertos. Estas IA están muy adaptadas a la resolución de problemas acotados y son relativamente predecibles e inteligibles, pero, sin embargo, son inútiles o contraproducentes fuera del problema para el que fueron diseñadas. Por el contrario, las IA no simbólicas suelen incluir redes neuronales que pueden ser entrenadas y permiten razonamiento probabilístico y aproximado, a veces se denominan sistemas de aprendizaje máquina o *machine learning* (ML). Un rasgo distintivo de estas IA es que su aprendizaje puede llevarlas a evolucionar en sentidos no previstos, posibilitando tanto aplicaciones no previstas en fase de diseño como usos aberrantes (Payne, 2021).

Una red neuronal puede imaginarse como una serie de nodos de decisión o neurones que producen salidas según diferentes probabilidades. Dichos nodos se organizan en capas y se conectan cada nodo con todos los nodos de la siguiente capa. Así, apilando capas, se producen multitud de posibles salidas para una entrada dada, representadas por el camino que la decisión toma y que se rigen por la función matemática aplicada en cada nodo y sus umbrales de probabilidades. Cuantas más capas se apilen, más precisión tendrá el modelo y más requerimientos computacionales tendrá su entrenamiento y operación.

El entrenamiento de los sistemas de ML consiste en supervisar las salidas que el sistema da frente a las entradas que recibe para, posteriormente, corregirlas. De este modo, el sistema de ML ajustará las probabilidades y funciones matemáticas con las que trabaja su red neuronal para dar salidas cada vez más adaptadas. Merece la pena reseñar aquí que, una vez entrenada una red neuronal, su operación consume mucha menos capacidad de computación; lo costoso es reentrenar una red.

Los sistemas de ML se pueden categorizar según el entrenamiento que reciben:

— ML de aprendizaje supervisado.
— ML de aprendizaje no supervisado.
— ML de aprendizaje de refuerzo.

Los sistemas ML de aprendizaje supervisado emplean datos etiquetados[6] para generar salidas en función de las entradas que se le introducen y reciben retroalimentación sobre sus salidas, esto los hace especialmente aptos para tareas acotadas como el reconocimiento de textos.

Los sistemas de ML no supervisados emplean datos sin etiquetar y no reciben retroalimentación sobres sus salidas, estos sistemas típicamente buscan patrones y aprenden a reconocerlos.

Finalmente, los sistemas con aprendizaje de refuerzo trabajan con datos sin etiquetar, pero reciben retroalimentación sobre las salidas que ofrecen, ya que tienen una finalidad concreta.

En los sistemas de ML se observan dos factores que influirán de manera notable sobre el análisis de vulnerabilidades y riesgos. Por un lado, estos sistemas dependen, en gran medida, del entrenamiento que reciban y del conjunto de datos que se emplee. Y por otro, cuando se apilan un gran número de capas en la red neuronal estos sistemas se denominan *deep*

[6] Etiquetar un dato se puede entender como dar significado a los datos que se introducen al sistema. Un ejemplo, para un sistema de reconocimiento de imágenes, sería presentar diversas imágenes de sillas asociadas a la etiqueta «asiento». Cuando la IA detecte una imagen similar, la categorizará como «asiento».

learning y se tornan tan complejos que se transforman en «cajas negras» cuyo comportamiento es difícilmente explicable o predecible. Se crean entonces situaciones en las que existen genuinas dudas acerca la bondad de las respuestas del sistema ML y comienzan a ser necesarios procedimientos de pruebas y validación (TEVV)[7] fiables para asegurarse de que la IA se comporta según los parámetros de diseño.

La necesidad de comprobar que la IA se comporta adecuadamente apunta al concepto de «fragilidad» de las IA. El estado del arte actual es que las IA son muy eficaces en problemas acotados, pero son «frágiles». La fragilidad significa que las IA son propensas a fallar impredeciblemente cuando se someten a pequeños cambios en las condiciones del entorno operativo (Balis y O'Neill, 2022; (Holland Michel, 2021)). Se trata esta, de una diferencia radical entre una IA y una inteligencia humana; mientras que la IA destaca por una superior capacidad de computación que permite exprimir cantidades ingentes de datos para obtener información valiosa, las inteligencias humanas presentan una gran capacidad de adaptación con la que realizan inferencias y generalizaciones e, incluso, emplean la intuición. Esta intuición no debe entenderse como un golpe de suerte, sino que consiste en un atajo que toma una mente altamente instruida para tomar decisiones rápidas basadas en su experiencia. Clausewitz lo identifica con el genio del comandante y Kahnemann (2011) lo reconoce en decisiones tomadas en situaciones de presión por profesionales altamente cualificados y expertos.

Cuando la fragilidad se combina con una complejidad tal que genera el efecto de «caja negra» aparece una situación en la que es necesario garantizar tanto que la IA está correctamente entrenada como que se está empleando para una tarea y en un entorno que para los que está entrenada.

A modo de ilustración, se puede citar el programa MAVEN del Ejército estadounidense. Tras la introducción de Sistemas Aéreos no Tripulados (UAS) dotados de cámaras de ultra alta resolución en labores de vigilancia en Afganistán, el ejército norteamericano se encontró que disponía de más metraje de vídeo de lo que sus analistas podían procesar y recurrió a empresas tecnológicas para desarrollar un proyecto que permitiese su procesado.

Las intenciones del Ejército norteamericano eran poder reconstruir hacia atrás los ataques de Dispositivos Explosivos Improvisados (IED) y realizar seguimiento sobre los perpetradores del ataque. Con ese seguimiento en diferido y durante los días previos al ataque se podían identificar los contactos de los atacantes, sus pisos francos, etc. Estos contactos entraban también en seguimiento y así sucesivamente, levantando las redes de IED. Este programa se entrenó con imágenes obtenidas sobre ciudades estadounidenses y alcanzó elevadas tasas de acierto, sin embargo, una vez

[7] Test, Evaluación, Verificación y Validación.

desplegado en Afganistán comenzó a dar respuestas anómalas y su tasa de acierto se redujo hasta el punto en el que los operadores desconfiaban de sus recomendaciones y fue preciso reentrenarlo. El motivo de este desajuste fue el cambio de fisonomía entre las ciudades norteamericanas y los pueblos afganos; ese cambio tuvo un efecto decisivo e imprevisto en el desempeño de MAVEN (Scharre, 2023).

En resumidas cuentas, los elementos sobre los que gravita la aplicación de las IA son los datos con los que se entrena, el proceso de entrenamiento y el algoritmo en sí mismo a los que se suma un cuarto factor: la interacción con los hombres que requiere unos niveles de confianza que no siempre se dan.

3 Vulnerabilidades de las inteligencias artificiales

Una vez examinados los tipos de IA existentes y vistos los principales factores que afectan a su implantación es necesario examinar los tipos de ataques que las IA pueden sufrir para, posteriormente, valorar los riesgos existentes. Para analizar las vulnerabilidades de los sistemas de IA, se empleará la siguiente clasificación, que excluye el daño físico a los sistemas:

- Vulnerabilidades derivadas de los datos.
- Vulnerabilidades derivadas del algoritmo.
- Vulnerabilidades derivadas de la interacción hombre-máquina.

Estas vulnerabilidades pueden deberse tanto a acciones malintencionadas de potenciales adversarios como a deficiencias en el sistema de IA. En relación con los ataques deliberados es importante reseñar que se pueden realizar de dos maneras, ataques de «caja blanca» y ataques de «caja negra». Realizar un ataque de «caja blanca» implica que se tiene conocimiento detallado del modelo que emplea la IA que se quiere atacar, lo que supone que se ha tenido acceso previo a él. Ante la dificultad de acceder al algoritmo, ya que normalmente se hallará bien custodiado, surgen los ataques de «caja negra» que son aquellos que se ejecutan cuando no se conoce el funcionamiento del algoritmo objetivo. Lógicamente, el rendimiento de un ataque de «caja negra» es menor que el de uno de «caja blanca», pero en la gran mayoría de los casos, se obtiene un efecto suficiente como para generar ventajas. Existe, además, la posibilidad de realizar ataques de «caja gris», que serían aquellos en los que se dispone de un conocimiento parcial del funcionamiento del algoritmo objetivo (Qiu et *al.*, 2019).

3.1 Vulnerabilidades derivadas de los datos

Según el Instituto de las Naciones Unidas para la Investigación del Desarme (Holland Michel, 2021), las vulnerabilidades derivadas de los

datos se subdividen en: datos incompletos, datos de mala calidad, datos discrepantes y datos incorrectos o falsos, y pueden estar causadas por:

- Condicionantes del entorno operativo (polvo, iluminación, ruido, etc.) que impiden el correcto funcionamiento de los sensores mediante los que el sistema adquiere la información del entorno.
- Ataques adversarios que alteran los datos.
- Variabilidad del entorno operativo, típica del escenario del conflicto en el que las acciones de los participantes alteran el entorno.
- Data drift, que vendría a ser grandes cambios no previstos en el desarrollo y entrenamiento del algoritmo, podría asemejarse a «sorprender» al algoritmo, aunque puede darse gradualmente[8].

Las vulnerabilidades derivadas de la manipulación de los datos se pueden dividir en técnicas adversariales y envenenamiento de datos. Fundamentalmente se basan en introducir información adicional en los conjuntos de datos (o de las etiquetas de los datos) que se emplean para el entrenamiento de la IA con la finalidad de introducir errores en el algoritmo. La diferencia estriba en que el ataque adversarial busca un efecto puntual, por ejemplo, conseguir una mala clasificación de una imagen una vez, mientras que el envenenamiento de datos busca que los datos manipulados sean tomados por datos válidos para el entrenamiento e introducir, así, efectos permanentes en el modelo que podrán ser bajo rendimiento, elevado tiempo de procesado o, simplemente, funcionamiento incorrecto. Así, se ha demostrado que variaciones sutiles en los datos de entrada (por ejemplo, variaciones en el brillo de los píxeles de una imagen imperceptibles por el ojo humano) pueden confundir al algoritmo y reducir su rendimiento (por ejemplo, clasificar un gato como una silla) (Qiu et *al*., 2019).

Por otro lado, modificaciones del entorno pueden producir que, inadvertidamente, los datos que entran en la IA difieran, sustancialmente, de los datos con que se entrenó. En este sentido, se han llevado a cabo estudios en los que se confundía el sistema de conducción de vehículos autónomos pegando pegatinas a las carreteras (Cummings, 2018).

Finalmente, otra posible técnica puede venir de la necesidad de entrenar un modelo con un reducido conjunto de datos. En este caso, una solución habitualmente empleada, es la generación de datos sintéticos para el entrenamiento, creando así una nueva vulnerabilidad ligada a los datos, el propio generador de datos sintéticos.

[8] A este respecto, debería pensarse en una evolución paulatina de los procedimientos de un agente que, tras un cierto periodo de evolución, hace que una IA que se enfrente a él se encuentre completamente desadaptadas a las técnicas que ese agente ahora emplea.

3.2 *Vulnerabilidades derivadas del algoritmo*

La manera más obvia de atacar el algoritmo es, simplemente, extraerlo para poder emplearlo a voluntad y anticipar sus decisiones. Estas técnicas pueden apoyarse por otras IA que producen aproximaciones al modelo objetivo. Una vez obtenido un modelo similar al objetivo, este podrá emplearse bien para predecir su comportamiento, bien para perfeccionar otros ataques, normalmente basados en los datos (Qiu et *al*., 2019).

Otro posible ataque sería el puro ataque cibernético para reentrenar el modelo o partes de este de manera inadvertida por el operador (Qiu et *al*., 2019).

También se podrían explotar puertas traseras en las redes neuronales. Estos ataques surgen a consecuencia de la transferencia de entrenamiento de modelos. La transferencia de entrenamiento se emplea ante la ausencia de datos para entrenar un modelo; en estos casos se emplean redes neuronales de dominio público preentrenadas con datos abundantes y se sustituyen las últimas capas por capas a medida que produzcan las salidas deseadas. La vulnerabilidad viene porque no se conozca el comportamiento de las capas que se toman del modelo, pudiendo estas incluir puertas traseras que un adversario podría explotar (Svenmarck et *al*., 2018).

Tanto las técnicas que atacan a los datos como las que afectan al algoritmo crean la necesidad de detectar cuándo el modelo de IA está manipulado y lleva a una lucha entre técnicas para de ataque y defensa, análoga a la tradicional lucha entre el proyectil y la coraza.

3.3 *Vulnerabilidades derivadas la interacción hombre-máquina*

Resta por analizar la interacción entre el hombre y la máquina. A este respecto se pueden diferenciar varios tipos de vulnerabilidades. Por un lado, destacan las vulnerabilidades asociadas con la credibilidad y, por otro, los sesgos. La credibilidad se relaciona con el rendimiento de la IA en relación con las expectativas que se ponen en ella. En este sentido, la credibilidad puede ser excesiva o demasiado poca, pero en cualquier caso es un problema que se dará en la mente de un ser humano y se relaciona con sus experiencias pasadas (Balis y O'Neill, 2022).

Los sesgos, se basan en las ideas preconcebidas en la mente de los seres humanos que se relacionan con una IA. Estos sesgos pueden manifestarse en diversas circunstancias, tanto el programador que desarrolla o entrena el modelo como la persona que selecciona los datos para entrenarlo, el equipo de validación de la IA o el operador que tiene que usar los productos que le ofrezca una IA. Toda vez que son seres humanos y tienen sesgos, son susceptibles de ser manipulados mediante operaciones en el dominio

cognitivo (Estado Mayor de la Defensa, 2024). A este respecto, cabe destacar que existen diversos sesgos cognitivos estudiados por la literatura científica de la psicología, aunque quizá, el más relevante sea el sesgo de confirmación que implica que una persona es más propensa a creer aquellas narrativas que confirman una idea anterior (Kahneman, 2011).

La desconfianza en las IA actúa no solo en la mente propia, sino en la mente de potenciales adversarios. Habida cuenta de que una mínima ventaja en el campo de la IA conlleva ventajas desproporcionadas, existen fuertes incentivos a comenzar una «carrera de armas». De este modo, si un Estado desarrolla una IA, otros estados podrán sentirse amenazados y se apresurarán a desarrollar y desplegar otras IA. En esta situación, la tentación de acortar plazos en los procesos TEVV puede ser muy fuerte y llevar a lo que que Scharre (2021) denomina una «carrera al fondo» en cuestión de seguridad.

4 Análisis de riesgos asociados a la implantación de la IA a las operaciones militares

Se toma como referencia el escenario de partida para visualizar cómo estas vulnerabilidades se transformarían en riesgos en dos situaciones, la implantación de la IA en las operaciones militares y su contraria, la renuncia a la implantación y se estudiará cómo la Función Inteligencia contribuye a mitigarlos.

4.1 Riesgos asociados a la implantación de la IA

Como ya se ha dicho, las IA razonan y toman decisiones, o las propondrán a un operador humano, tal como hacía la IA Blake frente al general García. Esta decisión de introducir una IA en apoyo a la decisión conlleva el riesgo de no comprender las propuestas que la IA ofrece. Tradicionalmente se ha optado por mantener un operador humano en el ciclo de decisión, ya sea para aprobar las sugerencias de la IA, elegir de entre un conjunto de opciones posibles, como para vetar y modificar las sugerencias erróneas. Así se asegura una cierta dosis de «sentido común» y, por otro lado, se dispone de una persona responsable de la decisión tomada.

No obstante, según progrese el desarrollo y entrenamiento de una IA sus decisiones serán, progresivamente, más y más difíciles de comprender por el ser humano, llegando al punto en el que la mera comprensión de una opción requiere del operador tanto esfuerzo cognitivo o más que decidir por sí mismo. La respuesta a esta disyuntiva es la introducción de las IA explicables, que son aquellas que explican la decisión que toman. Sin embargo, esto solo pospone el problema, ya que llegará el punto en el que las decisiones tampoco sean inteligibles (Balis y O'Neill, 2022).

Todo esto se complica en situaciones en las que se impone una rápida decisión, como pueda ser un sistema de ayuda e identificación de blancos en un carro de combate. De hecho, los sistemas antiaéreos (AEGIS, NASAMS, etc.) implementan desde hace décadas mecanismos en los que se «expulsa» al humano para poder afrontar situaciones acuciantes como la defensa antimisil de una formación naval o un ataque por saturación a una UDAA[9]; sin embargo, esta drástica decisión se toma porque se confía en que el sistema se va a comportar adecuadamente.

Desplegar IA cuyos datos de entrenamiento han podido ser alterados conlleva el riesgo de que los algoritmos tomen decisiones contrarias a los intereses propios. En esta situación estos errores podrían ser difíciles de detectar, particularmente cuando se refieren a decisiones tomadas bajo presión de tiempo.

Igualmente, la extracción del modelo podría hacer que los sistemas propios, además de volverse predecibles, fueran víctimas de ataques de manipulación de las entradas; por ejemplo, se podría engañar a un sistema de identificación de aeronaves, modificando ligeramente la silueta de las aeronaves propias con patrones de pintura o mediante EW a los sensores que proveen de entradas a la IA para aprovechar una vulnerabilidad conocida (o inducida) del modelo.

Otros riesgos podrían darse sin necesidad de intervención maliciosa del enemigo. Los cambios propios del campo de batalla podrán hacer que se generen efectos de *data drift* que desemboquen en un rendimiento mediocre

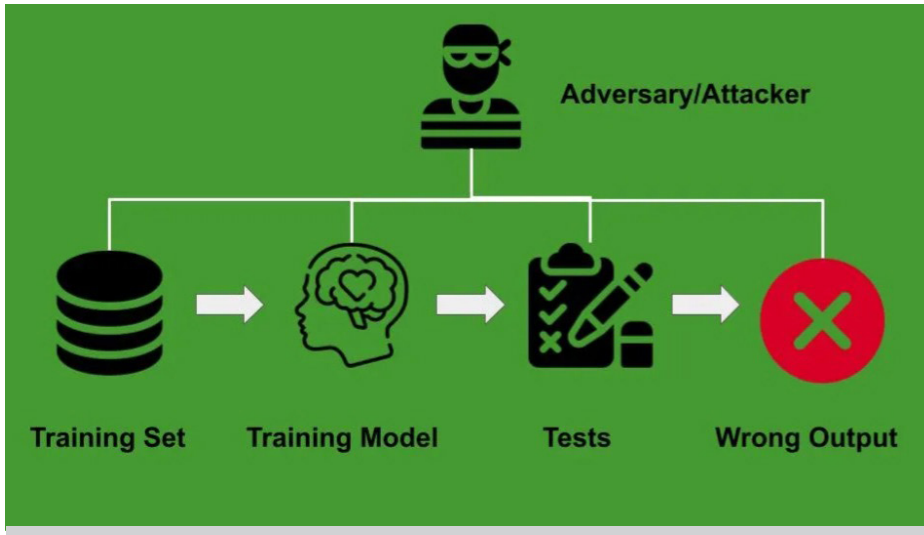

Figura 3. Técnicas de ataque adversarial (fuente: towardsdatascience.com)

[9] Unidad de Defensa Antiaérea.

o impredecible de los sistemas de IA. Este riesgo se puede exacerbar, ya que hay cierta escasez de datos relativos a conflictos armados con los que entrenar las IA propias que obligan a emplear técnicas de simulación, datos sintéticos, datos de terceros o, simplemente, datos mal seleccionados en el entrenamiento. Todos estos datos pueden conllevar sesgos que se trasladarán al algoritmo.

Una variación del riesgo del *data drift* es la simple aplicación de una IA para una tarea para la que no ha sido entrenada. En este caso se extaría exponiendo, sin paliativo posible, a todos los riesgos de la fragilidad y se debería, a falta de conocimiento tanto del algoritmo como del entorno operativo en el que se opera. La principal consecuencia de este riesgo es una pérdida de confianza en el algoritmo tal que se deje de usar (Balis y O'Neill, 2022; (Morgan et *al*., 2020)), lo que significaría que los recursos empleados en su desarrollo habrían sido mejor invertidos en cualquier otra tarea.

Este riesgo de falta de confianza es, posiblemente, el más importante. El ser humano quiere predecir el futuro y valora que sus compañeros de tareas sean predecibles, lo que será imposible si la IA opera fuera del marco para el que se desarrolló. Para mitigar este riesgo será necesario entrenar a los operadores y comandantes humanos para que sepan qué pedirle a una IA, dónde aplicarla y qué esperar de ella, y disponer de unos protocolos TEVV que aseguren que la IA se comporta según fue diseñada. No obstante, existe la versión contraria de este riesgo como es el «sesgo de automatización», que es la tendencia a asumir sin cuestionar las soluciones que propongan las IA, cuya mitigación es igual a la de la falta de confianza (Balis y O'neill, 2022).

No se debe olvidar el riesgo reputacional. Una imperfecta o poco ética aplicación de la IA puede producir un daño reputacional a explotar por el adversario, particularmente en lo tocante al Derecho Internacional de los Conflictos Armados (DICA). Así cabe preguntarse qué capacidad tendrá una IA de interpretar los detalles que le permitan aplicar los principios de, entre otros, Distinción, Proporcionalidad y Precaución, ampliamente reconocidos como claves del DICA y extendidos en la cláusula Martens[10]. Es evidente que cualquier incumplimiento del DICA por parte de un actor, será inmediatamente explotado por sus adversarios en el ámbito informativo.

La propia operación del algoritmo será otra posible fuente de riesgos. Será preciso proteger qué decisiones han sido tomadas por un algoritmo, así como las entradas que esta recibió para impedir que sea sometido a ingeniería inversa y se modele, aunque sea groseramente, su comportamiento

[10] Esta cláusula, incluida en el Protocolo Adicional 1, establece que las protecciones consagradas en los protocolos se deben basar en los principios de humanidad y los dictados de la conciencia pública.

para pasar de realizar ataques de «caja negra» a realizar ataques de «caja blanca» o «gris». Como ya se ha visto, esto permitiría la aplicación de técnicas muy adaptadas y eficaces frente a la IA objetivo.

Por último, resta hablar de los niveles estratégico y político. Si la introducción de IA tiene el efecto de comprimir los ciclos de decisión (Morgan et *al*., 2020; (Ryan 2022), podrán darse situaciones de gestión de crisis en las que se produzcan escalamientos indeseados y que el nivel estratégico disponga de menos flexibilidad para afrontar una crisis. Esta problemática se puede agravar cuando se combinen las IA en apoyo a la decisión con sistemas autónomos; entonces puede ocurrir que, ante la perspectiva de una guerra incruenta entre máquinas en la que no mueran combatientes, el nivel político sucumba a la tentación de iniciar conflictos. Conceptos como disuasión o coerción tendrán que ser forzosamente revisados según avance la aplicación de las IA en la toma de decisiones estratégicas y políticas (Payne, 2021).

Como se ha visto, en una situación en la que la puesta en funcionamiento de una IA por un actor supone un riesgo para otros actores, puede generarse una «carrera hacia el fondo». Consecuentemente, existirán dudas fundadas sobre la robustez de los sistemas desplegados o, dicho de otra manera, sospechas de que son frágiles e impredecibles. Se entra entonces en una dinámica en la que las decisiones estratégicas de los estados se tornan impredecibles, particularmente cuando la IA se aplica en apoyo a la toma de decisiones niveles políticos y estratégicos de decisión. Los estudios clásicos sobre teoría de decisión estratégica postulan que, en tal situación, se generarían incentivos perversos tendentes a protegerse frente a la sorpresa que, normalmente, toman la forma de ataques preventivos y posturas agresivas para conjurar el miedo a verse sorprendido (Schelling, 1960). Se hace preciso, entonces, restaurar la confianza.

4.2 Riesgos asociados a la no implantación de la IA

Como ya se ha dicho, la guerra es una actividad humana y es lógico pensar que el corpus doctrinal y los conceptos que utilizados para hacer referencia a ella lo reflejen y apunten a características y limitaciones de la mente humana. Así, se habla de principios como la voluntad de vencer, se emplean efectos cognitivos y usan estrategias que se basan en la disuasión, la coerción, la dislocación… que, parafraseando al general Gan (2021), suceden en la mente del adversario.

El modo de guerra español, consagrado en las doctrinas aliadas AJP-01, AJP-03, AJP-05 y en la PDC-01A, se fundamenta en una aproximación indirecta, basada en una superior maniobra que produce efectos de choque, se mete en el ciclo de decisión del enemigo, le roba la iniciativa y lleva a

efectos desproporcionados, incluso aprovechando la sorpresa. Se combaten en varios ámbitos de actuación, de los cuales uno es el cognitivo, y se ejecutan operaciones de influencia, de información, psicológicas y de comunicación; por mencionar algunos conceptos.

Es decir, existe un modo de hacer la guerra específicamente adaptado a enfrentarse a comandantes y combatientes humanos que tienen limitaciones cognitivas y sufren estrés, ansiedad y miedo. Cabe preguntarse si las herramientas conceptuales con las que se combate serán eficaces no solo frente a una IA, que no está sujeta a esas limitaciones de la mente humana, sino frente a una mente humana muy asistida por una IA y que, en consecuencia, es eminentemente racional y poco pasional.

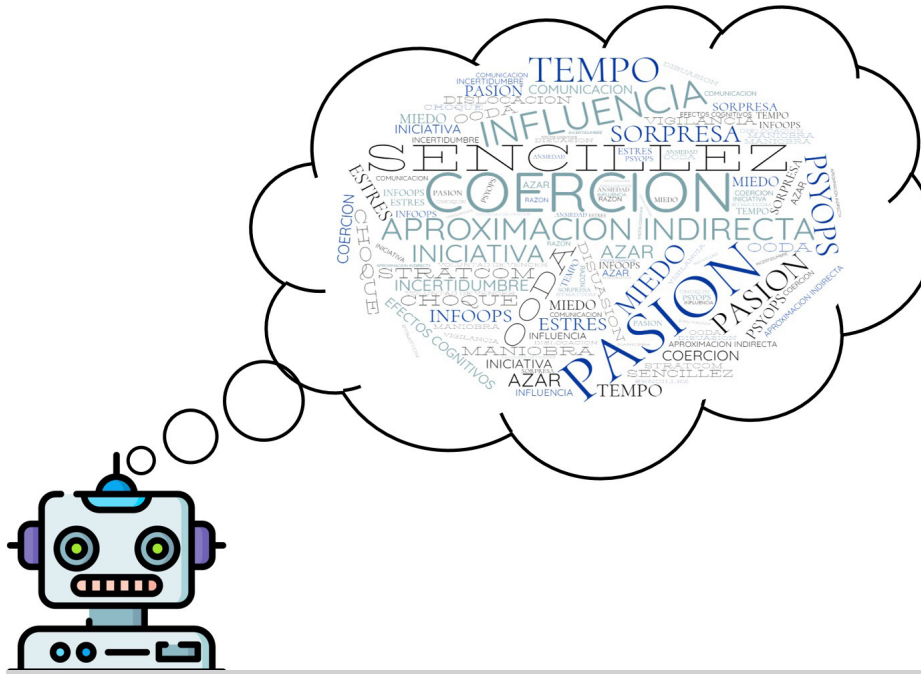

Figura 4. Robot usando conceptos de planeamiento (fuente: freepik.com)

La experiencia de aplicación de IA en el campo de los juegos por ordenador (como ajedrez, go, póker o simuladores de combate) permite afirmar que las IA «piensan distinto» y hace vislumbrar qué sucede cuando un humano se enfrenta a una IA. Lo más común que suelen referir quienes se han enfrentado a una IA es que esta emplea todo el tablero o escenario a la vez para hacer ataques constantes y sin pausa. Ello es lógico por cuanto la IA tiene capacidad de procesar toda la información que recibe y no necesita focalizar su limitada cognición en áreas del tablero como sus contrapartes

humanas. Al no sufrir estrés ni miedo, ni estar afectada por sesgos cognitivos como la aversión a las pérdidas[11], la defensa deja de tener ventajas y, por tanto, la IA siempre está dispuesta a hacer sacrificios a corto plazo para obtener ventajas posteriores; decisiones que a un humano le costaría mucho más tomar. Además, debido a su superior capacidad de computación, no tienen altibajos en su actividad, ni en el tiempo ni en el espacio (Payne, 2021).

Esto, traducido a términos militares, significa un tempo elevado y constante, sin cambios de fase, con actividad en toda la profundidad del despliegue, siempre a la ofensiva, empleando modos de acción muy agresivos y disponiendo siempre de ramas y secuelas para adaptar la actuación al devenir del combate. La consecuencia cognitiva de enfrentarse a un enemigo de este tipo es que el comandante humano deberá afrontar sensaciones de impotencia e indefensión. Como anécdota se puede mencionar que, durante el ciclo de partidas que Garry Kasparov jugó contra *Deep Blue*, hubo una ocasión en la que *Deep Blue* se equivocó. Kasparov, que le había atribuido *supercapacidades* al ordenador, interpretó ese error como que el ordenador era capaz de computar más de veinte movimientos por delante. Con esta presunción en mente, en la siguiente partida, se rindió en una situación que podría haber resuelto.

Sirva esto como ejemplo de lo que puede implicar enfrentarse a una IA sin otra de respaldo. Sería enfrentarse a un enemigo al que no se comprende, porque no piensa como un humano, contra el que las herramientas podrían mostrarse inútiles, minando la moral. Por muy adiestradas que estuvieran las FF. AA. sería como enfrentar a Nadal contra Federer, solo que Nadal jugaría con una pala de pingpong.

En esta situación es imperativo aprender a competir, donde eso sea posible, frente a una IA. Sin embargo, será tremendamente complicado encontrar adversarios que estén dispuestos a ejercer de esparrin y compartir esa información para adiestrar a las fuerzas propias, por no hablar de la dificultad para interpretar las enseñanzas así obtenidas. Del mismo modo, la renuncia a emplear IA en aplicaciones militares originará una falta de experiencia que impedirá desarrollar las técnicas que permitan afrontar con éxito a un adversario asistido por la IA.

Quedarse rezagado tendría, además, consecuencias en un entorno marcado por la proliferación. En un mundo en el que quedarse atrás puede tener desastrosas consecuencias, es previsible que, cada vez más, los

[11] Este sesgo se ejemplifica con el refrán «más vale pájaro en mano que ciento volando», es el sesgo que hace rechazar una hipotética ganancia futura por asegurar una posesión presente o que hace que las personas se arriesguen a pérdidas mayores ante una situación real de pérdida, como el jugador que acepta un doble o nada para tratar de evitar una pérdida. Para mayor detalle se recomienda el trabajo de Kahneman.

países amigos y aliados abracen esta tecnología. Se podrá llegar entonces a un punto en el que las unidades españolas tengan serias dificultades para integrarse en las operaciones militares de las alianzas y coaliciones o que España sea un candidato indeseable para ejercer el mando de unidades multinacionales. Dicho de otra manera, el hecho de no disponer de IA puede significar una vulnerabilidad para cualquier alianza o coalición que sí las emplee, bien por incapaces o bien por no confiables al hacer la guerra «a la humana». Todo esto minaría la posición internacional de España y reduciría su influencia en la arena global.

5 Gestión del riesgo desde el punto de vista de la inteligencia

Introducidos los riesgos presentes, se estudia ahora algunas opciones que la Función Conjunta Inteligencia pone a disposición de las FF. AA. para mitigarlos. La Función Inteligencia es «el resultado de la obtención dirigida y la elaboración de la información, relativa al entorno, capacidades e intenciones de los actores, con el fin de identificar las amenazas existentes y facilitar al Comandante decidir con oportunidad» (Estado Mayor de la Defensa, 2020). Además, la inteligencia se relaciona con la contrainteligencia, que se define como el «conjunto de actividades que conducen a identificar, analizar y contrarrestar las amenazas a la seguridad [...]» (*Íbid.*) y se relaciona con la Seguridad y con la Protección de la Fuerza.

Para analizar estos riesgos se divididen en dos: riesgos que no requieren de un adversario para afectar a las operaciones, y riesgos que se crean por acción de un adversario. Los primeros pueden deberse a la falta de conocimiento sobre uno mismo. Decía Sun Tzu: «[S]i conoces al enemigo y te conoces a ti mismo, no temas el resultado de cien batallas» (Tzu, 1999), a lo que sería preciso añadir, en línea con la definición de inteligencia, «y conoces el entorno operativo». Para aumentar el conocimiento de uno mismo será preciso disponer de unos procedimientos TEVV que produzcan IA robustas, tal como se intuye según la Estrategia de Inteligencia Artificial en el Ministerio de Defensa cuando establece los principios de Inteligibilidad y Trazabilidad, Fiabilidad y Transparencia, Gobernabilidad y Mitigación del sesgo (Ministerio de Defensa, 2023).

La importancia de los procesos TEVV estriba en el profundo conocimiento sobre los modelos que permite. En primer lugar, permite conocer en qué condiciones del entorno operativo la IA es confiable, lo que generará en el comandante ciertas necesidades de información para asegurar, constantemente, que las IA se emplean dentro de sus parámetros de diseño. A este respecto, el Instituto de Investigación para el Desarme de la ONU considera que, en caso de que un sistema autónomo viole el DICA, se podrían deducir consecuencias penales para aquellos comandantes que, sabiéndolo, hayan empleado IA fuera de sus parámetros de diseño o no hayan puesto celo

suficiente en cerciorarse de que las IA se emplean correctamente (Holland Michel, 2021).

En segundo lugar, el procedimiento TEVV permite establecer qué datos deben alimentar[12] al modelo para que funcione, pudiéndose convertir en necesidades de información si el comandante así lo estima. Finalmente, un procedimiento TEVV robusto proporciona un detallado conocimiento del comportamiento de los modelos, lo que aumenta su predictibilidad y permite verificar que los modelos se comportan como deben; estos indicadores sobre el comportamiento de los propios modelos podrían convertirse también en necesidades de información.

Los riesgos de la IA asociados al adversario se presentan, normalmente, derivados a su esfuerzo por obtener superioridad en la información, afectando a los ciclos de decisión propios. Así, el adversario buscará explotar las vulnerabilidades y riesgos de la IA para obtener beneficio, para lo que necesitará obtener un conocimiento detallado de ellas. No es de extrañar, por tanto, que intente obtener información sobre los datos que fundamentan las decisiones, la identidad y sesgos de las personas que deciden, las actividades concretas en las que se aplica la IA, los resultados de las decisiones y un largo etcétera. La consecuencia es clara: es vital proteger el ciclo de decisión.

Para alcanzar un nivel de protección suficiente, es imprescindible aplicar medidas de Seguridad de las Operaciones y Protección de la Fuerza orientadas a partir de una robusta contrainteligencia. En relación con los datos y algoritmos, se debe aplicar un estricto control al personal que accede a ellos para evitar filtraciones, incluyendo medidas de filtrado y entrevistas especiales. En el caso de la IA esto cobra mayor importancia si cabe, ya que, normalmente, los desarrollos y entrenamientos de las IA estarán subcontratados a empresas del ramo de Defensa. Por ello es fundamental desarrollar políticas y regulaciones que permitan realizar inspecciones de contramedidas de vigilancia técnica y asegurar que los datos y algoritmos en poder de empresas y personas están debidamente protegidos, que se aplican las medidas de SEGINFOSIT pertinentes, que el personal que trabaja con ellos está debidamente seleccionado y firma contratos de confidencialidad, y que, en caso de que pasen a trabajar para otras empresas, el conocimiento que puedan transferir es inútil, bien por su falta de contexto, bien por su obsolescencia. Es inaceptable que el mismo ingeniero que ha desarrollado modelos para las FF. AA. españolas pueda trasferir luego conocimiento a potenciales adversarios.

[12] Por «alimentar» debe entenderse la acción de introducir datos al algoritmo ya entrenado. El procedimiento TEVV dará un profundo conocimiento cualitativo sobre estos datos.

Asimismo, las operaciones de información adversarias actuarán en el domino informativo para influir en los «decisores» (se emplea aquí este término para designar al ente que decide, sea persona o algoritmo). Para evitar la desventaja, es preciso negar a potenciales adversarios la información sobre quién decide qué y, particularmente, qué fases y tareas del ciclo de decisión se apoyan en IA. De este modo, se obligará al adversario a dispersar su esfuerzo tanto en inteligencia para obtener ese conocimiento como en INFOOPS para producir los efectos deseados. A este respecto, es indudable que la realización de ejercicios y operaciones multilaterales supone un desafío que obliga a compaginar la protección del ciclo de decisión propio con la obligación de comunicarse lo suficiente como para trabajar con países amigos y aliados.

Por su parte, los procesos TEVV merecen un tratamiento especial. Pocas cosas serían más atractivas para un potencial adversario que favorecer que las FF. AA. españolas desplieguen soluciones deficientes. Por esto, se deberá proteger tanto al personal que participe en los procesos TEVV como al proceso en sí mismo, de principio a fin, incluyendo datos de partida y resultados obtenidos para evitar ofrecer a los adversarios oportunidades de realizar ingeniería inversa a los algoritmos.

Sin embargo, el ejercicio de la disuasión obliga a realizar compromisos, ya que, para disuadir a un adversario, es preciso un cierto grado de comunicación hacia potenciales adversarios (Schelling, 1960); es imposible disuadir a un adversario con quien la comunicación es imposible. Por lo tanto, hay que alcanzar un punto de equilibrio entre la información que se publica (o se deja que se haga pública) para influir al potencial adversario y los elementos que se deben proteger. Esto está claramente identificado en el corpus doctrinal de INFOOPS como Elementos Esenciales de Información Propia o EEFI por sus siglas en inglés. Además, la correcta identificación de estos EEFI permite la aplicación de técnicas de decepción, ya que, ante la falta de elementos de decisión, el adversario los buscará y se hará vulnerable a la decepción.

Además, es necesario asegurar a terceros países que España dispone de procedimientos TEVV robustos que impiden que entren en servicio IA mal desarrolladas con comportamientos erráticos. Así, al dar garantías de que las hipotéticas decisiones que se tomarían en una situación de crisis no son erráticas, se desactivaría la tentación de realizar ataques preventivos por miedo a verse sorprendido. Esta necesidad de construir confianza en las IA encuentra reflejo en estrategias de países del entorno, como los Estados Unidos (U.S. Department of Defense, 2023) o Reino Unido (U.K. Ministry of Defence, 2022). Sin embargo, no se debe dar un nivel de información que posibilite ataques a los procesos TEVV mismos, ni se deben publicar pormenores propios de los modelos que se sometan a pruebas. Es decir, hay que dar garantías de que se dispone de unos procedimientos TEVV robustos sin detallar ni el proceso ni los modelos que se prueben.

Desde el punto de vista de la Protección de la Fuerza esto implica un desafío colosal en un campo de batalla, y por extensión un entorno operativo (no se debe olvidar que las FF. AA. también realizan actividades en tiempo de paz), cada vez más sensorizado y frente a un adversario que aplique técnicas de *big data* que obliga a las FF. AA. a emplear una gran cantidad de su esfuerzo en la denegación de firmas[13] para dificultarle al adversario el acceso a información relevante (Ryan, 2022).

Sin embargo, no se podrá denegar completamente la firma propia al enemigo, por lo que habrá que coordinar íntimamente la Contrainteligencia con las INFOOPS, en todos los niveles de planeamiento y desde tiempo de paz, para identificar y proteger los EEFI a la vez que se ofrece una narrativa convincente y con visos de verosimilitud a los ojos del adversario.

En cuanto a los riesgos asociados al potencial empleo hostil de la IA, la situación se invierte; se debe volcar el esfuerzo en atacar el ciclo de decisión del adversario. De este modo, es necesario tener una imagen tan clara como sea posible del ciclo de decisión adversario para identificar qué indicadores o datos emplea para sus decisiones y cómo los obtiene, qué algoritmos emplea o, en su defecto, los resultados de sus decisiones para inferir cómo funcionan y qué humanos intervienen en estas decisiones.

Las consideraciones hechas para el proceso de TEVV propio son igualmente aplicables, pero en sentido inverso: la posibilidad de propiciar que los potenciales adversarios desplieguen soluciones deficientes y el elevado nivel de conocimiento que se puede obtener de un modelo si se consigue acceso a estas pruebas las convierten en objetivos altamente rentables sobre los que volcar el esfuerzo de inteligencia propio.

En el entorno actual es muy posible obtener buena cantidad de inteligencia mediante el uso de fuentes abiertas, por ello las disciplinas de OSINT y MASINT[14], y los campos de SOCMINT y STI[15] cobrarán una importancia capital. De este modo, las necesidades de información dirigirán el proceso de obtención hacia ganar conocimiento sobre los algoritmos que los potenciales adversarios emplean para sus decisiones y los datos sobre los que actúan. Obtenido este conocimiento, se deberán volcar otras capacidades de corte más ofensivo para atacar tanto los datos como los modelos o, al menos, conocer su funcionamiento.

---

[13] Se entiende firma como cualquier emisión o información, cambio en el patrón de actividad... que permite al adversario ganar conocimiento sobre las actividades propias. No tiene que referirse a emisiones electromagnéticas, ya que indicadores como el nivel de ocupación del *parking* de una Base, cambios en las rutas aéreas... pueden apuntar a un aumento de actividad militar y, por ende, delatar un inminente despliegue.

[14] Inteligencia de firmas.

[15] Inteligencia científica y tecnológica.

No se debe olvidar que gran parte del esfuerzo de obtención del adversario se enfocará, precisamente, en la actividad propia. Esto dará la oportunidad de aplicar el ingenio y emplear técnicas de decepción. Así, medidas tendentes a alterar la firma propia harán que, en el momento de la verdad, cuando el adversario deba aplicar sus algoritmos, estos se encuentren operando con datos para los que no están entrenados; se debe pensar en alterar, quizá sutilmente, las siluetas de las plataformas (o quizá tener previstos implementos que la alteren) o la disposición de las bases y despliegues, proporcionar información sesgada de las actividades que alimenten al sistema adversario con datos erróneos, etc. el ingenio jugará un gran papel en este campo.

En cualquier caso, implantación de la IA o no implantación, parece evidente que la entrada de un nuevo jugador, las IA, en el tablero del conflicto va a imponer una notable carga de trabajo sobre unos organismos dedicados a la Inteligencia y la contrainteligencia que deberán ser adecuadamente provistos de personal y medios. Igualmente, la irrupción de las IA en el entorno operativo obligará a una, si cabe, más estrecha relación entre las funciones de Inteligencia, Seguridad y Protección de la Fuerza de modo que se refuercen entre sí y protejan la fuerza propia al tiempo que detectan vulnerabilidades en el adversario.

6 Conclusión

En la Era de la Información es inevitable aplicar las herramientas que esta Era trae a las actividades humanas y, entre ellas, a la guerra. El estado actual de arte, con inteligencias bastante acotadas y «frágiles», apunta a la necesaria interacción entre el hombre y la máquina para poder conjugar el potencial de las IA con las capacidades de inferencia, generalización y adaptación propias de la inteligencia humana y pone de manifiesto la importancia del dominio cognitivo y la dimensión informativa del entorno operativo futuro.

El MDEF, siguiendo las directrices de la UE, ha optado en su estrategia por una implantación responsable de la IA que hace hincapié en aspectos como la rendición de cuentas y la robustez y que limita los casos de uso en los que la IA encuentra su lugar. Sin embargo, España y Occidente podrían verse inmersos en una carrera armamentística frente a adversarios que podrían no tener tantos escrúpulos como Occidente a la hora de aplicar esta tecnología.

Como todas las decisiones, la de introducir la IA en el campo de batalla presenta riesgos que es preciso analizar y mitigar para evitar que se transformen en amenazas. Para ello, se ha imaginado una situación de conflicto hipotético en el que un país que ha implantado una IA se enfrenta, apoyado

por un país que no la ha implantado, a un país que lo ha hecho más tardíamente o de manera imperfecta. Este marco mental permite visualizar cómo las vulnerabilidades inherentes a la IA en el campo de batalla se manifestarían en forma de riesgos y amenazas concretas.

La Función Conjunta Inteligencia, intensiva en la dimensión informativa del campo de batalla, ofrece una serie de soluciones aplicables para mitigar los riesgos que la IA trae consigo al campo de batalla moderno. Además, su relación con las actividades de Contrainteligencia, Protección de la Fuerza y Seguridad de Operaciones proporciona un marco de trabajo ideal para gestionar muchos de estos riesgos. De este modo, el comandante dispondrá de la capacidad de operar en un campo de batalla futuro en el que el propio devenir del combate se sumará a la acción del adversario para hacer que las vulnerabilidades de la IA se manifiesten en riesgos.

Con el superior conocimiento del entorno operativo y las intenciones hostiles de que la Inteligencia provee, sumado a un conocimiento exhaustivo de las capacidades propias, el comandante podrá emplear sus IA de forma segura y lícita sin incurrir en más riesgos que los que el propio combate imponga, incluso frente a la acción enemiga. Sin embargo, la inteligencia es una función dirigida, lo que implica que será preciso identificar los elementos de información precisos para alimentar el ciclo de inteligencia.

En un sentido contrario, la correcta aplicación de la contrainteligencia para dirigir las acciones de Protección de la Fuerza y de OPSEC hará posible que, incluso frente a adversario con superiores capacidades de IA, las FF. AA. españolas puedan operar con ciertas garantías de éxito. La decepción, el engaño y el ingenio jugarán un papel primordial en el campo de batalla futuro para confundir las decisiones enemigas. Para esto, será necesario conocer los ciclos de decisión enemigos y actuar sobre sus elementos más débiles con acciones en la dimensión informativa que podrían comenzar incluso antes de la apertura de hostilidades.

En el estudio de estos riesgos se ha detectado la necesidad de disponer de procedimientos TEVV robustos, pero no solo disponer de ellos, sino que será necesario hacer público y notorio este extremo. Solo así se podrá conjurar el peligro de que potenciales adversarios se sientan tentados de iniciar acciones hostiles preventivas por miedo a verse sorprendidos por decisiones imprevisibles tomadas por IA «frágiles». En este sentido, el concepto de disuasión seguirá vigente aunque requerirá soluciones de compromiso entre la información que se disemina y la que se protege.

En resumidas cuentas, la irrupción de las IA en el entorno operativo obligará a realizar un esfuerzo suplementario en inteligencia que deberá ser adecuadamente dotado si las FF. AA. españolas aspiran a mantener un papel relevante en el entorno operativo del futuro.

Bibliografía

Balis, C. y O'Neill, P. (2022). *Trust in AI: Rethinking Future Command | Royal United Services Institute* [en línea]. Londres, Royal United Services Institute. [Consulta: 22 de noviembre de 2022]. Disponible en: https://www.rusi.org/explore-our-research/publications/occasional-papers/trust-ai-rethinking-future-command

Cummings, M. (2018). Artificial intelligence and the future of warfare. *Artificial Intelligence and International Affairs: Disruption Anticipated* [en línea]. Londres, Chatham House for the Royal Institute of International Affairs London, pp. 7-18. ISBN: 978 1 78413 212 5. [Consulta: 2024]. Disponible en: https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf

Estado Mayor de la Defensa. (2020). *PDC-02 Doctrina de Inteligencia*. Madrid, Estado Mayor de la Defensa.

—. 2024. Visión del JEMAD de la Inteligencia Artificial en las FAS. Madrid, Estado Mayor de la Defensa.

Gan, F. (2021). Alocución del general Gan [en línea]. *Hispanidad*. [Consulta: 10 de enero de 2024]. Disponible en: https://www.hispanidad.com/uploads/s1/52/12/03/img-2071.mp4

Holland Michel, A. (2021). *Known Unknowns: Data Issues and Military Autonomous Systems*. [en línea]. [Consulta: 25 de enero de 2024]. Genova, Disponible en: https://unidir.org/publication/known-unknowns

Kahneman, D. (2011). *Pensar rápido, pensar despacio*. Barcelona, Penguin Books. 6ª.. ISBN: 978-84-9032-250-5.

Ministerio de Defensa. (2023). *Resolución 11197/2023, de 29 de junio, de la Secretaría de Estado de Defensa, por la que se aprueba la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa* [en línea]. Madrid. [Consulta: 26 de enero de 2024]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/2/0/20230706.pdf

Morgan, F. E. et al. (2020). *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World* [en línea]. Santa Monica, RAND Corporation PP - Santa Monica. ISBN: 9781977404923. [Consulta: 2024] Disponible en: https://www.rand.org/pubs/research_reports/RR3139-1.html

Payne, K. (2021). *I, Warbot: The Dawn of Artificially Intelligent Conflict*. Oxford University Press. ISBN: 978-0197611692.

Qiu, S. et *al*. (2019). Review of Artificial Intelligence Adversarial Attack and Defense Technologies [en línea]. *Applied Sciences*. Vol. 9, n.º 5. ISSN: 2076-3417. [Consulta: 25 de enero de 2024]. DOI 10.3390/app9050909. Disponible en: https://www.mdpi.com/2076-3417/9/5/909

Ryan, M. (2022). *War Transformed: The Future of Twenty-First-Century Great Power Competition and Conflict*. Naval Institute Press. ISBN: 978-1682477410.

Scharre, P. (2021). Debunking the AI Arms Race Theory [en línea]. *Texas National Security Review*. Vol. 4, n.º 3. [Consulta: 28 de enero de 2024]. Disponible en: https://tnsr.org/2021/06/debunking-the-ai-arms-race-theory/

—. (2023). Four Battlegrounds: Power in the Age of Artificial Intelligence. W. W. Norton & Company. ISBN: 978-0393866865.

Schelling, T .C. (1960). *The Strategy of Conflict*. Harvard University Press. ISBN: 978-0674840300.

Smith, R. (2005). *The Utility of Force*. 1. Londres, Penguin Books. ISBN: 978-0-141-02044-0.

Svenmarck, P. et *al*. (2018). Possibilities and Challenges for Artificial Intelligence in Military Applications [en línea]. *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*. [Consulta: 27 de enero de 2024]. Disponible en: https://www.researchgate.net/publication/326774966

Tzu, S. (1999). *El arte de la Guerra*. Madrid, Ediciones Martínez Roca. ISBN: 978-84-270-2499-1.

Unión Europea. (2024). *Artificial Intelligence Act* [en línea]. Bruselas, Parlamento Europeo. [Consulta: 20 de enero de 2024]. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf.

U.K. Ministry of Defence. (2022). *Defence Artificial Intelligence Strategy*. Londres, U.K. Ministry of Defence.

U.S. Department of Defense. (2023). *Data, Analytics, and Artificial Intelligence Adoption Strategy*. Washington D.C., U.S. Department of Defense.

¿Regreso al futuro? La función de inteligencia y las, no tan nuevas, amenazas a la Seguridad Nacional

Álvaro Cremades Guisado

Resumen

El progresivo desplazamiento del terrorismo internacional como prioridad para las políticas de Seguridad Nacional de un creciente número de países y la emergencia, en su lugar ,de la amenaza constituida por las acciones de otros Estados es una muestra perentoria de la transición hacia un nuevo entorno estratégico en la que se encuentran hoy las instituciones estatales dedicadas a la producción de inteligencia.

En ese sentido, la pugna entre grandes potencias con capacidades próximas a la paridad, como Estados Unidos, Rusia o China, abre importantes interrogantes sobre el futuro inmediato de dichas instituciones ante las amenazas a la Seguridad Nacional que derivan de esta competición estratégica. Si bien la producción de inteligencia es hoy una actividad que hace un uso intensivo de diferentes tecnologías, ante un escenario como el referido el poder de inteligencia de las naciones se encuentra también condicionado por la capacidad de «actuar concertadamente», estableciendo relaciones que permitan diferentes formatos de colaboración internacional en materia de inteligencia, lo que posibilita anticipar una mayor convergencia de la inteligencia y la diplomacia.

A tal efecto, el presente artículo se pregunta, con fines exploratorios, sobre los desafíos que esta era de competición estratégica entraña para las instituciones estatales dedicadas a la producción de inteligencia en diferentes áreas de su actividad, planteando la necesidad de una reflexión sosegada sobre sus procesos de adaptación a este nuevo entorno.

Palabras clave

Servicios de inteligencia, Guerra Fría, China, Rusia, Estados Unidos.

Back to the future? The intelligence function and the, not so new, threats to national security

Abstract

The progressive displacement of international terrorism as a priority for the national security policies of a growing number of countries and the emergence in its place of the threat posed by the actions of other States

is a compelling sign of the transition towards a new strategic environment in which state institutions dedicated to the production of intelligence find themselves today.

In that sense, the struggle between major powers with capabilities close to parity, such as the United States, Russia or China, raises important questions about the immediate future of these institutions in the face of threats to national security arising from this strategic competition. Although the production of intelligence is today an activity that makes an intensive use of different technologies, before a scenario such as the one referred to the intelligence power of nations is also conditioned by the ability to "act in concert" establishing relationships that allow different formats of international collaboration in intelligence, which allows anticipating a greater convergence of intelligence and diplomacy.

In this regard, this article asks for exploratory purposes about the challenges that this era of strategic competition entails for state institutions dedicated to the production of intelligence in different areas of their activity, raising the need for a calm reflection on their processes of adaptation to this new environment.

Keywords

Intelligence, Cold War, China, Russia, United States.

1 De la guerra global contra el terror al desafío sistémico chino

Siguiendo un estilo retórico que tiene sus antecedentes en las declaraciones de la «Guerra contra el Crimen» realizadas por el presidente Lyndon Johnson y de la «Guerra contra las Drogas» por el presidente Richard Nixon, el 16 de septiembre de 2001, el presidente George W. Bush declaraba desde las instalaciones del complejo de Camp David la «Guerra contra el Terror». Aunque este concepto sería fuertemente criticado desde sus mismos orígenes por diferentes motivos, la Guerra Global contra el Terrorismo (GWOT) terminaría por popularizarse como una denominación relativamente informal para un periodo de dos décadas, inmediatamente posterior a la posguerra fría, en cuyo transcurso la lucha contra las organizaciones terroristas internacionales cobraría una posición de centralidad en la política exterior y doméstica estadounidense (y, con ella, la de no pocas naciones aliadas), encontrando su epitafio en la finalización de la misión *Resolute Support* y la consiguiente retirada de la fuerza multinacional de la OTAN del territorio afgano en septiembre de 2021.

Aunque durante la Administración Obama la lucha contra el terrorismo internacional se mantendría como una de sus principales prioridades, durante el primer mandato de Barack Obama este concepto entraría en desuso a medida que las prioridades, en materia de política exterior, que habían caracterizado a su predecesor serían paulatinamente desplazadas a favor de una mayor atención a la emergencia de China como potencia regional y global: el denominado *Pivot to Asia*. En 2011, la entonces directora del Departamento de Estado, Hillary Clinton, ofrecería en las páginas de *Foreign Policy* una elocuente descripción de este giro:

> «A medida que la guerra en Irak se reduce y Estados Unidos comienza a retirar sus fuerzas de Afganistán, Estados Unidos se encuentra en un punto crucial. En los últimos 10 años, hemos asignado inmensos recursos a esos dos teatros. En los próximos 10 años, necesitamos ser inteligentes y sistemáticos sobre dónde invertimos tiempo y energía, para ponernos en la mejor posición para mantener nuestro liderazgo, asegurar nuestros intereses y promover nuestros valores. Por lo tanto, una de las tareas más importantes de la política de Estados Unidos en la próxima década será la de asegurar una inversión sustancialmente mayor -diplomática, económica, estratégica y de otro tipo- en la región de Asia y el Pacífico» (Clinton, 2011).

A partir de entonces, la atención prestada por los Estados Unidos a los acontecimientos en Asia Oriental aumentarían considerablemente, produciéndose un reforzamiento de sus relaciones bilaterales con socios como Japón o Australia, de su vínculo con organizaciones multilaterales como la Asociación de Naciones del Sudeste Asiático (ASEAN, en inglés), o de su papel en episodios como los relativos a las disputas en el llamado «Mar Meridional de China»; lo que sería visto por China como un intento de los

Estados Unidos por imponer una estrategia de contención ante su ascenso como potencia regional y global (*Task Force*, 2016). De forma simultánea, una Rusia de creciente actividad antagonista frente a la OTAN y los Estados Unidos en el espacio postsoviético, incluyendo episodios como la guerra ruso-georgiana de 2008 o la intervención militar sobre la península de Crimea en 2014, servirían como indicadores del regreso de dinámicas de pugna interestatal propias de la Guerra Fría (Pérez, 2019).

No sería, sin embargo, hasta la presidencia de Donald Trump que este cambio de prioridades obtendría una calificación más categórica. Se acuñaría entonces el concepto de «competición entre grandes potencias» (*great power competition*), para hacer referencia al regreso de ciertas dinámicas de pugna entre Estados ante la pretensión de la República Popular China (RPC) y de Rusia por cambiar el orden internacional, reafirmando su influencia regional y mundial, de acuerdo con la Estrategia de Seguridad Nacional adoptada en 2017 (The White House, 2017); noción que encontraría continuidad posterior (aún con algunos matices) en la Administración Biden bajo la denominación de «competición estratégica» (The White House, 2022).

Como cabe esperar, de esta caracterización se desprendería un notable cambio en los temas relativos a la Seguridad Nacional en agenda, ocupando la rivalidad entre actores estatales, aparentemente finiquitada con la desaparición de la Unión Soviética y la creencia en los Estados Unidos como «superpotencia solitaria» (Huntington, 1999), como fuente principal de la conflictividad en un sistema internacional cada vez más desglobalizado (Tovar, 2019).

La invasión rusa de Ucrania ha servido como coyuntura propicia para que la narrativa en torno a la competición entre grandes potencias o la competición estratégica haya trascendido las fronteras de los Estados Unidos, permeando las aproximaciones particulares que otros actores hacen a los actuales desafíos a la seguridad internacional. Buena muestra de ello es que la elaboración en 2022 de la Brújula Estratégica de la Unión Europea, dirigida a identificar las capacidades necesarias para adquirir un mayor grado de autonomía estratégica como actor global y proveedor de seguridad, haya incorporado esta noción:

> «[...] en esta era de creciente competición estratégica, de amenazas complejas a la seguridad y de ataque directo al orden de seguridad europeo, la seguridad de nuestros ciudadanos está en juego. [...] Después de tres décadas de fuerte interdependencia económica que se suponía rebajaría las tensiones, el regreso a las políticas de poder e incluso a la agresión armada es el cambio más significante en las relaciones internacionales» (European Union External Action, 2022: 14).

Del mismo modo, el concepto estratégico adoptado por la Organización del Tratado del Atlántico Norte (OTAN) en su cumbre de Madrid, celebrada en 2022, incluiría también una referencia directa a este concepto: «Nuestro mundo es disputado e impredecible [...] La inestabilidad persistente, la ascendente competición estratégica y el creciente autoritarismo desafían los intereses y valores de la Alianza» (NATO, 2023: 1).

Teniendo en cuenta lo anterior, no resulta extraño que, además, de la propia comunidad de inteligencia estadounidense, un creciente número de servicios de inteligencia de diferentes países hayan pasado a considerar también a las actividades de otros estados como principal desafío a su Seguridad Nacional, desplazando en esa posición al terrorismo internacional, como son los casos de Australia (Australian Security Intelligence Organisation, 2024), Noruega (Norwegian Intelligence Service, 2024), Estonia (Estonian Foreign Intelligence Service, 2024), Suecia (Swedish Security Service, 2024), Canadá (Canadian Security Intelligence Service, 2023), Dinamarca (Danish Defence Intelligence Service, 2023), Nueva Zelanda (New Zeland Intelligence and Security Service, 2022) entre otros. En lo que se refiere a España, tanto el Departamento de Seguridad Nacional (2023) como el Centro Conjunto de Desarrollo de Conceptos (2022) del Estado Mayor de la Defensa han señalado la relevancia adquirida por esta competitividad estratégica.

Como cabe esperar, este giro conceptual no es únicamente denominativo, sino que tiene notables implicaciones en cómo se conciben los conflictos que están por venir y en las capacidades necesarias para hacerles frente. Por ello, el abandono de la asimetría como fisionomía de los conflictos armados propia de la Guerra Global Contra el Terrorismo conduciría a la necesidad palmaria de adaptar las grandes maquinarias burocráticas relativas a la Seguridad Nacional (y entre ellas, la propia actividad estatal de inteligencia) a un nuevo entorno estratégico con un balance de fuerzas en el que los conflictos entre actores con capacidades próximas a la paridad (*near-peer competition*) pasaban a ser predominantes.

Esta competición sería persistente y polifacética, contemplando diversas acciones de diferente grado de intensidad en el continuo del conflicto sin necesariamente desencadenar un enfrentamiento armado (Joint Chief of Staff, 2019; Joint Chief of Staff, 2023), por lo que según Mazarr, Frederick y Crane (2022) se dirimiría en torno a cinco ejes fundamentales: la capacidad productiva total, la habilidad para dominar tecnologías de vanguardia, la movilización discrecional de recursos, la calidad de las instituciones nacionales, y las capacidades militares.

En consecuencia, aun cuando convergen en el panorama internacional actores no estatales que representan una amenaza para la seguridad internacional, así como diversos actores estatales que actúan como fuente de

inestabilidad local y/o regional, la condición de competidor estratégico se encuentra reservada para actores con capacidades próximas a la paridad o pares competidores respecto a los Estados Unidos que cuentan con la voluntad y la capacidad de antagonizar de manera sostenida y a escala global sin que exista un resultado previsible del conflicto (Szayna et *al*, 2001), actuando sus interacciones como clave de bóveda de múltiples y estratificadas dinámicas de competición para conformar «un mosaico complejo de competición global» (Mazarr et *al*, 2018: 33).

Llegados a este punto, una vez abordado el desarrollo histórico reciente del concepto de «competición estratégica» y cómo se ha expresado su socialización en el entorno de países aliados de los Estados Unidos, cabe preguntarse en qué medida la idea de la competición entre grandes potencias es correspondida por lo que son hoy considerados principales antagonistas globales de los Estados Unidos.

Especialmente tras la celebración del 18 Congreso Nacional del Partido Comunista Chino y la elección de Xi Jinping como secretario general, la RPC ha dado muestra de un creciente antagonismo a través de su política exterior, que deja atrás la concepción de bajo perfil propuesta en la década de los ochenta por el presidente Deng Xiaoping. China mantiene hoy lo que se ha denominado «Diplomacia de gran potencia con características chinas» (Wang Yi, 2022), reivindicando unas aspiraciones globales cuya realización está determinada por la capacidad del país por desenvolverse no solo en las dinámicas de la cooperación, sino también en las de la competición y la confrontación, pues, en palabras de Wang Yi (2023):

> «[...] el desarrollo del país ha entrado en un periodo en el que coexisten oportunidades estratégicas, riesgos y desafíos, y en el que aumentan los factores inciertos e impredecibles. Ante serios desafíos, debemos mantener el enfoque estratégico, avanzar a pesar de las dificultades, enfrentar las dificultades, atrevernos a luchar y ser buenos luchando».

De este modo, aunque el concepto de «lucha» cuenta en China con una larga tradición retórica que alude a esta noción para muy diferentes propósitos (algunos de los cuales no se refieren al uso de la fuerza (Kim y Prytherch, 2023)), resulta innegable que esta noción ha adquirido una innegable preeminencia en discurso oficial de las autoridades de la RPC, incluyendo las alocuciones del presidente Xi Jinping (Agencia de Noticias Xinhua, 2019). De este modo, tal y como queda recogido en las obras de síntesis del pensamiento del presidente chino:

> «*Todos los riesgos y desafíos que pongan en peligro la dirección del Partido Comunista de China y nuestro sistema socialista, todos* los riesgos y desafíos que pongan en peligro nuestra soberanía, seguridad e intereses de desarrollo [...] cuando se presenten, debemos combatirlos resueltamente, sin vacilar

> ni acobardarnos, y tener la audacia suficiente para golpear y vencer» (Jinping, 2023: 286).

En lo que a Rusia respecta, aunque existen voces que han puesto en entredicho su condición de competidor estratégico de los Estados Unidos (Dobbins, Shatz, y Wyne, 2018; Mankoff, 2021), no cabe duda de que la persistencia de ciertas inercias derivadas de la Guerra Fría y las aspiraciones mantenidas por el presidente Putin han facilitado que esta sea percibida como una superpotencia. No en vano, según Morales (2018), el presidente Putin se considera a sí mismo un *derzhavnik* (partidario de la idea de Rusia como gran potencia) que tiene como fundamento de su política exterior la conocida como «Doctrina Primakov», que rechaza la idea de un orden unipolar bajo la supremacía estadounidense. En esa dirección, la publicación en 2023 de un nuevo Concepto de Política Exterior contendría una interpelación directa a los Estados Unidos aludiendo formalmente a su corresponsabilidad global:

> «La Federación de Rusia está interesada en mantener la paridad estratégica, la coexistencia pacífica con los Estados Unidos y el establecimiento de un equilibrio de intereses entre Rusia y los Estados Unidos, teniendo en cuenta su condición de grandes potencias nucleares y su especial responsabilidad por la estabilidad estratégica y el estado de la seguridad internacional en general» (The Ministry of Foreign Affairs of the Russian Federation, 2023).

2 Una función de inteligencia para la competición estratégica

Aunque es sabido que las organizaciones terroristas que fueron perseguidas durante la GWOT contaban con sus propias capacidades para la producción de inteligencia que apoyase sus actividades, resulta difícilmente cuestionable que de la competición estratégica se desprenden importantes implicaciones para las instituciones estatales dedicadas a esta actividad. Los sucesos acaecidos el 11 de septiembre de 2001 y la consiguiente priorización de los esfuerzos dirigidos contra el terrorismo internacional conducirían a la adopción generalizada de soluciones organizacionales, en materia de inteligencia, que tendrían un enfoque eminentemente táctico, ya fuese en teatros de operaciones protagonizados por las actividades de contrainsurgencia (Operación Enduring Freedom, Operación Iraki Freedom, etc.) como en escenarios en los que predominaría la persecución de individuos y organizaciones mediante acciones policiales, configurándose como «información sensible al tiempo y específica al detalle usada para identificar, localizar y detener o erradicar terroristas» (Kenney, 2003: 200).

Aunque no es este lugar para evaluar los resultados de este enfoque en el trascurso de la GWOT, propósito que trasciende, por mucho, el alcance de este artículo, cabe preguntarse si esta concepción particular de lo que la inteligencia es y para lo que la inteligencia sirve se ajusta hoy a

las necesidades de quienes toman decisiones en un entorno estratégico como el descrito en las páginas anteriores. Ante este interrogante, en un contexto en el que los antagonismos entre actores con capacidades próximas a la paridad pasan a articularse como los desafíos principales, según Bury y Chertoff (2020), la predominancia de esta inteligencia táctica de orientación contraterrorista daría paso a la revalorización de la inteligencia estratégica y la adaptación de sus prácticas asociadas a las exigencias del entorno, incluso ante la persistencia del terrorismo como amenaza a la seguridad internacional.

Como se mencionaba anteriormente, las acciones concretas enmarcadas en competición estratégica entre potencias se desenvuelven de manera polifacética con diferentes grados de intensidad a través del continuo del conflicto, en cuyos extremos se encuentran las relaciones pacíficas de cooperación, por un lado, y el enfrentamiento armado abierto, por el otro. Esta concepción de las dinámicas de competición entre actores estatales implica reconocer la existencia de interacciones que no pueden considerarse plenamente pacíficas, como tampoco de confrontación explícita, lo que ha venido a denominarse como la zona gris, en la que, tal y como señala Jordán (2018), se encuadran acciones ambiguas y multidimensionales a las que se recurre de manera gradual y combinada para la consecución de intereses en juego, y entre las que se encuentran las acciones agresivas de inteligencia, entre otras estrategias (tales como operaciones de influencia, coerción económica, los conflictos por delegación, etc.).

Todo lo anterior, con el propósito de incapacitar a otros actores antagonistas a la hora de atribuir responsabilidades sobre una acción determinada y evitar así, mediante la denegación plausible, una escalada que pudiera culminar con un conflicto abierto entre las partes, al tiempo que se persiste en la persecución de los intereses propios. Así, como ha señalado Cook (2023), esta nueva normalidad supone un desafío mayúsculo para las organizaciones dedicadas a la producción de inteligencia, que deberán adaptar sus procedimientos a un entorno caracterizado por la ambigüedad.

Debido a la naturaleza consustancial que tuvieron respecto a las lógicas de la bipolaridad imperantes durante la Guerra Fría, siendo estrictos se puede afirmar que el tipo de acciones que quedan abarcadas por lo que hoy se conoce como zona gris no representan una novedad, pues son sobradamente conocidas las «medidas activas» llevadas a cabo por la inteligencia soviética en el transcurso de esta pugna (Kalugin, 2009; Rid, 2020), como también lo son las numerosas operaciones encubiertas realizadas por los Estados Unidos (Best, 1996). No obstante, conceptos como estos no desaparecerían una vez finiquitada la pugna entre ambas superpotencias ante la emergencia de una gran potencia como la RPC, que por su parte promovería las acciones encuadradas en las «tres guerras» o de «guerra irrestricta»,

incluyendo como forma transmilitar de conflicto la guerra de inteligencia (*Intelligence Warfare*).

No es esta una cuestión menor, pues si hoy China es considerada como una gran potencia con aspiraciones globales que rivaliza con el hegemón estadounidense es debido a un «ascenso pacífico», facilitado por la inteligencia como función de Estado que adquiriría una creciente relevancia a partir de la década de los ochenta, cuando la creación del Ministerio de Seguridad del Estado (MSS, en inglés) permitiría dar al país un salto cualitativo sin precedentes en materia de inteligencia exterior y contrainteligencia (Guo, 2012).

Así, de acuerdo con los reportes parlamentarios presentados por la comunidad de inteligencia de los Estados Unidos a finales de la década de los noventa, además de los asuntos relativos a su seguridad interior y la monitorización de la «cuestión taiwanesa», los servicios de inteligencia chinos tendrían como prioridad la recolección de información económica y tecnológica para favorecer su desarrollo nacional, ya fuera de fuentes abiertas o sometida a secreto comercial o a clasificación gubernamental (Central Intelligence Agency and Federal Bureau of Investigation, 1999). A tenor de lo anterior, no resulta exagerado afirmar que la modernización del Ejército Popular de Liberación durante las últimas décadas habría sido difícilmente posible sin la adquisición de tecnología militar o de doble uso extranjera por medios tanto lícitos (información de fuentes abiertas, adquisición mediante proveedores legítimos, etc.) como ilícitos (infiltrados, empresas fachada, adquisición a través de grupos del crimen organizado, etc.) (Dallas, Lewis y Pollack, 2010).

En sus intentos por entender el funcionamiento de una inteligencia china cada vez más activa, a finales de la década de los ochenta se impondría la idea de que esta guiaba sus operaciones de recolección de información a través de lo que en occidente se denominó mediáticamente «Estrategia de los mil granos de arena» (Overend, 1988; Moore, 1996)[1], concepto ideado por los analistas de la Oficina Federal de Investigación (FBI, en inglés) para referirse a la particular forma de proceder que esta seguía en sus operaciones de recolección de información. A diferencia de la inteligencia soviética y de la estadounidense, que recurrían habitualmente a la práctica

[1] Dicho concepto proviene de una metáfora empleada por un oficial del FBI, sin identificar, para explicar el funcionamiento de las actividades de recolección de información de la inteligencia china, que se cita a continuación de su fuente original: «Si los granos de arena fueran objetivos de inteligencia, los soviéticos sacarían a la superficie un submarino en la oscuridad de la noche y enviarían un pequeño grupo a la playa para traer de vuelta varios cubos de arena. Los chinos enviarían 1000 bañistas a la playa a plena luz del día y cada bañista traería un grano de arena». La popularización de esta analogía llevaría a que aparecieran diferentes versiones posteriores, siendo con frecuencia atribuida a Moore, quien la publicaría en un artículo bajo su autoría algunos años más tarde.

del espionaje para tener acceso a información de alto valor, según Moore (1999), la inteligencia china hacía uso de los miembros de la diáspora china (turistas, estudiantes, empresarios, etc.) para que actuasen en el exterior como operadores que recolectaban conjuntamente grandes volúmenes de información de diferente índole, así como a ciudadanos estadounidenses que visitaban China con fines académicos siendo objeto de acciones de elicitación para favorecer su indiscreción y dar acceso de manera bienintencionada a información sensible; sin existir una vinculación entre estos colaboradores informales y los servicios de inteligencia chinos ni ninguna contraprestación monetaria (Loeb y Pincus, 1999).

Moore (1996: 378)[2] definiría este método de recolección de información basado en el concepto chino de Guanxi (que se refiere al ejercicio de la influencia a través de la interacción social) como «inteligencia actuarial», cuya utilidad reside en la agregación de esfuerzos de una gran masa de recolectores de pequeñas piezas de información, dificultando al mismo tiempo la persecución judicial de estas actividades al no constituir los casos individuales casos de la entidad suficiente como para justificar un procesamiento por espionaje de los implicados.

Esta característica aproximación a las operaciones de recolección de información por parte de la inteligencia exterior china parece haber pervivido con el tiempo. Para dar fundamento jurídico a estas prácticas sería aprobada, en 2017, la Ley de Inteligencia Nacional, disposición actualmente en vigor, y por la que se establece la obligada colaboración de todo ciudadano y organización con los esfuerzos nacionales de inteligencia (artículo 7), incluso a posible petición por parte de los organismos nacionales de inteligencia (artículo 14), tanto en territorio chino como en el extranjero (artículo 10). Sin embargo, resulta necesario señalar que esta concepción de las prácticas empleadas por los servicios de inteligencia chinos no ha estado exenta de controversia. Entre las críticas a la noción de la «Estrategia

[2] Moore se refiere aquí a la actuaría como disciplina dedicada a la gestión de riesgos mediante la estadística a la que la industria aseguradora recurre para estimar el margen de rentabilidad de sus actividades a partir del análisis de grandes volúmenes de datos sobre sus asegurados:

> «Si grandes cantidades de personas se unen a la actividad de inteligencia, algunos serán habilidosos, enérgicos, o solo meros recolectores afortunados. También es posible alcanzar un gran agregado de recolección tomando piezas extremadamente pequeñas. Cuando un número extremadamente grande de personas se ven involucradas, sin embargo, se vuelve difícil predecir el comportamiento de un solo individuo. A cierto punto, parece que el peso de los números asume el control y el problema pasa a ser principalmente estadístico».

En ese sentido, no resulta exagerado afirmar que se trataría de un precedente remoto de lo que hoy se conoce como *crowdsourcing intelligence*.

de los mil granos de arena» destaca la posición planteada por Mattis (2011, 2012), quien afirma que esta aproximación tradicional, basada en las presunciones básicas de que la inteligencia china se centra en la utilización de chinos étnicos como fuentes, en el protagonismo de recolectores aficionados sobre oficiales de inteligencia, en la particularidad distintiva de los procedimientos empleados por China respecto a los de servicios de inteligencia occidentales, y en la preferencia por grandes volúmenes de información escasamente protegida que es efectivamente integrada, tiene notables implicaciones negativas para entender el funcionamiento de estas instituciones (Mattis, 2011)[3]. Esta misma posición es compartida por otros autores, como Hannas, Mulvenon y Puglisi (2013: 348), para quienes «por demasiado tiempo, la literatura sobre las operaciones de inteligencia chinas se ha basado en un conjunto de proverbios y palabrería desactualizados».

Aunque no es lugar este para profundizar en esta controversia, la evidencia disponible parece indicar que los servicios de inteligencia chinos no revisten tan fuertes particularidades en sus operaciones de recolección de información y que sus prácticas resultan equiparables a las empleadas por otras comunidades de inteligencia, con la capacidad de realizar operaciones cuyo alcance no es propio de meros aficionados.

Tal y como señala el informe presentado ante el Parlamento Británico por su Comité de Inteligencia y Seguridad (ISC, en inglés), se ha podido comprobar que la inteligencia china cuenta con la capacidad de explotar fuentes humanas, tanto en términos tradicionales como haciendo uso de las redes sociales, pero destaca la capacidad altamente efectiva de realizar operaciones en el ciberespacio, cosechando un considerable nivel de éxito en la penetración de gobiernos extranjeros y compañías tecnológicas, ya sea a través de instituciones oficiales o de actores informalmente vinculados a la RPC, tales como los denominados *hackers* patrióticos y cibercriminales (Intelligence and Security Committee of Parliament, 2023).

Uno de los ejemplos más claros de estas capacidades reside en la brecha de seguridad de la Oficina de Gestión de Personal (OPM), institución responsable de la gestión de recursos humanos del gobierno federal, revelada a la opinión pública en junio de 2015. De acuerdo con los documentos publicados por los órganos parlamentarios estadounidenses, en relación con este episodio, las dimensiones de los datos comprometidos

[3] Mattis señala particularmente cuatro: la subvaloración del grado de amenaza representado por los servicios de inteligencia chinos, al ser considerados como dependientes de recolectores aficionados; la indiferenciación entre los diferentes actores que pueden verse involucrados en actos de espionaje económico, al considerar todos estos actos como resultado de operaciones de los servicios de inteligencia chinos, y el énfasis en el riesgo representado por individuos particulares más que en los propios servicios de inteligencia chinos.

serían masivos, al afectar a los registros personales de 4,2 millones de empleados y exempleados del Gobierno Federal de los Estados Unidos, así como la documentación referida a las solicitudes de habilitación de seguridad (formularios SF-86, investigaciones de antecedentes), realizadas por 21,5 millones de personas, de los cuales se verían comprometidos los datos dactiloscópicos de 5,6, lo que llevaría a afirmar que estas filtraciones «dañarían los esfuerzos de contrainteligencia de al menos una generación que está por venir» (Committee on Oversight and Government Reform, 2017: V).

Tal y como apunta Dorfman (2020a; 2020b), los servicios de inteligencia chinos habrían adquirido por esta vía un conocimiento inédito respecto a la comunidad de inteligencia estadounidense y sus integrantes, adquiriendo muy abundante información personal sensible de funcionarios y contratistas con puestos relevantes en el aparato de Seguridad Nacional que no solo podría ser potencialmente utilizada como medio de coerción, sino que también podría ser empleada a fin de exponer a personal operativo estadounidense en terceros países y a desmantelar las redes de activos de la CIA en China. Sea como fuere, la casuística reciente apunta a que China sería responsable de un creciente número de acciones de ciberespionaje contra instituciones gubernamentales y otras entidades críticas de diferentes países, tanto en su vecindario regional más próximo (Recorded Future, 2021; Microsoft, 2023) como a escala global, como muestran las informaciones reveladas por la supuesta filtración de información de I-Soon, compañía contratista de diferentes instituciones estatales de la RPC (incluyendo el MSS, el Ministerio de Seguridad Pública (MPS, en inglés) y el Ejército Popular de Liberación (PLA, en inglés)) que habría comprometido la seguridad de los sistemas informáticos de agencias gubernamentales de todo el mundo desde 2013 (Robinson, 2024), además de otras APT atribuidas a los servicios de inteligencia chinos (National Cyber Security Centrum, 2024).

Si el conflicto en el actual entorno estratégico está protagonizado por Entidades de Inteligencia Extranjera (FIE, en inglés) con capacidad suficiente como para realizar con éxito un número considerable de operaciones de obtención de información de alto nivel de sofisticación, todo parece indicar que la contrainteligencia pasa a cobrar un valor sustancialmente mayor en términos de Seguridad Nacional al asumido durante las últimas tres décadas. Sin embargo, cabe preguntarse si, ante una amenaza como la aquí descrita, la concepción tradicional de contrainteligencia que ha imperado en los Estados Unidos y sus actividades típicamente asociadas son instrumentos suficientes. A este respecto, es necesario señalar que durante el pasado reciente el desempeño de la contrainteligencia estadounidense ha sido oficial y públicamente puesto en entredicho en varias ocasiones: tal y como se reconocía en el informe realizado sobre la situación de la

comunidad de inteligencia estadounidense tras el fallo de inteligencia que conduciría a la Operación Iraki Freedom en 2003, los esfuerzos de contrainteligencia de los Estados Unidos «siguen siendo fracturados, miopes y solo marginalmente eficaces» (The Commision on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005: 486), llamando a adoptar un cambio estructural para hacer frente a las acciones de creciente agresividad y sofisticación de las que estarían siendo objeto los Estados Unidos.

Pese a esta explícita caracterización, y a las medidas adoptadas durante las dos últimas décadas en materia de contrainteligencia[4], de manera más reciente se ha insistido en la obsolescencia relativa de las entidades adscritas a este negociado, afirmando de manera directa que «el sistema de contrainteligencia de EE. UU. no está posicionado para enfrentar el panorama de amenazas FIE para la sociedad en su conjunto que hoy enfrenta el país» (Select Committee on Intelligence, 2022: 129).

Olson, director de contrainteligencia de la CIA, a comienzos de la década de los noventa explica esta disfuncionalidad a partir de diferentes causas:

> «Me gustaría poder declarar que el NCIX estuvo a la altura de las grandes esperanzas que la comunidad de contrainteligencia tenía para él en su inicio. Ha tenido un buen liderazgo y ha hecho muchas cosas positivas, pero ha sufrido los cambios en las prioridades de seguridad nacional, los recortes en la financiación y la reducción del personal» (Olson, 2021, 75).

A este respecto, a los factores anteriormente mencionados Olson añadiría que la conjunción de las funciones de seguridad y contrainteligencia producida en 2014 habría supuesto una priorización de la primera sobre la segunda. Esta superposición funcional también es referida por Van Cleave (2007a: 13), quien ocupó la responsabilidad de NCIX entre 2003 y 2006, cuando incide en la desviación en la que habría incurrido la contrainteligencia estadounidense, «optimizada para una posición defensiva de trabajar

[4] Uno de los últimos actos de Bill Clinton como presidente de los Estados Unidos sería mandatar la reorganización del sistema de contrainteligencia estadounidense mediante la Directiva de Decisión Presidencial (PDD, en inglés) 75, estableciendo diferentes organismos para tal propósito, como la Junta Directiva de Contrainteligencia Nacional (NCIPB, en inglés), liderada por el Ejecutivo Nacional de Contrainteligencia (NCIX, en inglés), contando con su oficina adjunta (ONCIX, en inglés) para la elaboración de la Estrategia Nacional de Contrainteligencia.
Con la creación en 2004 de la Oficina del Director de Inteligencia Nacional (ODNI, en inglés), el ONCIX, en inglés pasaría a integrarse en su seno para la coordinación de las actividades de contrainteligencia en el seno de la Comunidad de Inteligencia Estadounidense. Diez años más tarde, en el marco de la fusión del ONCIX con el Centro de Evaluación de Seguridad (CSE, en inglés), el Centro Especial de Seguridad (SSC, en inglés) y el Grupo de Trabajo Nacional sobre Amenazas Internas (NITTF, en inglés), la entidad pasaría a ser denominada Centro Nacional de Contrainteligencia y Seguridad (NCSC, en inglés).

casos individuales en casa, más que trabajar en los servicios de inteligencia extranjeros como objetivos estratégicos», con énfasis en las investigaciones de contrainteligencia para la judicialización de personas involucradas en actos de espionaje o la expulsión de diplomáticos implicados este tipo de actividades (Van Clave, 2007b).

Ante dicha situación, esta misma autora ha reivindicado el establecimiento de un programa de contrainteligencia estratégica, entendida esta como «la dirección e integración de las actividades de contrainteligencia para comprometer o alterar la capacidad de los servicios de inteligencia extranjeros de dañar los intereses de Seguridad Nacional de los EE. UU. en el país o a nivel mundial» (Van Cleave, 2022: 13); aproximación que necesariamente implica la adopción de un enfoque ofensivo (dirigido a identificar, evaluar, neutralizar y explotar las capacidades de los actores antagonistas) y coordinado a escala nacional (trascendiendo los márgenes organizacionales de los departamentos de contrainteligencia de cada institución y las rivalidades existentes entre ellos) que eventualmente permita dar una respuesta estratégica coherente ante los competidores estratégicos de los Estados Unidos.

Llegados a este punto, cabe preguntarse acerca de las capacidades de entidades dedicadas a la contrainteligencia en China a la hora de neutralizar las operaciones de recolección de información por parte de servicios de inteligencia extranjeros. Indudablemente, la eficacia de eventuales acciones de este tipo que requieran de personal en territorio chino está fuertemente condicionada por las capacidades tecnológicas a disposición de la RPC, y más particularmente, de sus instituciones estatales dedicadas a las actividades de contrainteligencia, que, de manera pública, han confirmado intensificar sus esfuerzos de contraespionaje ante la actividad de los servicios de inteligencia estadounidenses (Ministry of State Security, 2024).

De acuerdo con las estimaciones realizadas por Bischoff (2023), China se posiciona como el país más videovigilado del mundo, tanto por el número total de cámaras de CCTV instaladas (626 millones, con Shanghái como ciudad con mayor número de cámaras, con 12 825 589 totales) como por el número de cámaras por milla cuadrada (con Shenzen como la ciudad más densamente videovigilada, con 7462,89 cámaras por milla cuadrada), haciendo que las veinte ciudades más videovigiladas del mundo sean chinas. Asimismo, el país asiático es una reconocida potencia en materia de Tecnología de Reconocimiento Facial, que ha implementado a gran escala en diferentes ámbitos de la vida cotidiana de la sociedad china (Bischoff, 2022) con la potencial utilización como medio de detección de los comportamientos considerados incívicos, sino también de seguimiento de los movimientos de personas sitas en territorio chino. A estas capacidades tecnológicas de vigilancia, es necesario añadir que China cuenta, desde 2014,

con una ley de contraespionaje, que, en su reforma de 2023, plantea una definición expansiva de lo que se considera como «actos de espionaje»[5], y otorga, además, a los órganos de Seguridad Nacional chinos, mediante provisión suplementaria, la capacidad de prevenir, detener y sancionar actos que pongan en peligro la Seguridad Nacional distintos del espionaje.

De manera coincidente con la revisión de dicha ley, el MSS crearía su cuenta oficial en WeChat (aplicación multipropósito que incluye servicios de mensajería, redes sociales o pagos virtuales, entre otros), declarando en su primera publicación que «el trabajo de contraespionaje requiere de la movilización de todas las partes de la sociedad, lo cual también combina el "trabajo abierto" y el "trabajo secreto", así como el "trabajo especializado" con "el trabajo público de masas"» (Quingquing, 2023). Por si lo anterior no fuera suficiente, hay que añadir que la comunidad de inteligencia china ha dado muestras de una concepción ofensiva de la contrainteligencia incluso fuera de su propia jurisdicción, tal y como lo demuestra el establecimiento de comisarías de policía exteriores chinas adscritas al MPS, mediante las que vendrían ejerciendo medidas coactivas contra integrantes de la oposición en la diáspora (Ramírez, 2024).

Por todo lo anterior, el territorio chino parece presentarse como un entorno particularmente hostil para las actividades de cualquier servicio de inteligencia extranjero. Debido al alto riesgo de detección que asumiría su personal, capacidades de contrainteligencia como las aquí señaladas hacen difícilmente replicables algunas de las prácticas asociadas al espionaje tradicional, de manera particular aquellas dirigidas a la obtención de información de manera encubierta. Al fin y al cabo, tal y como señala Prunckun (2019), uno de los motivos que conduciría al empleo intensivo durante la Guerra Fría de medios de recolección de información basados en tecnología (particularmente, la obtención de imágenes aéreas y satelitales) radicaría en el comparativamente alto costo de mantener operadores y fuentes humanas sobre el terreno; preferencia que se vería relativamente alterada a favor del agente encubierto con el inicio de la GWOT, protagonizada por actores no estatales más vagamente definidos.

Sea como fuere, al mismo tiempo que de la innovación tecnológica derivan notables desafíos para la obtención de información encubierta, por

[5] De acuerdo con el artículo 4 del citado texto legal, los actos de espionaje comprenden: la realización, instigación y financiamiento de actividades que amenacen la Seguridad Nacional, tanto dentro como fuera del territorio nacional; la participación en una organización dedicada al espionaje, la aceptación de tareas o la pretensión de alinearse con ella; las actividades dirigidas a la obtención de secretos de Estado, inteligencia y otros elementos relacionados con la Seguridad Nacional o el interés nacional; las acciones de diferente tipo contra la integridad de redes y sistemas de instituciones estatales e infraestructuras; la identificación de objetivos, y la conducción de otras actividades de espionaje.

medio de agentes ante la implantación masiva de tecnologías de vigilancia, también ofrece potenciales oportunidades que podrían suponer una ampliación del empleo de la inteligencia de fuentes humanas, tanto en su captación como en su manejo (Gioe, 2017; Cunnliffe, 2023). Buena muestra de ello son las acciones realizadas por la CIA con la intención de reclutar fuentes de manera virtual, primero mediante la creación de una página propia en la Red Tor (Central Intelligence Agency, 2019) y, más recientemente, con un canal de Telegram específicamente dedicado a establecer contacto con ciudadanos rusos (Central Intelligence Agency, 2023); o la utilización, por supuestos ciudadanos chinos, de perfiles falsos de la red social profesional LinkedIn con la finalidad de contactar a funcionarios extranjeros para incitarles a revelar información sensible a cambio de una contraprestación económica (Wong, 2019).

Aunque el papel de la inteligencia militar ante la competición estratégica no se circunscribe a los escenarios de guerra convencional, ya que sus capacidades distintivas ofrecen abundantes prestaciones también ante las acciones en la zona gris, su relevancia resulta evidente cuando se hace referencia a la posibilidad de una guerra interestatal. Si bien de la competición estratégica se desprende una pugna entre actores que persiguen intereses incompatibles sin necesidad de desencadenar un enfrentamiento armado entre ellos, la posibilidad de una guerra de alta intensidad no puede ser descartada como resultado de la agudización de las dinámicas de competición entre Estados. El desencadenamiento de una guerra abierta como resultado de la zona gris es un escenario evitable, afirma Baques (2021), aunque existe la posibilidad de que esta, más que una alternativa al uso de la fuerza convencional, constituya una serie de acciones con una finalidad preparatoria de un conflicto armado convencional. Esta posibilidad queda ejemplificada por la denominada Operación Militar Especial, iniciada el 24 de febrero de 2022, preludiada por toda una serie de acciones coactivas propias de la zona gris, iniciadas sobre Ucrania en marzo de 2014 y con un desenlace cuyas razones son todavía hoy desconocidas (Colom-Piella, 2023).

Precisamente ante la posibilidad de que las acciones en la zona gris deriven en una guerra con sus competidores, los Estados Unidos procederían, años atrás, a impulsar diferentes esfuerzos dirigidos a la modernización de su fuerza, que en el caso particular del Ejército de los Estados Unidos conducirían a acuñar las Operaciones Multi-Dominio como nuevo concepto operativo que, además de plantear las dinámicas propias de la competición con Rusia y China, anticipa los escenarios de combate a gran escala en los que los EE. UU. no gozarían de superioridad en todos los dominios de la guerra y en los que sus actores antagonistas podrían coartar su libertad de acción y las de las fuerzas aliadas en el teatro de

operaciones haciendo uso de sistemas Anti-Acceso y de Denegación de Área (A2/AD) (Pulido, 2022).

De un cambio doctrinal de esta naturaleza se desprende un nuevo planteamiento de las capacidades de inteligencia militar, de la misma forma que los conflictos contrainsurgentes intraestatales que adquirieron un mayor protagonismo tras los atentados del 11 de septiembre de 2001 supusieron una reconsideración de la inteligencia como función de combate para adaptar su desempeño a la fisonomía particular de los conflictos asimétricos. Es pertinente recordar las advertencias realizadas por Flynn, Pottinger y Batchelor (2010) al calor de la experiencia estadounidense en Afganistán, incidiendo en la diferente naturaleza de la inteligencia requerida para los esfuerzos contrainsurgentes frente a la que resulta de utilidad para el desarrollo de una guerra convencional, tanto en lo que se refiere a los medios de recolección de información empleados para una y otra (concediendo un papel destacado a los medios tecnológicos en esta última) (Flynn, Pottinger y Batchelor, 2010: 12)[6] como en la predominancia en esta primera de la inteligencia táctica (de naturaleza local) sobre la estratégica (de alcance nacional) (Flynn, Pottinger y Batchelor, 2010: 11)[7]. En esta dirección, Hoehn (2020) señala que la transformación realizada sobre los procedimientos asociados a la inteligencia militar, que pasaba entonces a operar en entornos de una relativa permisividad y con superioridad en todos los dominios, no se ajustaría a las exigencias de un teatro de operaciones altamente disputado como los que se pueden anticipar a consecuencia de la paridad de capacidades entre los actores:

> «[…] el objetivo principal compartido por los jefes de los servicios de inteligencia es pasar de una fuerza para entornos permisivos e intensiva en recursos humanos a una fuerza para entornos de alto nivel de amenaza e intensiva en automatización que es efectiva en costes, que puede identificar de manera confiable objetivos elusivos, y que puede permitir que una fuerza militar interoperable de los EE. UU. para obtener y mantener la ventaja de la información» (Hoehn, 2020: 14).

---

[6] «En un conflicto convencional, las unidades de tierra dependen fuertemente de la inteligencia de los mandos superiores para ayudarles a navegar la niebla de la guerra. Satélites, aviones espía y más activos arcanos controlados por personas que están lejos del campo de batalla informan a las unidades de tierra sobre la fuerza, la localización, y la actividad del enemigo incluso antes de que la unidad de tierra llegue. La información fluye mayoritariamente de arriba abajo […] En una contrainsurgencia, este flujo es (o debería ser) revertido. El soldado o el trabajador de desarrollo es normalmente la persona mejor informada sobre el entorno y el enemigo. Ascender a través de los niveles de jerarquía es normalmente un viaje hacia mayores grados de ignorancia».

[7] «Una de las particularidades de la guerra de guerrillas es que la información a nivel táctico está cargada de importancia estratégica mucho más que en los conflictos convencionales».

En línea con esta nueva concepción de las operaciones militares contra competidores con capacidades próximas a la paridad, el Ejército de los Estados Unidos establecería la adaptación de sus capacidades de inteligencia para estar inicialmente operativas en 2028 y de manera plena para 2035, determinando las acciones específicas a acometer por la inteligencia para prestar apoyo a la fuerza en los escenarios de competición, conflicto armado y regreso a la competición (TRADOC, 2020).

Tal y como señala Gómez (2021), la adaptación de la inteligencia militar, y, más particularmente, de la Inteligencia, Vigilancia y Reconocimiento Conjuntos (JISR, en inglés), a los postulados de las operaciones multidominio representa en sí mismo un complejo reto. En consecuencia, aun cuando hoy se confía en la superioridad estadounidense en esta materia frente a las capacidades de sus más notables competidores, «sin una continua recalibración de los activos que componen la actividad de ISR y los datos que recolectan, los Estados Unidos se arriesga a perder su ventaja estratégica» (Harrington y McCabe, 2021). Esta preocupación se explica a partir del proceso de modernización del PLA en este ámbito, en lo que se refiere a inteligencia de señales, sistemas de radar, sistemas de Alerta Temprana y Control Aerotransportado, vehículos aéreos no tripulados, sensores de guerra antisubmarina, entre otras capacidades (McCabe, 2021).

Al mismo tiempo, tal y como señala Haver (2023), también se habría producido una intensificación y diversificación del empleo de inteligencia de fuentes abiertas por parte del PLA, facilitando insumos a nivel estratégico (tendencias políticas, factores económicos y sociales, etc.), a nivel operacional (intenciones de otras fuerzas militares, su coordinación, organización y mando, etc.) y a nivel táctico (información relativa al despliegues, sistemas de armas y equipamiento, etc.). Además, tal y como advierte Watling (2021), aun cuando se goce de superioridad en la recolección de información de todas las fuentes, debido a las condiciones en las que se desarrollaría un conflicto entre actores con capacidades próximas a la paridad, la existencia de un entorno electromagnético disputado puede comprometer la centralización efectiva mediante centros de fusión de la información obtenida y la difusión de inteligencia a las unidades tácticas, dependientes de los insumos facilitados por elementos superiores de la cadena de mando a la hora de contar con una imagen del campo de batalla que les ofrezca un nivel adecuado de conciencia situacional (Gómez, 2023)[8]. Al calor de la experiencia de la invasión rusa de Ucrania,

[8] A este respecto, Gómez señala que este tipo de vulnerabilidades habrían sido recurrentes durante los primeros meses de Operación Militar Especial, a consecuencia de las deficiencias de las redes de comunicación rusas y por la acción de las acciones de guerra electrónica sobre ellas, llevando al empleo de redes de comunicaciones no

incluso la inteligencia de fuentes abiertas parece cobrar una importancia renovada, facilitando mayores capacidades anticipatorias ante el despliegue ruso gracias a las imágenes satelitales de uso comercial y en análisis de redes sociales (Hockenhull, 2022).

3 Inteligencia y poder: actuar concertadamente

A diferencia de otros conceptos propios de otros campos de estudio de las Ciencias Sociales, en los que existe una larga tradición de discusión en torno al poder y de sus diferentes derivaciones, los estudios de inteligencia carecen, en la actualidad, de un estudio profundo y sistemático de lo que este concepto significa y de cómo este se materializa en las particulares actividades que los servicios de inteligencia realizan. En la década de los noventa, Michael Herman acuñaría el concepto de «poder de inteligencia» (*intelligence power*), tomando prestada la definición general de poder realizada por Freedman en el ámbito de los Estudios Estratégicos, consistente «en la capacidad de producir efectos que son más ventajosos de lo que habría sido el caso» (Freedman, 2014: 18), sin dotar de contenido teórico particular su aplicación en el ámbito de los Estudios de Inteligencia. Contribuciones más recientes han tratado de dar respuesta a este requerimiento, como es el caso de Sims (2022), quien considera el poder de inteligencia como la potencialidad de reducción de incertidumbre que permita la adquisición de una ventaja decisoria ante un competidor, lo que estaría determinado por cuatro elementos fundamentales: las capacidades superiores de recolección de información relevante; la autonomía suficiente de los esfuerzos de recolección respecto a la política y las amenazas ya conocidas como para anticipar lo inesperado; la superior transmisión de inteligencia entre sus productores y sus consumidores, y la superior capacidad para ocultar y divulgar información con fines competitivos. Otros autores, adscritos a los denominados Estudios Críticos de Inteligencia, han ofrecido sus aproximaciones alternativas a la noción de poder de inteligencia (Van de Kerke y Hijzen, 2021).

Como se ha podido ver en páginas anteriores, la convergencia entre capacidades de inteligencia y desarrollo tecnológico se ha acelerado durante las últimas décadas, lo que puede generar la tentación de entender el poder de inteligencia como una mera proyección de los medios tecnológicos a disposición de un determinado Estado, especialmente aquellos referidos a la recolección de información. Sin embargo, tal y como advierte Arendt (2006: 60), el ejercicio del poder no radica tanto en el uso de la fuerza o en la sofisticación de los instrumentos empleados para ello, sino

seguras sobre las que la obtención de inteligencia de comunicaciones habría facilitado la identificación de objetivos.

más bien en «la capacidad humana, no simplemente para actuar, sino para actuar concertadamente».

Aunque resulta innegable que hoy la producción de inteligencia se ha tornado una actividad que hace un uso intensivo de la tecnología. El poder nacional en esta materia no puede ser explicado y valorado a partir de un criterio exclusivamente tecnológico. Además de ser una aproximación unilateral al poder de inteligencia ante el que se podrían interponer no pocos inconvenientes, supone una concesión de protagonismo omnímodo a los países más tecnológicamente desarrollados (las grandes potencias) que no contempla la capacidad de agencia de actores que no reúnen tal condición, sumiendo sus intereses autónomos en una condición de subalternidad permanente, lo que admite cierta discusión. A fin de cuentas, el propio Herman reconocería que el poder de inteligencia tiene una dimensión relacional cuando afirmaba que «El poder de la Inteligencia Nacional es una función no solo de las capacidades nacionales sino también de la cooperación extranjera y del producto que obtiene» (Herman, 2004: 217), por lo que, en coherencia con ello, corresponde reconocer que el devenir de la competición estratégica como complejo mosaico de relaciones de competición estará altamente condicionado, además de por la gestión de los antagonismos entre grandes potencias en escenarios como los ya descritos, por el poder relacional de estas a la hora de establecer alianzas con otros Estados.

Buena muestra de lo anterior es la importancia adquirida por otros actores estatales no considerados grandes potencias en entorno estratégico descrito. Aunque es una categoría actualmente subteorizada que abarca países de muy diversas características (Edstrom y Westber, 2020), con frecuencia las potencias intermedias son actores que asumen una posición de ambivalencia relativa entre grandes potencias que les aleja de las narrativas construidas a partir de antagonismos de suma cero entre ellas (Sweijs y Mazarr, 2023). En esa misma dirección, Long (2022) ha señalado que ni siquiera los pequeños Estados están condenados a ser meros actores pasivos en su relación con las grandes potencias, pues pueden aprovechar para beneficio propio y por diferentes vías las relaciones asimétricas que establecen con ellas. Lejos de ser meras reflexiones academicistas, la importancia en el orden internacional de las naciones con un grado de desarrollo económico y tecnológico sustancialmente mejor que del que gozan las grandes potencias no es una novedad para los servicios de inteligencia, que constatarían esta realidad ya durante los años de la Guerra Fría (CIA, 1976). Ello es perfectamente aplicable a las actividades de inteligencia, pues tal y como señala Gioe (2023), las capacidades de los Estados en este ámbito no son siempre proporcionales a su poder militar o tecnológico, por lo que las instituciones dedicadas a la producción de inteligencia de potencias intermedias y pequeñas potencias pueden asumir un papel destacado

no solo en su esfera de influencia regional, sino también en términos globales (Carmichael, 2012)[9].

La necesidad de actuar concertadamente junto a actores estatales de intereses diversos requiere de una reconsideración de las dinámicas y mecanismos de cooperación internacional en diferentes ámbitos, y el de la inteligencia no parece ser una excepción. Si durante el siglo XX y hasta bien entrada la posguerra fría los vínculos entre servicios de inteligencia de diferentes naciones había presentado características relativamente estables, como la predilección por relaciones bilaterales en este ámbito a través de representaciones diplomáticas (Alexander, 1998; Walsh, 2009), el inicio de la GWOT generó la expectativa de que, ante la disolución de la dinámica de bloques, la consumación del proceso de globalización y la transnacionalización de las amenazas a la seguridad internacional, la cooperación en materia de inteligencia adquiriría nuevas formas organizacionales, con un mayor peso de los foros multilaterales (algunos creados durante la Guerra Fría, otros constituidos tras el 11-S) y una colaboración más amplia (Hulnick, 2001; Lefebvre, 2003; Aldrich, 2011; Svendsen, 2011).

¿Qué formas particulares adoptará la colaboración internacional en materia de inteligencia en la era de la competición estratégica? Resulta imposible dar respuesta unívoca y precisa a este interrogante, aunque es posible presumir que, tal y como afirma Whitaker (2024), «incluso cuando una Guerra Fría renovada está siendo proclamada, negociar la compartición de inteligencia en este más complejo mundo multipolar será muy diferente y más desafiante que en el pasado». En ese sentido, tal y como ha reconocido el Secretario de Estado Blinken, de la competición estratégica se desprenden nuevos y sustanciales desafíos para la diplomacia estadounidense en lo que se refiere al establecimiento de alianzas y asociaciones con otras naciones (Blinken, 2023), lo que de manera reciente está suponiendo una reconsideración significativa del papel reservado a la comunidad de inteligencia para este propósito (Blinken, 2022).

Aunque inteligencia y diplomacia han sido tradicionalmente funciones de Estado entre las ha mediado una superposición funcional y una separación institucional, lo que ha conducido a relaciones con frecuencia conflictivas (Herman, 1998; Stempel, 2010), existen notables evidencias de que la comunidad de inteligencia estadounidense se inclina en la actualidad por un nuevo modelo que las integre de manera más efectiva. Así lo demuestra la modificación realizada al Manual de Asuntos Exteriores (FAM, en inglés) del Departamento de Estado de los EE. UU. a comienzos de 2024, mediante la cual se introduciría un nuevo apartado de política en materia de diplomacia

[9] Un ejemplo elocuente de esta desproporción lo representa el caso de Cuba, cuyos servicios de inteligencia han tenido, durante las últimas décadas, un desempeño operativo mayor del que podría esperarse de un pequeño país, incluso ante los Estados Unidos.

de inteligencia, entendida esta como «el uso de inteligencia para apoyar las actividades diplomáticas y la diplomacia pública para promover los objetivos de política exterior de EE. UU. informar a los socios, construir alianzas, facilitar la cooperación, impulsar la convergencia en los enfoques y puntos de vista, y verificar los tratados» (U.S. Department of State, 2024), y que otorga al Centro de Política de Inteligencia e Intercambio de Información de la Oficina de Inteligencia e Investigación (PSC/INR) la gestión en el seno del Departamento de Estado de las acciones revelación de inteligencia para el público general y/o entidades extranjeras en coordinación con otros elementos de la Comunidad de Inteligencia y/o del Departamento de Defensa, lo que ha recibido la denominación de «desclasificación estratégica» (Burns, 2024)[10].

Un procedimiento como el aquí descrito, iniciado a instancias de la Dirección de Inteligencia del Consejo de Seguridad Nacional de los Estados Unidos pero gestionado por la Oficina del Director Nacional de Inteligencia (Calabresi, 2024), encuentra su demostración más reciente y sustancial en los prolegómenos de la invasión rusa de Ucrania, cuando las autoridades estadounidenses revelaron a la opinión pública las intenciones rusas con un doble objetivo: llevar a cabo una acción de comunicación estratégica con fines disuasivos, por un lado; e inhibir el efecto informativo de la narrativa rusa sobre el masivo despliegue de tropas en la frontera con Ucrania, presentado como un acto exclusivamente defensivo incluso pocos días antes del anuncio de la Operación Militar Especial realizado el 24 de febrero de 2022 (Huminski, 2023).

Desde entonces, según la información revelada por el secretario asistente de la INR, Brett M. Holmgren (2023), el creciente número de peticiones de desclasificación tramitadas durante los últimos años (900 en 2021, 1200 en 2022) pondría de manifiesto que la utilidad de este tipo de procedimientos no se circunscribiría a un episodio particular, sino que las autoridades estadounidenses recurrirían a ellos con otros propósitos, como demostrar la transferencia de material de defensa chino a Rusia en el marco de la invasión.

En consecuencia, y aunque esta es una práctica que encuentra no pocas limitaciones y riesgos asociados (Gómez, 2023) todo parece indicar que la inteligencia como función de apoyo a las actividades diplomáticas de los

[10] De acuerdo con el citado FAM, la diplomacia de inteligencia estaría regida por siete principios fundamentales: el alineamiento con objetivos políticos; la integración con otros elementos de poder nacional; la priorización del fortalecimiento de alianzas y asociaciones como fines; la utilización de inteligencia creíble y proveniente de diferentes fuentes; la naturaleza distintiva de la inteligencia que es revelada, no siendo accesible por otras vías; la facilidad de comunicación para informar e influenciar a la audiencia objetivo de manera efectiva, y la protección de métodos y fuentes.

Estados Unidos adoptará en el futuro próximo una dimensión con escasos precedentes, además de diversas manifestaciones que trascenderán la concepción tradicional las relaciones entre inteligencia y diplomacia.

La advertencia anterior es una llamada a la cautela no solo en lo que se refiere a la cooperación internacional en materia de inteligencia entre Estados, sino también en cuanto al papel reservado en este ámbito a actores de otra naturaleza. En la actualidad, la creciente importancia adquirida en los asuntos que conciernen a la Seguridad Nacional por diversos actores de interés, tales como entidades universitarias, organizaciones empresariales, contratistas del Estado u otras entidades gubernamentales, es un hecho que presenta no pocas posibilidades en lo que a la capitalización institucional de recursos y talentos de las denominadas «reservas de inteligencia» (Arcos y Antón, 2010). No obstante, esta es una apuesta que no está exenta de riesgos: estos actores de interés, cuya cultura organizacional está con frecuencia más orientada a la publicidad de sus actividades que a la reserva, pueden ser considerados objetivos blandos por parte de servicios de inteligencia extranjeros, que permiten maximizar los resultados de sus operaciones de obtención debido a una menor conciencia sobre el carácter sensible de la información de la que son depositarios y los consiguientes estándares de seguridad menos estrictos que los esperables en cualquier institución experimentada en los asuntos que conciernen a la Seguridad Nacional (National Counterintelligence and Security Center, 2023).

Además de ser objetos de la penetración por parte de servicios de inteligencia extranjeros, estos actores de interés pueden ser también susceptibles a la infiltración por parte de dichas entidades, que tratan de posicionar a sus activos en posiciones relevantes desde la que recabar información sensible en cercanía a centros decisorios clave a escala nacional y/o internacional parapetándose en organizaciones legítimas.

Se puede señalar como muestra de todo lo anterior la implicación de estudiantes e investigadores universitarios en actividades de espionaje, aprovechando las condiciones de movilidad internacional y cooperación interinstitucional que caracterizan a la academia para obtener información de diferente naturaleza. Aunque esta problemática ha llegado a suscitar una especial preocupación en los Estados Unidos sobre los estudiantes de origen chino (Golden, 2018), no falta casuística reciente que pone de manifiesto el empleo de esta táctica de infiltración por parte de los servicios de inteligencia rusos, como son las detenciones en 2022 de dos supuestos activos del GRU de los que, haciendo uso de pasaportes brasileños falsificados, uno de ellos habría tenido acceso a los programas de investigación sobre amenazas híbridas en la Universidad de Tromsø, y el segundo habría estado a las puertas de vincularse a la Corte Penal Internacional en

La Haya como estudiante en prácticas (General Intelligence and Security Service, 2022).

4 Conclusión

Como se ha señalado en páginas anteriores, los cambios en el entorno en el que operan las instituciones estatales dedicadas a la producción de inteligencia han venido acompañados de una reconsideración más o menos profunda de su funcionamiento. Así sucedería una vez desaparecida la lógica de la bipolaridad imperante durante la Guerra Fría, cuando el proyecto kantiano de paz perpetua parecía al fin materializarse a través de las redes de interdependencia articuladas al albor de la globalización dos siglos después de publicado el opúsculo del regiomontano, y por consiguiente, las «viejas guerras» parecían entrar en declive para dejar paso a nuevas formas de conflicto protagonizadas por actores no estatales, dando lugar las amenazas a una cada vez más diversificado entendimiento de lo que la seguridad representa encontraban novísimas manifestaciones (Kaldor, 2012).

Ante tales expectativas, y con una amenaza existencial como la que había representado la Unión Soviética sin comparecer, en la que pasaba a ser considerada superpotencia solitaria se desencadenaría un intenso debate sobre el papel reservado ante este nuevo escenario estratégico a la inteligencia estadounidense. Al margen de las más variopintas iniciativas planteadas en el transcurso de las reformas implementadas entonces (Kerr, 1994), lo cierto es que uno de los más significativos efectos de esta discusión sería una fuerte disminución durante la década de los noventa de las diferentes partidas presupuestarias que financiaban a la comunidad de inteligencia de los Estados Unidos, mermando sus recursos humanos de manera sustancial y condicionando su adaptación a lo que estaría por venir en años venideros (Zegart, 2023).

El caso anterior pone de manifestó que la transformación de las instituciones dedicadas a la producción de inteligencia, incluso cuando adoptan la forma del cambio incremental y adaptativo, es un propósito mucho más fácil de enunciar que de realizar, siendo sus efectos ulteriores inciertos y sus resultados subóptimos. Debido a la naturaleza particular de la misión que les es encomendada y por las capacidades extraordinarias que les son conferidas, como organizaciones de naturaleza burocrática no se caracterizan de manera general por su permeabilidad ante este tipo de procesos y presentan numerosas particularidades ante cualquier tentativa de transformación, lo que con cierta frecuencia ha conducido a que el cambio profundo se produzca de manera reactiva ante hechos o tendencias que ponen en entredicho la eficacia de sus procedimientos estandarizados (Cremades y Cancelado, 2021).

Sin embargo, las evidencias actualmente disponibles de que la inteligencia como función de Estado se encuentra hoy en términos generales en pleno proceso de transición resultan abundantes. De forma muy reciente, tanto William Burns, director de la CIA, como el teniente general Scott D. Berrier, director de la DIA, han declarado públicamente que sus respectivas agencias se encuentran inmersas en sendos procesos de transformación para adaptar su funcionamiento a las exigencias de la competición estratégica (Burns, 2023; Dickson y Harding, 2023). En esta misma dirección, en 2023 verían la luz nuevos materiales doctrinales sobre inteligencia publicados por el Ministerio de Defensa británico y por el Ejército de los Estados Unidos, constatando la importancia adquirida por las denominadas *peer threats*, como ya habían adelantado otros manuales de campo y publicaciones doctrinales publicados algunos años antes (Department of the Army, 2018; North Atlantic Treaty Organization, 2020). Como otras naciones se estarían apropiando de esta tendencia de manera congruente con sus intereses nacionales es hoy un interrogante abierto, cuya respuesta resultará determinante para la cooperación internacional en materia de inteligencia.

Por último, conviene reconocer que el panorama político general podría no ser el más favorecedor para culminar con el éxito deseado procesos de cambio de importancia tan trascendental. El clima de polarización social que atraviesan muchas sociedades democráticas dificulta la adopción de acuerdos de Estado que faciliten una continuidad a largo plazo de las políticas públicas en materia de Seguridad Nacional. Al mismo tiempo, la emergencia de todo tipo de hiperliderazgos (Lasalle y Quero, 2019) impone un determinado estilo en la toma de decisiones que representa un desafío considerable para el establecimiento de unas relaciones entre productores y consumidores de inteligencia mínimamente productivas, condición indispensable para cualquier tentativa de cambio institucional. En ese sentido, las aspiraciones maximalistas que se alejan de la responsabilidad y el sentido común ofreciendo soluciones unívocas a problemas complejos pueden no ser el camino más adecuado. Merece la pena recordar aquí las cautas palabras del genio del renacimiento español, Baltasar Gracián, cuando advertía que «todo arrojamiento está condenado por la Discreción a despeño, aunque tal vez lo absuelva la ventura. Conviene ir detenido donde se teme mucho fondo» (Gracián, 2012: 146).

Bibliografía

Agencia de Noticias Xinhua. (2019). *习近平在中央党校（国家行政学院）中青年干部培训班开班式上发表重要讲话*. [Consulta: 2024]. Disponible en: https://www.gov.cn/xinwen/2019-09/03/content_5426920.htm

Aldrich, R. J. (2011). International intelligence cooperation in practice. En: Born, H., Leigh, I. y Wills, A. (eds.). Routledge, International Intelligence Cooperation and Accountability.

Alexander, M. S. (1998). Introduction: Knowing Your Friends, Assessing Your Allies – Perspectives on Intra-Alliance Intelligence. En: *Knowing Your Friends: Intelligence Inside Alliances and Coalitions from 1914 to the Cold War*. Routledge.

Arcos, R. y Antón, J. (2010). Reservas de Inteligencia: hacia una Comunidad ampliada de Inteligencia. Inteligencia y Seguridad. *Revista de Análisis y Prospectiva*. 8, pp. 11-38.

Arendt, H. (2006). *Sobre la violencia*. Madrid, Alianza Editorial. 144 pp.

Australian Security Intelligence Organisation. (2024). *Director-General's Annual Threat Assessment 2024*. [Consulta: 2024]. Disponible en: https://www.asio.gov.au/director-generals-annual-threat-assessment-2024

Baques, J. (2021). *De las guerras híbridas a la zona gris: la metamorfosis de los conflictos en el siglo XXI*. Universidad Nacional de Educación a Distancia. 362 pp.

Best, R. A. (1996). *Covert Action: An Effective Instrument of U.S. Foreign Policy?* Congressional Research Service. [Consulta: 2024]. Disponible en: https://www.everycrsreport.com/files/19961021_96-844_a3fe515109001b58e7be8b2af3841f9e91066400.pdf

Bischoff, P. (2022). Facial recognition technology (FRT): 100 countries analyzed. *Comparitech*. [Consulta: 2024]. Disponible en: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/

—. (2023). Surveillance camera statistics: which cities have the most CCTV cameras?. Comparitech. [Consulta: 2024]. Disponible en: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Blinken, A. J. (2022). *Secretary Antony J. Blinken Remarks to Employees at the Office of the Director of National Intelligence*. [Consulta: 2024]. Disponible en: https://www.state.gov/secretary-antony-j-blinken-remarks-to-employees-at-the-office-of-the-director-of-national-intelligence/

—. (2023). Secretary Antony J. Blinken Remarks to the Johns Hopkins School of Advanced International Studies (SAIS) "The Power and Purpose of American Diplomacy in a New Era". [Consulta: 2024]. Disponible en: https://www.state.gov/secretary-antony-j-blinken-remarks-to-the-johns-hopkins-school-of-advanced-international-studies-sais-the-power-and-purpose-of-american-diplomacy-in-a-new-era/

Burns, W. J. (2024). Spy and Statecraft: Transforming the CIA for an Age of Competition. *Foreign Affairs*. [Consulta: 2024]. Disponible en: https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns

Bury, P. y Chertoff, M. (2020). New Intelligence Strategies for a New Decade. *The Rusi Journal*. 165(4), pp. 1-12. [Consulta: 2024]. Disponible en: https://www.tandfonline.com/doi/full/10.1080/03071847.2020.1802945

Calabresi, M. (2024). Inside the White House Program to Share America's Secrets. *Time*. [Consulta: 2024]. Disponible en: https://time.com/6835724/americas-intelligence-secrets/

Canadian Security Intelligence Service. (2023). *CSIS Public Report 2022*. [Consulta: 2024]. Disponible en: file:///C:/Users/alvcr/Downloads/CSIS_Public_Report_2022_DIGITAL-eng.pdf

Carmichael, S. W. (2012). *True Believer: Inside the investigation and capture of Ana Montes, Cuba's Master Spy*. Annapolis, Naval Institute Press. 207 pp.

Central Intelligence Agency. (1976). *Research Study: The Dynamics of "Small State" Leverage: Implications for North-South Relations*. [Consulta: 2024]. Disponible en: https://www.cia.gov/readingroom/docs/CIA-RDP79T00889A000800020001-9.pdf

—. (2019). CIA's Latest Layer: An Onion Site. [Consulta: 2024]. Disponible en: https://www.cia.gov/stories/story/cias-latest-layer-an-onion-site/

—. (2023). CIA Launches Telegram Channel. [Consulta: 2024]. Disponible en: https://www.cia.gov/stories/story/cia-launches-telegram-channel/

Central Intelligence Agency and Federal Bureau of Investigation. (1999). *Report to Congress on Chinese Espionage Activities Against the United States*. [Consulta: 2024]. Disponible en: https://www.cia.gov/readingroom/docs/DOC_0001282625.pdf

Centro Conjunto de Desarrollo de Conceptos. (2024). *Entorno Operativo 2035: Primera Revisión*. Ministerio de Defensa. [Consulta: 2024]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/n/entorno_operativo_2035_primera_revisi_n.pdf

Clinton, H. (2011). América's Pacific Century. *Foreign Policy*. [Consulta: 2024]. Disponible en: https://foreignpolicy.com/2011/10/11/americas-pacific-century/

Colom-Piella, G. (2023). Pensamiento militar ruso y suposiciones sobre la zona gris y la guerra en ucrania. *Revista de Pensamiento Estratégico y*

Seguridad CISDE. 8(2), pp. 91-103. [Consulta: 2024]. Disponible en: http://uajournals.com/ojs/index.php/cisdejournal/article/view/1300

Committee on Oversight and Government Reform. (2017). *The OPM Data Breach: How the Government Jeopardized Out National Security for More than a Generation*. [Consulta: 2024]. Disponible en: https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

Cook, A, G. (2023). Addressing Challenges to the Conduct of Intelligence Operations in an Age of Ambiguity. *Communication and Public Diplomacy*. 2(1), pp. 160-172.

Cremades-Guisado, A. y Cancelado-Franco, H. (2021). La inteligencia como organización burocrática: disfunciones del modelo weberiano. *Revista Científica General José María Córdova*. 19(34), pp. 479-496. [Consulta: 2024]. Disponible en: https://revistacientificaesmic.com/index.php/esmic/article/view/701

Cunliffe, K. S. (2023). Cyber-enabled tradecraft and contemporary espionage: assessing the implications of the tradecraft paradox on agent recruitment in Russia and China. *Intelligence and National Security*. 38(7), pp. 1075-1094. Disponible en: https://www.tandfonline.com/doi/full/10.1080/02684527.2023.2216035

Dallas, B., Lewis, J. G. y Pollack, J. H. (2010). *Advanced Technology Acquisition Strategies of the People's Republic of China*. [Consulta: 2024]. Disponible en: https://irp.fas.org/agency/dod/dtra/strategies.pdf

Danish Defence Intelligence Service. (2023). *Intelligence Outlook 2023*. [Consulta: 2024]. Disponible en: https://www.fe-ddis.dk/globalassets/fe/dokumenter/2023/udsyn/-intelligence_outlook_2023-.pdf

Departamento de Seguridad Nacional. (2023). *Informe Anual de Seguridad Nacional 2022*. Presidencia del Gobierno. [Consulta: 2024]. Disponible en: https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2022

Department of the Army. (2018). *FM 2-0: Intelligence*. [Consulta: 2024]. Disponible en: https://irp.fas.org/doddir/army/fm2-0-2018.pdf

—. (2023). FM 2-0: Intelligence. Disponible en: https://irp.fas.org/doddir/army/fm2_0.pdf

Dickson, J. y Harding, E. (2024). *DIA Demonstrates Practical Innovation for Mission Success. Center for Strategic & International Studies.*

[Consulta: 2024]. Disponible en: https://www.csis.org/analysis/dia-demonstrates-practical-innovation-mission-success

Dobbins, J., Shatz, H. J. y Wyne, A. (2018). *Russia Is a Rogue, Not a Peer; China is a Peer, Not a Rogue: Different Challenges, Different Responses*. Rand Corporation. [Consulta: 2024]. Disponible en: https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE310/RAND_PE310.pdf

Dorfman, Z. (2020a). Beijing Ransacked data as U.S. Sources went dark in China. *Foreign Policy* [Consulta: 2024]. Disponible en: https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/

—. (2020b). China used stolen data to expose operatives in Africa and Europe. Foreign Policy. [Consulta: 2024]. Disponible en: https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/

Dulles, A. (1965). *The Craft of Intelligence*. Nueva York, The New American Library of World Literature. 256 pp.

Edstrom, H. y Westberg, J. (2020). *Military Strategy of Middle Powers: Competing for Security, Influence, and Status in the 21st Century*. Routledge.

Eftimiades, N. (1994). *Chinese Intelligence Operations*. Naval Institute Press.

—. (2020). A Series on Chinese Espionage. Vol. I: Operations and Tactics. Vitruvian Press.

Estonian Foreign Intelligence Service. (2024). *International Security and Estonia*. [Consulta: 2024]. Disponible en: https://raport.valisluurea-met.ee/2024/assets/VLA_ENG-raport_2024_240122_Web.pdf

European Union. (2022). *A Strategic Compass for Security and Defence*. [Consulta: 2024]. Disponible en: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Flynn, M., Pottinger, M. y Batchelor, P. D. (2010). *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*. Center for a New American Security. [Consulta: 2024]. Disponible en: https://www.cnas.org/publications/reports/fixing-intel-a-blueprint-for-making-intelligence-relevant

Freedman, L. (2014). Strategic Studies and the problem of power. En: Mahnken, T. G. y Maiolo, J. A. (eds.). *Strategic Studies: A Reader*. Routledge University Press.

General Intelligence and Security Service. (2022). *AIVD disrupts activities of Russian intelligence officer targeting the International Criminal*

Court. [Consulta: 2024]. Disponible en: https://english.aivd.nl/latest/news/2022/06/16/aivd-disrupts-activities-of-russian-intelligence-officer-targeting-the-international-criminal-court

Gioe, D. V. (2023). The Ruse of the New Spycraft Regimes. *Foreign Policy*. Disponible en: https://foreignpolicy.com/2023/10/21/intelligence-spies-global-south-us-egypt-ethiopia-india-espionage/

—. (2017). 'The More Things Change': HUMINT in the Cyber Age. En: Dover, R., Dylan, H. y Goodman, M. (eds.). The Palgrave Handbook of Security, Risk and Intelligence. Londres, Palgrave Macmillan.

Golden, D. (2018). *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities*. Henry Holt and Co. 352 pp.

Gómez, A. S. (2021). Tendencias de evolución de la inteligencia militar. Instituto Español de Estudios Estratégicos, *Documento de Opinión 35/2021*. [Consulta: 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO35_2021_ANGGOM_Inteligencia.pdf

—. (2023). La inteligencia en la guerra de Ucrania. Observaciones preliminares. En: Cuadernos de Inteligencia 1. [Consulta: 2024]. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/c/u/cuaderno__inteligencia_1.pdf

Gracian, B. (2019). *Oráculo manual y el Arte de la Prudencia*. Madrid, Cátedra. 261 pp.

Guo, X. (2012). *China's Security State: Philosophy, Evolution, and Politics*. Cambridge University Press. 486 pp.

Hannas, W. C., Mulvenon, J. y Puglisi, A. B. (2013). *Chinese Industrial Espionage: Technology acquisition and military modernization*. Oxon. Routledge. 494 pp.

Harrington, J. y McCabe, R. (2021). *Modernizing Intelligence, Surveillance, and Reconnaissance to "Find" in the Era of Security Competition*. Center for Strategic & International Studies. [Consulta: 2024]. Disponible en: https://www.csis.org/analysis/modernizing-intelligence-surveillance-and-reconnaissance-find-era-security-competition

Haver, Z. (2023). Private Eyes: China's Embrace of Open-Source Military Intelligence. *Recorded Future*. [Consulta: 2024]. Disponible en: https://go.recordedfuture.com/hubfs/reports/ta-2023-0601.pdf

Herman, M. (1998). Diplomacy and intelligence. *Diplomacy & Statecraft*. 9(2), pp. 1-22.

—. (2004). Intelligence power in peace and war. Cambridge University Press. 414 pp.

Hilsman, R. (1956). Strategic Intelligence and National Decisions. Glencoe. *The Free Press*. 187 pp.

Hitchen, N. (2022). An Untuned Instrument: Strategic Counterintelligence in the Sino-American Technology Competition. *The Hamiltonian*. [Consulta: 2024]. Disponible en: https://hamiltonian.alexander-hamiltonsociety.org/security-and-strategy/an-untuned-instrument-strategic-counterintelligence-in-the-sino-american-technology-competition/

Hockenhull, J. (2022). *How open-source intelligence has shaped the Russia-Ukraine war*. [Consulta: 2024]. Disponible en: https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war

Hoehn, J. R. (2020). Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition. *Congressional Research Service*. [Consulta: 2024]. Disponible en: https://crsreports.congress.gov/product/pdf/R/R46389/4

Holmgren, B. M. (2023). *Intelligence and Diplomacy: A New Moder for a New Era*. [Consulta: 2024]. Disponible en: https://www.state.gov/intelligence-and-diplomacy-a-new-model-for-a-new-era/

Hulnick, A. S. (1991). Intelligence cooperation in the post-cold war era: A new game plan? *International Journal of Intelligence and CounterIntelligence*. 5(4), pp. 455-465.

Huminski, J. C. (2023). Russia, Ukraine, and the Future Use of Strategic Intelligence. *PRISM*. 10(3), pp. 9-25. [Consulta: 2024]. Disponible en: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3511951/russia-ukraine-and-the-future-use-of-strategic-intelligence/

Intelligence and Security Committee of Parliament. (2023). *China*. [Consulta: 2024]. Disponible en: https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf

Interagency OPSEC Support Staff. (2004). *Intelligence Threat Handbook*. [Consulta: 2024]. Disponible en: https://nsarchive.gwu.edu/document/21414-document-18

Interim National Security Strategy Guidance. (2021). *Washington, The White House*. [Consulta: 2024]. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

Johnson, L. K. (2024). Intelligence Collection Priorities in an Age of Renewed Superpower Conflict: Toward a More Expansive Perspective.

The Journal of Intelligence, Conflict, and Warfare. 6(3), pp. 1-31. [Consulta: 2024]. Disponible en: https://journals.lib.sfu.ca/index.php/jicw/article/view/6336/5667

Johnson, L. K. y Scheid, K. J. (1997). Spending for Spies: Intelligence Budgeting in the Aftermath of the Cold War. *Public Budgeting Finance*. 17(4), pp. 7-27.

Joint Chief of Staff. (2019). *Joint Doctrine Note 1-19, Competition Continuum*. [Consulta: 2024]. Disponible en: https://irp.fas.org/doddir/dod/jdn1_19.pdf

—. (2023). Joint Concept for Competing. [Consulta: 2024]. Disponible en: https://smallwarsjournal.com/blog/joint-concept-competing?utm_source=pocket_saves

Jones, S. G. (2023). *The Role of Special Operations in Great Power Competition*. Statement before the House Committee on Armed Services, Subcommittee on Intelligence and Special Operations. [Consulta: 2024]. Disponible en: https://www.congress.gov/118/meeting/house/115334/witnesses/HHRG-118-AS26-Wstate-JonesS-20230208.pdf

Jordán, J. (2018). El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo. *Revista Española de Ciencia Política*. 48, pp. 129-151. [Consulta: 2024]. Disponible en: https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf

Joske, A. (2022). *Spies and Lies: How China's Greatests Covert Operations Fooled the World*. Melbourne, Hardie Grant Publishing. 288 pp.

Kaldor, M. (2012). *New & Old Wars: Organised Violence in a Global Era*. Polity Press. 268 pp.

Kalugin, O. (2009). *Spymaster: My Thirty-two Years in Intelligence and Espionage Against the West*. Basic Books. 466 pp.

Kenney, M. (2003). From Pablo to Osama: Counter-terrorism Lessons from the War on Drugs. *Survival*. 45(3), pp. 187-206. [Consulta: 2024]. Disponible en: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2003.9688585

Kent, S. (1965). *Strategic Intelligence for American World Policy*. Hamden, Archon Books. 226 pp.

Kerr, S. (1994). The debate on US post-Cold War intelligence: One more new botched beginning? *Defense Analysis*. 10(3), pp. 323-350.

Kim, P. M. y Prytherch, M. (2023). *Douzheng: Unraveling Xi Jinping's call for struggle*. Brookings Institution. [Consulta: 2024]. Disponible

en: https://www.brookings.edu/articles/douzheng-unraveling-xi-jinpings-call-for-struggle/

Lasalle, J. M. y Quero, J. (2019). Hiperliderazgo: ¿de qué estamos hablando? En Gutiérrez-Rubí, A. y Morillas, P. *Hiperliderazgos. CIDOB Report #4*. [Consulta: 2024]. Disponible en: https://www.cidob.org/es/articulos/cidob_report/n1_4/hiperliderazgo_de_que_estamos_hablando

Lefebvre, S. (2003). The Difficulties and Dilemmas of International Intelligence Cooperation. *Intelligence Journal of Intelligence and Counterintelligence*. 16(4), pp. 527-542.

Loeb, V. y Pincus, W. (1999). China Prefers the Sand to the Moles. *The Washington Post*. [Consulta: 2024]. Disponible en: https://www.washingtonpost.com/archive/politics/1999/12/12/china-prefers-the-sand-to-the-moles/5204a605-9184-4fe3-9bab-1d8a7e1e234d/

Long, P. (2022). *A Small State's Guide to Influence in World Politics*. Oxford University Press. 241 pp.

Mankoff, J. (2021) Russia in the Era of Great Power Competition. *The Washington Quarterly*. 44:3, pp. 107-125. [Consulta: 2024]. Disponible en: https://www.tandfonline.com/doi/full/10.1080/0163660X.2021.1970905

Mattis, B. (2012). Beyond Spy vs. Spy: The Analytic Challenge of Understanding Chinese Intelligence Services. *Studies in Intelligence*. 56(3), pp. 47-57. [Consulta: 2024]. Disponible en: https://www.cia.gov/static/Beyond-Spy-vs-Spy.pdf

Mattis, P. L. (2012). Assessing Wester Perspectives on Chinese Intelligence. *International Journal of Intelligence and Counterintelligence*. 25(4), pp. 678-699.

Mazarr, M. J. et al. (2018). *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives*. Rand Corporation. [Consulta: 2024]. Disponible en: https://apps.dtic.mil/sti/pdfs/AD1096831.pdf

Mazarr, M. J., Frederick, B. y Crane, Y. K. (2022). Understanding a New Era of Strategic Competition. *Rand Corporation*. [Consulta: 2024]. Disponible en: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA200/RRA290-4/RAND_RRA290-4.pdf

McCabe, T. R. (2021). Chinese Intelligence, Surveillance, and Reconnaissance Systems. *Journal of Indo-Pacific Affairs*. [Consulta: 2024]. Disponible en: https://media.defense.gov/2021/Mar/07/2002595026/-1/-1/1/25%20MCCABE.PDF

Microsoft. (2023). *Digital threats from East Asia increase in breadth and effectiveness*. Microsoft Threat Intelligence. [Consulta: 2024]. Disponible en: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

Ministry of Defence. (2023). *Joint Doctrine Publication 2-00: Intelligence, Counter-intelligence and Security Support to Joint Operations*. [Consulta: 2024]. Disponible en: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf

Ministry of State Security. (2024). You can do anything for intelligence while I shall do nothing against espionage?. *People's Daily Online*. [Consulta: 2024]. Disponible en: http://en.people.cn/n3/2024/0218/c90000-20134150.html

Moore, P. D. (1996). Chinese culture and the Practice of "Actuarial" Intelligence. En: Daye, D. D. A. *Law Enforcement Sourcebook of Asian Crime and Cultures: Tactics and Mindsets*. CRC Press. 426 pp.

—. (1999). China's Subtle Spying. The New York Times. [Consulta: 2024]. Disponible en: https://www.nytimes.com/1999/09/02/opinion/chinas-subtle-spying.html

Morales, J. (2018). La comunidad de expertos sobre política exterior en Rusia. Instituto Español de Estudios Estratégicos. *Documento de Opinión 92/2018*. [Consulta: 2024]. Disponible en: file:///C:/Users/alvcr/Downloads/Dialnet-LaComunidadDeExpertosSobrePoliticaExteriorEnRusia-6715635.pdf

Moulton, T. (2023). Naval Intelligence and Great Power Competition: Rethinking the Community Paradigm. *WAR ROOM, U.S.* Army Naval College. [Consulta: 2024]. Disponible en: https://warroom.armywarcollege.edu/articles/naval-intelligence/

Naational Cyber Security Centrum. (2024). *Ministry of Defence of the Netherlands unconvers COATHANGER, a stealthy Chinese FortiGate RAT*. [Consulta: 2024]. Disponible en: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf

National Counterintelligence and Security Center. (2023). *Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies*. [Consulta: 2024]. Disponible en: https://www.dni.gov/files/NCSC/documents/products/Risk_Mitigation_Web_2023.pdf

National People Congress. (2017). *National Intelligence Law of the People's Republic China (adopted at the 28th Meeting of the Standing Committee of the 12th National People's Congress on June 27, 2017*. [Consulta: 2024]. Disponible en: https://web.archive.org/web/20170704114235/http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm

—. (2023). Counter-espionage Law of the People's Republic China (adopted at the 11 Meeting of the Standing Committee of the 12th National People's Congress on November 1, 2017, and revised at 2 Meeting of the Standing Committee of the 14 National People's Congress on 26 April, 2023). [Consulta: 2024]. Disponible en: https://web.archive.org/web/20230518165130/http://www.npc.gov.cn/npc/c30834/202304/a386e8ffa3d94047ab2f0d89b1ea73c4.shtml

New Zealand Security Intelligence Service. (2022). *Annual Report 2022*. [Consulta: 2024]. Disponible en: https://www.nzsis.govt.nz/assets/NZSIS-Documents/NZSIS-Annual-Reports/2021-22-NZSIS-Annual-Report.pdf

North Atlantic Treaty Organization. (2020). *AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*. Edition B.

—. (2022). NATO 2022 Strategic Concept. Adopted by Heads of State and Government at the NATO. Madrid. [Consulta: 2024]. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

Norwegian Intelligence Service. (2024). *Focus 2024*. [Consulta: 2024]. Disponible en: https://www.etterretningstjenesten.no/publikasjoner/focus

Office of the Director of National Intelligence. (2023). *National Intelligence Strategy 2023*. [Consulta: 2024]. Disponible en: https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf

Oleson, P. C. (2020). Chinese Offensive Intelligence Operations. *The Intelligencer, Journal of U.S. Intelligence Studies*. 26(1), pp. 9-12. [Consulta: 2024]. Disponible en: https://www.afio.com/publications/OLESON_Chinese_Offensive_Intelligence_Operations_AFIO_Vol26_No1_INTEL_Fall_2020.pdf

Olson, J. M. (2019). *To Catch a Spy: The Art of Counterintelligence*. Washington D.C., Georgetown University Press. 256 pp.

Overend, W. (1988). China Seen Using Close U.S. Ties for Espionage: California Activity Includes Theft of Technology and Surpasses That

of Soviets, Experts Believe. *Los Angeles Times*. [Consulta: 2024]. Disponible en: https://www.latimes.com/archives/la-xpm-1988-11-20-mn-463-story.html

O'Rourke, R. (2024). *Great Power Competition: Implications for Defense – Issues for Congress*. Congressional Research Service. [Consulta: 2024]. Disponible en: https://crsreports.congress.gov/product/pdf/R/R43838/99

Pérez, J. M. (2019). El desafío de Rusia a Occidente. *Revista Ejércitos*. [Consulta: 2024]. Disponible en: https://www.revistaejercitos.com/articulos/el-desafio-de-rusia-a-occidente-apuntes-sobre-la-nueva-guerra-fria/

Prunckun, H. (2019). *Counterintelligence: Theory and Practice*. Rowman & Littlefield. 254 pp.

Pulido, G. (2022). *Guerra multidominio y mosaico: El nuevo pensamiento militar estadounidense*. Catarata. 221 pp.

Qingqing, C. (2023). China's Ministry of State Security debuts on WeChat, calls on society to contribute to counter-espionage efforts. *Global Times*. [Consulta: 2024]. Disponible en: https://www.globaltimes.cn/page/202308/1295465.shtml

Ramírez, M. (2024). China, ¿una inteligencia <<de todo a cien>>? Instituto Español de Estudios Estratégicos. *Documento de Opinión 16/2024*. [Consulta: 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO16_2024_MANRAM_China.pdf

Recorded Future. (2021). *Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia*. [Consulta: 2024]. Disponible en: https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf

Reddick, J. y Martin, A. (2024). Leaked documents open the lid on China's commercial hacking industry. *Recorded Future News*. [Consulta: 2024]. Disponible en: https://therecord.media/china-commercial-hacking-industry-isoon-leaks

Rid, T. (2020). *Actives Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux. 528 pp.

Robinson, D. (2024). i-SOON Leak. *Internet 2-0*. [Consulta: 2024]. Disponible en: https://internet2-0.com/i-soon-leak/

Select Committee on Intelligence. (2022). *Organizational Assessment: The National Counterintelligence and Security Center*. [Consulta: 2024]. Disponible en: https://www.rubio.senate.gov/wp-content/

uploads/_cache/files/81fc6844-9253-45b8-b6a1-b8c70b-12d17a/300E063DC1CCDA7BA7D57A4420CF5699.ap-report-22-01-r.pdf

Shedd, D. R. (2020). The Intelligence Posture America Needs in an Age of Great-Power Competition. En: Wood, D. L. (ed.). *Index of U.S. Military Strength. The Heritage Foundation*, pp. 71-88. [Consulta: 2024]. Disponible en: https://www.heritage.org/sites/default/files/2020-11/2021_IndexOfUSMilitaryStrength_WEB_0.pdf

Sims, J. E. (2022). *Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar*. Oxford University Press.

Stempel, J. D. (2010). *Diplomacy and Intelligence*. *Oxford Research Encyclopedia of International Studies*. [Consulta: 2024]. Disponible en: https://oxfordre.com/internationalstudies/display/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-151

Svendsen, A. D. M. (2011). *Intelligence Cooperation and the War on Terror: Anglo-American security relations after 9/11*. Routledge.

Swedish Security Service 2022/2023. (2024). *The Swedish Security Service 2022/2023*. [Consulta: 2024]. Disponible en: https://www.sakerhetspolisen.se/download/18.3222e1b7187a064b07057/1682587027358/SP_A%CC%8Arsbok_2022_Eng_Accessible.pdf

Sweijs, T. y Mazarr, M. J. (2023). *Mind the Middle Powers. Warontherocks*. [Consulta: 2024]. Disponible en: https://warontherocks.com/2023/04/mind-the-middle-powers/

Szayna, T. S. et *al*. (2001). The emergence of peer competitors: a Framework for Analysis. *Rand Corporation*. [Consulta: 2024]. Disponible en: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1346/RAND_MR1346.pdf

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. (2005). *Report to the President of the United States*. [Consulta: 2024]. Disponible en: https://www.govinfo.gov/content/pkg/GPO-WMD/pdf/GPO-WMD.pdf

The Ministry of Foreign Affairs of the Russian Federation. (2023). *The Concept of the Foreign Policy of the Russian Federation*. [Consulta: 2024]. Disponible en: https://mid.ru/en/foreign_policy/fundamental_documents/1860586/

The White House. (2017). *National Security Strategy of the United States of America*. [Consulta: 2024]. Disponible en: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

—. (2022). National Security Strategy. [Consulta: 2024]. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Toler, A., Postma, F. y Grozev, C. (2022). *The Brazilian Candidate: The Studious Cover Identity of an Alleged Russian Spy*. Bellingcat. [Consulta: 2024]. Disponible en: https://www.bellingcat.com/news/americas/2022/06/16/the-brazilian-candidate-the-studious-cover-identity-of-an-alleged-russian-spy/

Tovar Ruiz, J. (2020). *La política internacional de las grandes potencias*. Madrid, Editorial Síntesis. 245 pp.

U.S. Army. (2020). *AFC Pamphlet 71-20-3: Army Futures Command Concept for Intelligence 2028*. [Consulta: 2024]. Disponible en: https://apps.dtic.mil/sti/pdfs/AD1128558.pdf

U.S. Department of State. (2024). *Foreign Affairs Manual*. [Consulta: 2024]. Disponible en: https://fam.state.gov/

Van Cleave, M. (2007a). Strategic Counterintelligence: What Is It and What Should We Do About It?. *Studies in Intelligence*. 51(2), pp. 1-22. [Consulta: 2024].

—. (2007b). Counterintelligence and National Security. National Defense University. [Consulta: 2024]. Disponible en: https://apps.dtic.mil/sti/pdfs/ADA471485.pdf

—. (2022). Hearing on Protecting American Innovation: Industry, Academia and the National Counterintelligence and Security Center. [Consulta: 2024]. Disponible en: https://www.intelligence.senate.gov/sites/default/files/os-mvcleave-092122.pdf

Van de Kerke, T. W. y Hijzen, C. W. (2021). Secrecy, evidence, and fear: exploring the construction of intelligence power with Actor-Network Theory (ANT). *Intelligence and National Security*. 36(4), pp. 527-540.

Walsh, J. I. (2009). *The International Politics of Intelligence Sharing*. Columbia University Press.

Walton, C. (2023). *Spies: The Epic Intelligence War Between East and West*. New York, Simon & Schuster. 640 pp.

Wang Yi (2022). *Maintain a Global Vision,Forge Ahead with Greater Resolve and Write a New Chapter in Major-Country Diplomacy with Chinese Characteristics*. [Consulta: 2024]. Disponible en: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/wjbz_663308/2461_663310/202212/t20221225_10994828.html

—. (2023). 贯彻对外关系法，为新时代中国特色大国外交提供坚强法治保障. [Consulta: 2024]. Disponible en: http://politics.people.com.cn/n1/2023/0629/c1001-40023485.html

Watling, J. (2021). Preparing Military Intelligence for Great Power Competition: Retooling the 2-Shop. *The RUSI Journal*. 166(1), pp. 68-80. [Consulta: 2024]. Disponible en: https://www.tandfonline.com/doi/full/10.1080/03071847.2021.1923408

Whitaker, R. (2024). Intelligence Cooperation in Historical Perspective: From Cold War to Bipolarity in a Multipolar World. En: Juneu, T., Massie, J. y Munier, M. (eds.). *Intelligence Cooperation Under Multipolarity*. University of Toronto Press.

Wise, D. (2011). *Tiger Trap: America's Secret Spy War with China*. Boston, Houghton Mifflin Harcourt.

Wong, E. (2019). How China Uses Linkedin to Recruit Spies Abroad. *The New York Times*. [Consulta: 2024]. Disponible en: https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html

Xi, J. (2023). *新时代中国特色社会主义思想学习纲要*.

Zegart, A. (2023). Defense Budgeting: What Spymasters Really Need. *Hoover Institution*. [Consulta: 2024]. Disponible en: https://www.hoover.org/research/defense-budgeting-what-spymasters-really-need

Zegart, A. B. (2022). *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton, Princeton University Press. 405 pp.

Evolución de las ciberamenazas: nuevos actores para nuevos escenarios

Francisco Marín Gutiérrez

> «Las telecomunicaciones y los sistemas automatizados de tratamiento de la información son muy susceptibles a la interceptación, el acceso electrónico no autorizado y las formas conexas de explotación técnica, así como a otras dimensiones de la amenaza de inteligencia hostil».
>
> *NSDD-145 US National Policy on Telecoms and Automated Information Systems Security, septiembre de 1984.*

Resumen

Los actores de las ciberamenazas son los individuos o grupos originadores de amenazas en el ámbito del ciberespacio y se consideran diversas categorías de los mismos, cada una de ellas con diferentes atributos, motivaciones, niveles de habilidad y tácticas. Estos utilizan el ciberespacio para llevar a cabo acciones ofensivas o, en la mayoría de los casos, para obtener información que proporcione ventajas de carácter estratégico o comercial, o que resulte de interés para la ejecución de posibles futuros ataques.

Los cambios derivados de los nuevos escenarios de enfrentamiento y de la propia dinámica de la tecnología han modificado el tradicional espectro de las amenazas, que se ha diversificado y se ha vuelto más impreciso. No solo han surgido nuevos actores, sino que también los tradicionales han evolucionado adquiriendo una naturaleza dotada de múltiples facetas.

Por todo ello, el analista de inteligencia de ciberamenazas ve dificultado su papel y necesita ser capaz de anticipar ataques futuros, manteniendo para ello un criterio más amplio e intercambiando información con todos aquellos interlocutores afectados por la misma amenaza, que incluye a los sectores público y privado.

Palabras clave

Cibercrimen, Hacktivismo, Actores ofensivos del sector privado, Proveedores comerciales de vigilancia.

Evolution of cyberthreats: new actors for new scenarios

Abstract

Cyberthreat actors are the individuals or groups originating threats in cyberspace and are considered to be various categories of actors, each with different attributes, motivations, skill levels and tactics. They use cyberspace to carry out offensive actions or, in most cases, to obtain information that provides them strategic or commercial advantages, or that is of interest for the execution of possible future attacks.

The changes resulting from new scenarios of confrontation and the dynamics of technology itself have modified the traditional threats spectrum, which has become more diversified and imprecise. Not only have new actors emerged, but the traditional ones have also evolved, acquiring a multifaceted nature.

Therefore, the cyber threat intelligence analyst is challenged in his role and needs to be able to anticipate future attacks by maintaining a broader approach and exchanging information with all those stakeholders affected by the same threat, including the public and private sectors.

Keywords

Cybercrime, Hacktivism, Private sector offensive actors, Commercial surveillance vendors.

En el ámbito del ciberespacio una amenaza es cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un sistema de las tecnologías de la información y las telecomunicaciones, resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio sistema.

Por su parte, los actores de ciberamenazas son los individuos o grupos originadores y/o iniciadores de amenazas, considerándose diversas categorías de los mismos, cada una de ellas con diferentes atributos, motivaciones, niveles de habilidad y tácticas. A partir de la campaña masiva de ciberataques prorrusos contra Estonia en 2007 comenzó a alterarse la división comúnmente aceptada de los actores de ciberamenazas —actores-estado, crimen organizado y hacktivismo[1]—, y los cambios de los últimos cinco años derivados de los escenarios de enfrentamiento y de la propia dinámica de la tecnología han configurado una nueva situación. Actualmente se encuentran entidades no estatales que utilizan técnicas avanzadas propias de los estados, apoyándose en grupos de cibercrimen organizado y *hackers* a modo de *proxy* —adversario por delegación—, e incluso a un crimen organizado y un nuevo hacktivismo convertidos en proveedores de servicios para aquellos que deseen realizar acciones ofensivas en el ciberespacio.

Esta tendencia implica un cambio en los escenarios tradicionales y los convierte en algo más complejo. Por ello, los analistas no pueden centrarse únicamente en detectar y responder a las ciberamenazas ya conocidas, sino que también necesitan ser capaces de anticipar ataques futuros obteniendo información de aquellos nuevos actores que atentan contra su organización de una manera novedosa y representan una amenaza desconocida para la misma.

1 El ecosistema tradicional de las ciberamenazas

Es un hecho conocido que la magnitud y frecuencia de los ciberincidentes y del uso ilícito del ciberespacio han aumentado en los últimos años y han convertido la ciberseguridad en una prioridad de organizaciones y gobiernos (*Estrategia de Seguridad Nacional 2021*, 2021). En este sentido, los más recientes conflictos han evidenciado que el espectro de las amenazas en el ciberespacio se ha diversificado y se ha vuelto más impreciso. No solo han surgido nuevos actores, sino que también los tradicionales han evolucionado adquiriendo una naturaleza dotada de múltiples facetas y otros que hasta ahora no resultaban relevantes han adquirido una mayor importancia.

[1] Ver definición en el apartado 4.

Para clasificar los actuales actores suele tomarse como referencia la taxonomía empleada por el Centro Criptológico Nacional (CCN), que se considera la más adecuada por ser dicho organismo el responsable de la gestión de ciberincidentes que afecten a los organismos y empresas públicas en España. Dicha clasificación reconoce actualmente tres grandes grupos de actores: actores-estado, cibercrimen y hacktivismo. Se debe señalar que el yihadismo o el ciberterrorismo no se consideran ya como actores independientes pues en los últimos años sus actividades han quedado englobadas dentro del hacktivismo o, en algunos casos, asimiladas a las de los actores-estado.

Además de lo anterior, resulta también interesante caracterizar la ciberamenaza según su creciente nivel de sofisticación, dando lugar a tres categorías (*Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, 2012):

— Profesionales que dependen de otros para desarrollar el código malicioso.
— Profesionales que pueden desarrollar sus propias herramientas para explotar vulnerabilidades públicamente conocidas, así como descubrir nuevas vulnerabilidades.
— Individuos / organizaciones que disponen de importantes recursos y pueden dedicarlos a buscar y crear vulnerabilidades en los sistemas.

Simplificando conceptos, los actores de ciberamenazas más evolucionados —tercera categoría de la anterior clasificación— se correspondían hasta no hace mucho con los actores-estado, los inmediatamente anteriores con el cibercrimen y los más básicos con el hacktivismo. Pero, como se ha mencionado, los conflictos actuales han generado cambios sustanciales, y actores que antes eran considerados de importancia menor alcanzan ahora elevados niveles de sofisticación, siendo incluso contratados por los que son considerados principales.

Para este trabajo se ha tomado como base la actual clasificación del CCN, si bien se ha optado por añadir las categorías de nuevos actores del sector privado y los actores internos para evidenciar el creciente papel que estos desempeñan. Se analiza, a continuación, lo sucedido en las distintas categorías y se muestra cómo, en muchos casos, sus capacidades se entrelazan y confunden.

2 Actores-estado: organizaciones que actúan como estados y subcontratación

Los actores-estado son las ciberamenazas que disponen de mayores capacidades y recursos —humanos y materiales— para llevar a cabo operaciones en el ciberespacio. Estos actores son normalmente elementos

especializados de los servicios de inteligencia, Fuerzas Armadas y Cuerpos de Seguridad del Estado del que directamente dependen, y son conocidas genéricamente como Amenazas Persistentes Avanzadas (*Advanced Persistent Threats*, APTs). De las mismas tanto el sector público como el privado intentan realizar un meticuloso seguimiento por ser los actores más peligrosos. Se considera que focalizan sus operaciones en tres categorías de actividades: ciberespionaje, acciones ofensivas y operaciones de influencia.

- Ciberespionaje: es un terreno clave para las operaciones de obtención de información. En los últimos años ha crecido enormemente el número de países que dispone de la capacidad de realizar operaciones de espionaje en este ámbito. Se estima que actualmente más de cien países poseen dicha capacidad y su especialización sigue creciendo, de la misma manera que lo hace la amenaza que representa. Además del beneficio que se puede obtener utilizando unos recursos limitados, es un método con el que se corre un riesgo mucho menor que en el espionaje tradicional porque, dada la dificultad de atribución de las acciones en el ciberespacio, resulta muy sencillo negar la responsabilidad de las operaciones. No se trata solamente de obtener datos que proporcionen una ventaja competitiva sobre sus adversarios, sino también de obtener información sobre el grado de implantación de las medidas de seguridad en, por ejemplo, las infraestructuras críticas de otra nación al objeto de disponer de datos suficientes que posibiliten planificar ataques futuros.
- Acciones ofensivas: organizaciones capaces de desarrollar operaciones en el ciberespacio están ya presentes en la mayor parte de ejércitos de países desarrollados dada la importancia de este ámbito de actuación. Las acciones ofensivas en el ciberespacio tienen el objetivo conseguir, desde el ámbito ciberespacial, efectos que apoyen las operaciones desarrolladas en los otros ámbitos. En este sentido, en la invasión rusa de Ucrania se ha podido ver, de manera limitada, esta combinación de acciones, con grupos rusos tipo APT como Sandworm y APT28, actuando sobre objetivos que estaban siendo atacados simultáneamente mediante métodos cinéticos tradicionales.
- Operaciones de influencia: para los Estados los medios de comunicación que utilizan el ciberespacio como plataforma de difusión —a través de las redes sociales, por ejemplo— desempeñan un papel clave para orquestar campañas de manipulación contra sus competidores o dirigidas a sus propias audiencias nacionales, existiendo evidencias de que ochenta y un países utilizan las redes sociales para difundir propaganda y desinformación política (2020 Global Inventory of Organized Social Media Manipulation, 2021).

Figura 1. Un grupo APT lo componen personas que pueden ser perseguidas internacionalmente como evidencia ésta alerta del FBI contra miembros del GRU - Servicio de Inteligencia Militar ruso -, responsable del grupo conocido como APT28 (Disponible en https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks)

A la hora de ejecutar todas estas actividades los actores-estado no solo utilizan recursos propios, sino que también pueden utilizar como *proxy* a otro tipo de organizaciones, como grupos criminales o hacktivistas, según se muestra en los siguientes apartados. De igual manera los actores estatales contratan infraestructuras de compañías privadas de telecomunicaciones —normalmente localizadas en otras naciones— para enmascarar, por ejemplo, sus campañas de ciberespionaje.

Por otro lado, resulta habitual que algunas naciones se valgan de sus empresas e instituciones académicas para el desarrollo de *malware* (código o programas maliciosos), incrementando así el potencial para llevar a cabo ciberataques. A modo de ejemplo, documentos gubernamentales norteamericanos citan universidades específicas en Shanghái implicadas en operaciones de piratería informática patrocinadas por el Estado y que han recibido

financiación de múltiples programas de subvenciones del gobierno chino y que mantienen posibles vínculos con el Ejército Popular de Liberación para apoyar la investigación relacionada con la «guerra de la información» (*2022 Annual Report to Congress of the U.S.-China Economic and Security Review Commission*, 2022). Otros documentos enumeran diversos centros universitarios chinos que ahora investigan sobre el uso de tecnologías como la inteligencia artificial y el *Machine Learning* (aprendizaje automático) aplicados a las capacidades cibernéticas militares (Cary, 2021).

En relación con los conflictos actuales, una de las lecciones identificadas en la guerra de Ucrania contra Rusia —y en parte refrendada por lo visto hasta ahora en el enfrentamiento de Hamas contra Israel— es que el conflicto en el ámbito ciberespacial se ha visto configurado por la participación a gran escala de actores no estatales dentro de una guerra entre estados. Debido a la reducción del umbral para llevar a cabo ciberataques, los actores de un estado-nación ya no son los únicos con capacidad ofensiva (Duguin y Pavlova, 2023). Igualmente, en el caso del conflicto en Ucrania, ambos beligerantes solicitaron en los primeros días de las hostilidades el apoyo de individuos particulares dispuestos a unirse a un «ejército cibernético», iniciativas que han reforzado y modelado al nuevo hacktivismo, según se muestra posteriormente.

3 Crimen organizado: el cibercrimen como servicio

La cibercriminalidad ha experimentado, en todos los ámbitos, un fuerte crecimiento, paralelo al incremento del desarrollo y uso de las tecnologías de la información y las comunicaciones. Se puede afirmar que las organizaciones dedicadas profesionalmente al ciberdelito, por su continuo crecimiento y evolución, constituyen una de las grandes amenazas a la seguridad mundial, y su utilización del ciberespacio ha llevado a la aparición de nuevos «modelos de negocio» más lucrativos que incluyen los ataques a objetivos nunca considerados anteriormente como los hospitales, afectados por numerosos casos de *ransomware* (secuestro de datos). Además de beneficiarse directamente de esta clase de operaciones, los grupos de cibercriminales ofrecen actualmente, como si de empresas proveedoras de servicios se tratara, diversos tipos de capacidades a otros grupos afines, a compañías que quieren eliminar a un competidor o a cualquiera que esté dispuesto a pagar por sus habilidades. Entre dichas capacidades destacan:

— Acceso como servicio (Access-as-a-Service, AaaS): oferta de servicios delictivos que cobra a los clientes por los accesos a las redes ajenas, predominantemente corporativas, y que resultan fundamentales para los ataques posteriores. Destacan en esta categoría los denominados «Intermediarios de Acceso Inicial» (Initial Access Brokers, IAB), que venden a sus clientes credenciales de acceso a cuentas e infraestructuras expuestas en internet. Son un mercado

en auge y no solo posibilitan los ataques de ransomware y las estafas en línea, sino que también pueden facilitar un ciberataque de un estado contra las infraestructuras críticas del adversario simplificando la fase inicial de reconocimiento. En este sentido existen análisis que recogen cómo en el último año se han puesto a la venta en foros de hacking en ruso credenciales de acceso a infraestructuras de 21 de los 32 países de la OTAN (Clay y Osta, 2024).

— Distributed Denial of Service-for-hire (DDoS-for-hire): en este tipo de servicio los ciberdelincuentes ofrecen, mediante pago, la capacidad de llevar a cabo ataques de denegación de servicio distribuido (DDoS)[2] por encargo. Modelo de ello es el grupo ruso Killnet, que comenzó como proveedor de una capacidad DDoS de alquiler para acabar transformado en grupo hacktivista prorruso.
— Phishing-as-a-Service (PHaaS): oferta de servicios por la que se venden kits de phishing ya preparados —generan correos electrónicos suplantando las direcciones de entidades legales— con el objetivo de obtener información personal y financiera de particulares para su posterior explotación.

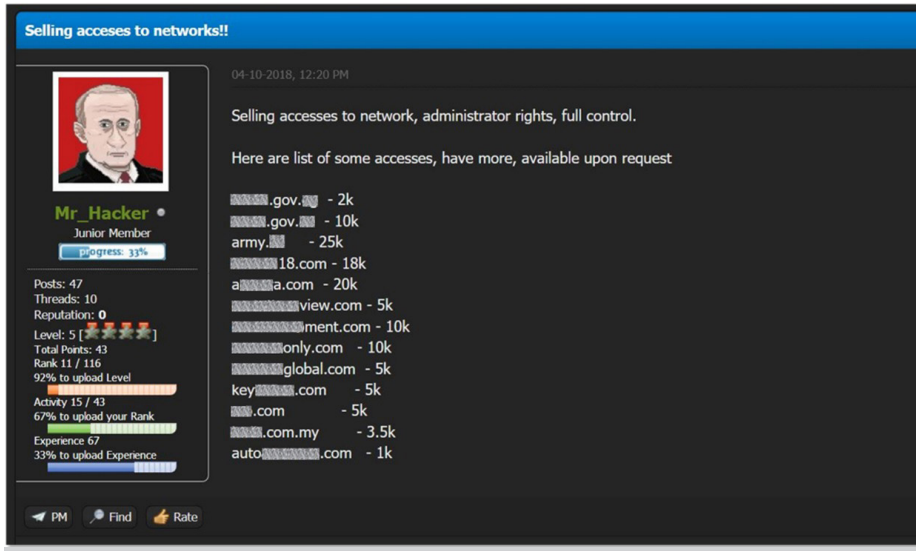

Figura 2. Ejemplo de oferta en la dark web donde un Intermediario de Acceso Inicial vende accesos a redes de distintas empresas (Disponible en https://www.kelacyber.com/the-secret-life-of-an-initial-access-broker/

[2] Se trata de un ataque a un sistema de ordenadores o red mediante el cual se sobrecarga o inunda una máquina objetivo con solicitudes hasta que el tráfico normal es incapaz de ser procesado, lo que provoca que un servicio o recurso sea inaccesible a los usuarios legítimos.

— Ransomware-as-a-Service (RaaS): modelo según el cual los cibercriminales crean un kit malicioso capaz de lanzar un ataque de ransomware que se vende o alquila a los interesados, proporcionando incluso la formación necesaria para poder lanzar el ataque. Según los acuerdos establecidos, el botín del rescate puede ser divido entre el proveedor de servicios, programador y atacante.

Las nuevas herramientas a su alcance posibilitan a los cibercriminales llevar a cabo ciberataques cada vez más ambiciosos contra empresas e instituciones financieras, habiéndose perpetrado incluso robos en diferentes bancos de todo el mundo obteniendo y explotando el acceso al sistema de pagos SWIFT. Se debe destacar que algunas de estas acciones delictivas no corresponden a grupos criminales tradicionales sino incluso a naciones, entre las que destaca Corea del Norte. Respecto a dicha nación, ya en 2019 un informe del Grupo de Expertos establecido para vigilar el cumplimiento de las sanciones impuestas a Corea del Norte por el Consejo de Seguridad de la ONU afirmaba que:

> «El alcance y la sofisticación crecientes de los ciberataques perpetrados por la República Popular Democrática de Corea para robar fondos de instituciones financieras y bolsas de criptomoneda también permiten al país eludir sanciones financieras y generar ingresos de formas más difíciles de rastrear y sujetas a menos supervisión y regulación gubernamental» (*Report of the Panel of Experts established pursuant to resolution 1874 (2009) S/2019/691*, 2019).

Y el mismo documento concluía que «la proporción de ingresos procedentes de ataques de ciberactores de la República Popular Democrática de Corea ha aumentado en relación con los ingresos generados por otras actividades». En este mismo sentido, informes de empresas de ciberseguridad afirman que ciberactores patrocinados por el Estado de la República Popular Democrática de Corea, como el grupo Lazarus, fueron responsables de robos de criptomoneda por valor de casi 1700 millones de dólares en 2022, estimando que el país utiliza los hackeos de criptodivisas para financiar sus programas de armas nucleares (Chainalysis, 2023).

Por otro lado, desde el inicio del conflicto entre Rusia y Ucrania se ubican grupos y perfiles asociados al cibercrimen que han respaldado al Gobierno ruso y han puesto a disposición del ejército todos sus recursos (*malware* e infraestructura) (Centro Criptológico Nacional, 2023). No obstante, ya existían antecedentes de tales conexiones y así, durante el breve conflicto en 2008 entre Rusia y Georgia, los primeros realizaron múltiples ataques informáticos contra infraestructuras críticas georgianas utilizando *botnets* —redes de equipos infectados por un atacante remoto— que pertenecían, o habían sido utilizadas anteriormente, por la *Russian Business Network* (RBN) (Kenneth, 2009), organización cibercriminal que ganó notoriedad en 2007 y 2008.

La RBN también proporcionó alojamiento en servidores seguros a foros de internet que resultaban esenciales para la coordinación y control de los

ciberataques, proporcionando un servicio que garantizaba el anonimato de los atacantes frente a los investigadores de los Equipos de Respuesta a Emergencias Informáticas (CERT) extranjeros. Se debe destacar la agresión contra Georgia, proporcionaba a los *hackers* atacantes listados de objetivos, enlaces a *malware* para atacar las páginas web del Gobierno georgiano, así como consejos prácticos para aquellos con menor experiencia. Curiosamente, la RBN cesó sus actividades poco después de finalizar dicho conflicto.

De nuevo, en 2022, una vez iniciada de la invasión de Ucrania, varios grupos de ciberdelincuentes rusos manifestaron públicamente el apoyo a su gobierno, amenazado con llevar a cabo ciberataques contra países y organizaciones que proporcionasen apoyo material a Ucrania o en represalia por supuestas ofensivas cibernéticas contra el gobierno o el pueblo rusos. Estas amenazas pronto se cumplieron, y coincidieron con ataques contra infraestructuras y sitios web ucranianos. La seriedad de la amenaza representada por esta categoría de actores motivó que las autoridades de ciberdefensa estadounidenses, australianas, canadienses, neozelandesas y británicas publicaran una declaración conjunta afirmando que varios grupos de ciberdelincuentes rusos —The CoomingProject, Killnet, Mummy Spider, Salty Spider, Scully Spider, Smokey Spider, Wizard Spider, Xaknet Team— constituyen una amenaza para las infraestructuras críticas (Cybersecurity and Infrastructure Security Agency, 2022).

4 Hacktivismo híbrido: *proxies* y nuevos intereses

El término *hacktivismo*, acuñado en 1994 por el grupo de *hackers* Cult of the Dead Cow (2019) a partir de las palabras *hacker* y activismo, se puede definir como la utilización de técnicas de piratería informática para promover los objetivos del activismo político o social, sin intención de causar daños graves (por ejemplo, mediante el robo de datos, desfiguración de sitios web, o ataques tipo DDoS).

Hasta 2022 dicho hacktivismo estaba constituido por colectivos desestructurados y descentralizados, con muy diversas agendas que temporalmente se agrupaban en torno a grupos más afamados como Anonymous, que durante años había lanzado múltiples campañas basándose en las preferencias y deseos de sus miembros sin que existiera ninguna afiliación o conexión ideológica real entre los miembros del grupo, ni aparentemente ningún programa a largo plazo. Cualquier grupo o individuo, independientemente de su afiliación política, era bienvenido (*The New Era of hacktivism – State-mobilized hacktivism proliferates to the west and beyond*, 2022).

Poco antes de la invasión de Ucrania por Rusia parecía que los actores tradicionales del hacktivismo como fenómeno idealista sufrían un cierto declive, si bien algunos analistas advirtieron de la posibilidad de un

aumento paulatino en la instrumentación del hacktivismo y de Anonymous como banderas de conveniencia en conflictos híbridos o en ciberataques donde confluyen varios intereses de parte por actores que pretenden una ganancia, ya sea geopolítica, militar, económica o de otra naturaleza (Centro Criptológico Nacional, 2023). Tras la invasión se produjo un cambio en la situación y los principales grupos hacktivistas surgidos en 2022 comparten las características propias de organizaciones estructuradas: cuentan con ideología política definida, una jerarquía diseñada con un claro liderazgo, un proceso de reclutamiento formal e incluso herramientas específicas que los grupos proporcionan a sus miembros.

Además, los grupos han decidido incrementar su visibilidad protagonizando operaciones de relaciones públicas para darse a conocer publicitando ampliamente sus éxitos en redes sociales y sitios web. Estos nuevos grupos no consisten ya en unos pocos individuos al azar que llevan a cabo pequeños ataques DDoS o de desfiguración contra sitios web de bajo nivel sino que llevan a cabo operaciones bien estructuradas, que les permite realizar ataques selectivos en oleadas, a la vez que atraen a individuos más cualificados.

Los grupos del nuevo hacktivismo prorruso se implicaron directamente en el conflicto realizando, sobre todo, campañas de ataques de denegación de servicio, algunos centrados en actividades dentro de Ucrania, pero la mayoría contra cualquier nación que haya proporcionado ayuda al gobierno de Zelensky o incluso se opusiera a la agenda rusa. Existen informes públicos con evidencias técnicas que vinculan a grupos hacktivistas prorrusos como XakNet Team, Infoccentr y CyberArmyofRussia_Reborn con el agente de la amenaza APT28, asociado a la Unidad 26165 de la Dirección Principal de Inteligencia del Ejército ruso (GRU) (Mandiant Intelligence, 2022).

Dentro de los grupos prorrusos existe una nueva tendencia, según la que actualmente ofrecen como servicio sus

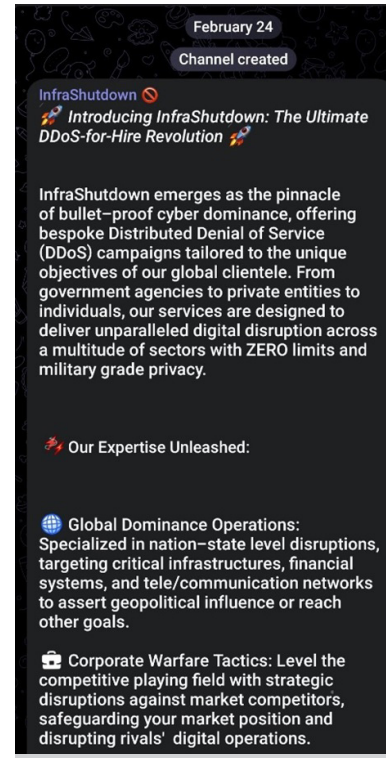

Figura 3. Anuncio del grupo hacktivista prorruso Anonymous Sudan ofertando sus capacidades de ataque mediante el servicio Infrashutdown (Disponible en https://twitter.com/Cyberknow20/status/1761718688460554427/photo/1.)

capacidades de ejecutar ataques DDoS, comportándose como grupos ya citados del cibercrimen. Ejemplo de ello es el reciente anuncio del grupo Anonymous Sudan, que anuncia su servicio *infrashutdown*, haciendo hincapié en su capacidad para ofrecer campañas DDoS personalizadas dirigidas a una amplia gama de entidades, desde organismos gubernamentales hasta empresas privadas y particulares (Ashish, 2024).

Ucrania, por su parte, además de contar con el apoyo de entidades hacktivistas con afiliación previa conocida al movimiento Anonymous, decidió concentrar sus esfuerzos y el mismo 26 de febrero de 2022, el viceprimer ministro y ministro de transformación digital ucraniano, Mykhailo Fedorov, anunció la formación del IT Army of Ukraine, organización patriótica que debía reunir todo el talento disponible y centralizar sus esfuerzos de manera coherente contra objetivos rusos. El IT Army ha sido capaz no solo de llevar a cabo ataques tipo DDoS para paralizar páginas y servicios, sino que también ha exfiltrado información de entidades rusas y ha llevado a cabo ataques limitados contra infraestructuras críticas tanto en Rusia como en los territorios ocupados.

Enlazando con los actores anteriores, la facilidad de adquisición y utilización de servicios dedicados a los ataques tipo DDoS en foros y mercados asociados al cibercrimen hace que entidades con limitadas capacidades técnicas sean capaces de llevar a cabo este tipo de acciones, facilitando la aparición de nuevas comunidades de este nuevo hacktivismo más agresivo y politizado.

5 Nuevos actores del sector privado: una floreciente industria

La creciente necesidad de capacidades ofensivas en el ciberespacio ha llevado al progresivo aumento de un mercado mundial de empresas privadas de ciberseguridad que satisfaga la demanda de gobiernos y agentes privados. Pero las actividades cibernéticas del sector privado plantean importantes retos pues la naturaleza de los servicios que prestan a los gobiernos difumina las funciones y responsabilidades de los sectores público y privado. Además, existe el problema de la distinción entre actividades legítimas e ilegítimas, ya que la deslocalización de las empresas —a veces consistente en un reducido número de empleados trabajando desde distintas naciones— dificultan determinar la jurisdicción aplicable y la supervisión del cumplimiento de los requisitos legales nacionales e internacionales.

Existen diversas actividades en las que el sector privado contribuye a la proliferación de capacidades cibernéticas ofensivas, siendo las siguientes las más importantes:

— Investigación, venta y explotación de vulnerabilidades: individuos o grupos que investigan y venden tanto las vulnerabilidades (agujeros de seguridad en sistemas de software y hardware) identificadas

en los sistemas, como los exploits, códigos desarrollados para la explotación de una vulnerabilidad concreta.
— Desarrollo de malware (Malware-as-a-service): los proveedores desarrollan, mantienen y suministran programas maliciosos para utilizarlos contra objetivos en nombre de un cliente.
— Capacidades de ciberintrusión: suministro de software comercial de vigilancia intrusiva —a veces denominado spyware— que proporciona al usuario la capacidad de obtener acceso remoto a un sistema informático, sin el consentimiento del usuario, administrador o propietario de dicho sistema, con el fin de acceder a un sistema y recopilar sus contenidos.
— Capacidades destructivas o disruptivas: permite aplicar en un sistema informático un efecto perjudicial a través de medios cibernéticos. Esto incluye tanto las herramientas diseñadas para permitir la intrusión como aquellas que provocan una interferencia en la tecnología operativa (como ransomware o software destructivo borrador, conocido como wiper)
— Sistemas de apoyo técnico: se incluye aquí el suministro de tecnologías destinadas a apoyar los aspectos operativos de la operación, tales como el alojamiento en servidores seguros, el registro de nombres de dominio, programas de mando y control, los servicios de redes y las cuentas de entrega que intervienen en la creación inicial de una operación cibernética ofensiva. Muchos proveedores de los servicios de internet (ISP), utilizados por los delincuentes, no realizan un seguimiento exhaustivo de sus usuarios, no almacenan metadatos ni responden a peticiones legales de información sobre el cliente, facilitando así el anonimato imprescindible en las acciones criminales.
— Gestión de operaciones: incluye la realización de operaciones, la organización estratégica de recursos y equipos, las decisiones iniciales sobre objetivos y otras funciones necesarias para gestionar eficazmente una organización que lleva a cabo ciberoperaciones.
— Formación y apoyo: ofrece la formación necesaria para que los usuarios de los programas de operaciones cibernéticas ofensivas sean capaces de utilizarlos con éxito.

Resulta evidente que algunos de estos servicios son ofrecidos también por grupos de cibercrimen, e incluso por hacktivistas, pero en este documento se hace referencia a las actividades económicas ofrecidas dentro de un marco legal.

Los principales protagonistas capaces de ofrecer la variada gama de capacidades presentadas son los conocidos como actores ofensivos del sector privado (*Private Sector Offensive Actors*, PSOA), entidades comerciales que se dedican a la industria de la cibervigilancia y al desarrollo y venta de ciberarmas, incluidos *exploits* y *software* malicioso.

La industria de la vigilancia comercial ha surgido para cubrir un lucrativo nicho de mercado: la venta de tecnología punta a gobiernos de todo el mundo para aprovechar las vulnerabilidades existentes tanto en dispositivos como en aplicaciones digitales de consumo e instalar subrepticiamente programas espía en los terminales de los particulares objeto de vigilancia. De esta manera, los también denominados proveedores comerciales de vigilancia (*Commercial Surveillance Vendors*, CSVs) están fomentando la proliferación de herramientas de piratería peligrosas (*Buying Spying Insights into Commercial Surveillance Vendors*, s. f).

Estas entidades se presentan a sí mismas como proveedores de servicios generales de seguridad y análisis de la información dirigidas a clientes comerciales y afirman que sus herramientas están diseñadas para abordar problemas de seguridad. Para legitimar sus productos alegan que sus servicios se centran en las acciones contra delincuentes y terroristas, si bien muchos de los países que los utilizan en realidad lo hacen contra periodistas y opositores políticos. La realidad es que la industria mundial de la cibervigilancia ha hecho ampliamente accesible la vigilancia como servicio, que incluye diversas herramientas y programas maliciosos avanzados como, Pegasus, DevilsTongue y Predator, dotando a entidades gubernamentales y no gubernamentales de capacidades exclusivas de actores muy sofisticados. Aunque las tecnologías de vigilancia tienen su finalidad, cada vez existe una mayor preocupación acerca de las implicaciones relativas a privacidad, derechos humanos y consideraciones éticas.

Otra tendencia detectada ha sido que un número de empresas privadas, cada vez mayor, realizan campañas de manipulación informativa en el

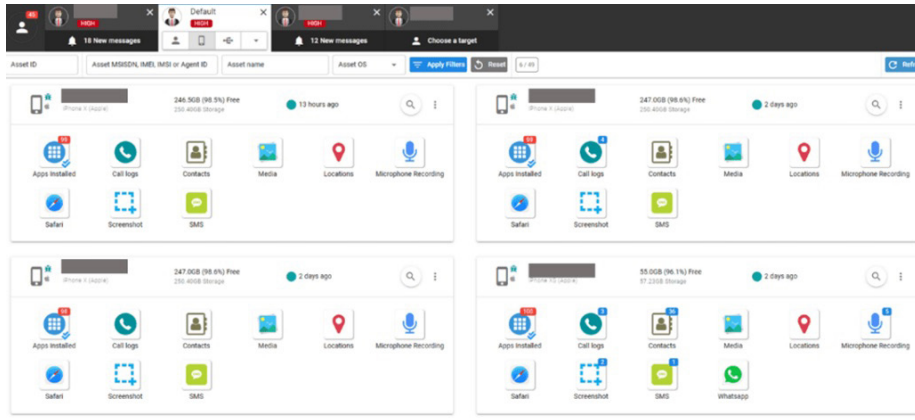

Figura 4. Aspecto del panel de control del programa de ciberespionaje Predator (Disponible en https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/#:~:text=This%202022%20commercial%20proposal%20only,also%20included%20in%20the%20proposal)

ciberespacio. En informes recientes se han identificado en 48 países organizaciones difundiendo propaganda computacional en nombre de un actor político y se estima que desde 2018 se han creado más de 65 empresas que ofrecen propaganda en el ciberespacio como servicio[3]. Las técnicas más utilizadas por estas entidades para impulsar la tendencia de determinados mensajes políticos son la creación de cuentas títere (*sock-puppets*), la utilización de redes controladas de forma automática (*botnets*) para difusión de contenidos en redes sociales y la puesta en práctica de estrategias de microsegmentación de audiencias (*microtargeting*).

Para complicar el escenario, existen empresas especializadas que realmente pueden estar sirviendo de tapadera para las actividades de los Estados. Un buen ejemplo lo constituye OpZero, empresa rusa creada en 2021 con sede en la ciudad de San Petersburgo que ha sorprendido a algunos analistas por la cantidad de recursos de que parece disponer. Resulta llamativo que OpZero haya estado buscando *exploits* para ejecución remota de código de Signal —aplicación de mensajería instantánea y llamadas—, ofreciendo hasta 1,5 millones de dólares por un producto por el que otras empresas importantes del sector como Zerodium ofrecen 500 000 $ (Radauskas, 2022). La hipótesis manejada es que Rusia, al carecer, en aquel momento, de capacidad de acceso al cifrado de las comunicaciones de Signal dentro de Ucrania, decidió utilizar empresas como OpZero a modo de filial de una agencia de inteligencia para solventar estas necesidades técnicas tan particulares.

Por otra parte, existen fuentes que afirman que una gran potencia en capacidades ciberespaciales como China supuestamente utiliza también a actores privados para llevar a cabo tareas de obtención de información. Concretamente, en documentos recientemente filtrados se afirma que la empresa iSoon recibe encargos de instituciones gubernamentales para la obtención de información tanto de objetivos nacionales —organizaciones prodemocráticas de Hong Kong y miembros de la etnia uigur de Xinjiang— como de gobiernos y empresas extranjeros (Nelson, 2024).

Esta proliferación de actores descontrolados supone un riesgo adicional y por ello la idea de crear una normativa contra el uso indebido de programas de ciberespionaje comerciales va adquiriendo cada vez más fuerza. En marzo de 2023, en la Cumbre para la Democracia liderada por los estados Unidos, 35 Estados respaldaron los «Principios rectores sobre el uso gubernamental de las tecnologías de vigilancia» para garantizar un uso responsable de la tecnología de vigilancia. Además, los gobiernos de Australia, Canadá, Costa Rica, Dinamarca, Francia, Nueva Zelanda, Noruega, Suecia, Suiza, Reino Unido y Estados Unidos emitieron una declaración conjunta.

[3] 2020 Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute.

En ella se reconocía que estas herramientas han sido utilizadas indebidamente en todo el mundo por regímenes autoritarios y en democracias, y se comprometían a desarrollar y aplicar políticas para desalentar el uso indebido de programas de ciberespionaje comerciales y fomentar el desarrollo y la aplicación de principios de uso responsable (The White House, 2023).

El pasado febrero, el Reino Unido y Francia pusieron en marcha el Proceso de Pall Mall (PMP), un diálogo dedicado a atajar la proliferación y el uso irresponsable de las capacidades comerciales de ciberintrusión. Como resultado veinticinco naciones —entre las que se encuentran los Estados Unidos— firmaron una declaración reconociendo la necesidad de un desarrollo y un uso legítimo y responsable de dichas capacidades, comprometiéndose a desarrollar un marco de colaboración con la participación de representantes de los Estados, la industria, la sociedad civil y el mundo académico (*The Pall Mall Process declaration: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities*, 2024). Se espera que en breve puedan presentarse resultados concretos.

6 Actores internos (*insiders*): la potenciación de un actor tradicional

Por si no resultara suficiente la gama de actores ya expuesta, dentro del panorama de potenciales ciberamenazas se debe incorporar a otros que siempre estuvieron ahí pero que han incrementado sus capacidades. Son los denominados actores internos o *insiders* —empleados desleales o negligentes de una organización— y resultan de especial relevancia pues sus acciones pueden facilitar el acceso de agentes de la amenaza estatales o de grupos criminales a la organización a la que pertenecen. De hecho, la *dark* web ha creado un activo mercado donde los descontentos pueden convertir fácilmente en dinero su acceso a información privilegiada y por ello los actores de amenazas más sofisticados utilizan esta porción de internet para localizar y contratar a posibles candidatos que les ayuden a introducir programas maliciosos dentro del perímetro de seguridad de una organización (Condello, Pogemiller y Wulkan, 2017) y actuar posteriormente contra ella. Como resultado de lo anterior, se evidencia que cualquier persona con acceso a la red interna, independientemente de su capacidad técnica o antigüedad, puede llegar a representar un riesgo.

También se puede considerar dentro de esta categoría a los clientes enfadados o decepcionados pues, gracias a las herramientas actualmente disponibles, también tienen una capacidad limitada de convertirse en actores de amenazas en el ámbito ciberespacial, afectando especialmente a los aspectos reputacionales de la organización o entidad atacada. Normalmente no persisten ni siguen una carrera delictiva y los ataques se llevan a cabo bajo un intenso estado emocional del autor pero, a pesar de ello, pueden provocar graves daños. Las empresas del sector del juego y las apuestas se

enfrentan a estas amenazas con más frecuencia que otros sectores debido a la implicación emocional de sus clientes (Geenens y Smith, (2022).

Existen ejemplos sorprendentes, como el caso del banco holandés Bunq, que en 2017 recibió un ataque tipo DDoS realizado por un cliente de dieciocho años al que se había incrementado el coste de mantenimiento de la cuenta (Finextra, 2017). Asimismo, se puede reseñar el ataque sufrido por la empresa desarrolladora de videojuegos Blizzard Entertainment, que en octubre de 2020 sufrió un ataque tipo DDoS de veinticuatro horas de duración por parte de jugadores descontentos tras anunciar la decisión de retrasar hasta finales de ese mismo año el lanzamiento de una expansión para un famoso juego (Starym, 2020).

En definitiva, las personas con información privilegiada siguen siendo la forma más eficaz de acceder al interior de una organización y son utilizadas —a veces de forma voluntaria y otras no— por agentes patrocinados por el Estado o ciberdelincuentes para acceder inicialmente al entorno de una víctima.

7 Conclusión

Si en algún momento los actores-estado tuvieron el monopolio de las ciberarmas más sofisticadas, esa era ha terminado y el sector privado es ahora responsable de una parte significativa de las herramientas más avanzadas que se utilizan en las operaciones ofensivas actuales.

El cibercrimen representa una constante amenaza para la Seguridad Nacional y la estabilidad económica, siendo especialmente relevantes los *Initial Access Brokers* al proporcionar el acceso de la práctica totalidad de los vectores de ataque.

Las características del nuevo hacktivismo y su utilización a modo de *proxy* permiten movilizar a los actuales grupos para que sigan narrativas gubernamentales concretas y realicen acciones ofensivas en beneficio de una nación, alcanzando objetivos estratégicos con mayores niveles de éxito y un impacto mediático de enorme amplitud.

Se considera probable que los grupos hacktivistas mejoren su arsenal y sean capaces de llevar a cabo ataques destructivos propios de un actor-estado. Resulta preocupante que cada vez más gobiernos, inspirados por el éxito de los nuevos grupos del hacktivismo híbrido movilizados por Rusia, los incorporen a su arsenal a corto y medio plazo.

La proliferación de *software* ofensivo comercial está transformando el panorama de las ciberamenazas. Este mercado en expansión amplía enormemente el grupo potencial de actores estatales y no estatales con acceso a capacidades de intrusión cibernética y crea la oportunidad de un uso malintencionado e irresponsable de tales recursos, lo que hace más difícil mitigar

y defenderse de las amenazas que plantean, en ausencia de supervisión o de una comprensión de cómo se aplican las normas internacionales.

En el panorama en constante evolución de los ciberconflictos, adelantarse a los actores maliciosos es un reto constante. Resultan evidentes los enormes beneficios de la inteligencia artificial y el aprendizaje automático en la mejora de las defensas de la ciberseguridad, pero no se debe olvidar que los actores de las ciberamenazas también han adoptado estas tecnologías para desarrollar vectores de ataque más sofisticados y peligrosos. Se considera más probable que la tecnología de IA amplifique las ciberamenazas existentes antes que crear otras totalmente nuevas, pero es casi seguro que aumentará drásticamente la velocidad y la escala de algunos ataques. Es es la amenaza que se debe afrontar.

El panorama al que se enfrenta al analista de inteligencia de ciberamenazas es cada día más complejo: organizaciones que actúan como estados, estados que actúan como grupos cibercriminales o mediante supuestos grupos patrióticos, unido a empresas que proporcionan sofisticados recursos a actores que anteriormente carecían de importancia. Para hacer frente a esta situación resulta imprescindible abordar el análisis con un criterio amplio, utilizar bases de datos centralizadas e intercambiar información con todos aquellos interlocutores afectados por la misma amenaza, que abarcan no solo a las Fuerzas y Cuerpos de Seguridad del Estado, sino también a empresas especializadas e incluso a organizaciones académicas. Solo así se comprenderá la amenaza a la que se hace frente.

Bibliografía

2020 Global Inventory of Organized Social Media Manipulation [en línea]. (2021). Oxford Internet Institute. [Consulta: 12 de febrero de 2024]. Disponible en: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors.pdf

2022 Annual Report to Congress of the U.S.-China Economic and Security Review Commission [en línea]. (2022). U.S. Government Publishing Office. [Consulta: 20 de febrero de 2024]. Disponible en: https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf

Buying Spying Insights into Commercial Surveillance Vendors. (s .f.). Google Threat Analysis Group. [Consulta: 7 de febrero de 2024]. Disponible en: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors.pdf

Cary, D. (2021). *Academics, AI, and APTs. How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research* [en línea]. Georgetown University, CSET Issue Brief. [Consulta: 20 de feberero de 2024]. Disponible en: https://cset.georgetown.edu/publication/academics-ai-and-apts/.

Centro Criptológico Nacional. (2023a). *CCN-CERT IA 03-22 Hacktivismo Anual 2021* [en línea]. [Consulta: 18 de febrero de 2024]. Disponible en https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/6594-ccn-cert-ia-03-22-informe-anual-2021-hacktivismo-y-ciberyihadismo-1/file?format=html.

—. (2023b). CCN-CERT IA_35-23 Ciberamenazas y Tendencias 2023. [Consulta: 16 de febrero de 2024]. Disponible en: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html

Chainalysis Team. (2023). 2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers [en línea]. *Chainalysis*. [Consulta: 14 de febrero de 2024]. Disponible en https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/

Clay, E. y Osta, Z. (2024) *Initial Access Broker Landscape in NATO Member States on Exploit Forum* [en línea]. Flare. [Consulta: 18 de febrero de 2024]. Disponible en: https://flare.io/learn/resources/initial-access-broker-landscape-in-nato-member-states-on-exploit-forum/

Condello, T, Pogemiller, D. y Wulkan, I. (2017). *Monetizing the Insider. The Growing Symbiosis of Insiders and the Dark Web*. [en línea]. RedOwl Intsights. [Consulta: 23 de enero de 2024]. Disponible en https://www.nationalinsiderthreatsig.org/itrmresources/RedOwl%20Report-Monetizing%20The%20Insider%20Through%20The%20Dark%20Web.pdf.

Corbin, K. (2009). Lessons From the Russia-Georgia Cyberwar [en línea]. *Internet News*. [Consulta: 28 de febrero de 2024]. Disponible en: https://www.Internetnews.com/security/lessons-from-the-russia-georgia-cyberwar/

Cybersecurity and Infrastructure Security Agency. (2022). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Alert AA22-110A* [en línea]. Cybersecurity & Infrastructure Security Agency (CISA). [Consulta: 13 de febrero de 2024]. Disponible en: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Duguin, S. y Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict* [en línea]. Directorate General for External Policies of the Union. [Consulta: 12 de febrero de 2024]. Disponible en https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.

Finextra. (2017). Dutch bank sentences teenage DDoS culprit to community service [en línea]. [Consulta: 24 de febrero de 2024]. Disponible en https://www.finextra.com/newsarticle/31075/dutch-bank-sentences-teenage-ddos-culprit-to-community-service.

Geenens, P. y Smith, D. (2022). *Hacker's Almanac. A field guide to understanding and applying threat intelligence for a modern security strategy*. [en línea]. Radware Ltd.

Khaitan, A. (2024). Anonymous Sudan Launches New DDoS-for-Hire Service, Filling Skynet Botnet Void [en línea]. *The Cyber Express*. [Consulta: 2 de marzo de 2024]. Disponible en: https://thecyberexpress.com/anonymous-sudan-infrashutdown/

Mandiant Intelligence. (2022). *GRU: Rise of the (Telegram) MinIOns* [en línea]. [Consulta: 21 de febrero de 2024]. Disponible en: https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

Nelson, N. (2024). iSoon's Secret APT Status Exposes China's Foreign Hacking Machinations [en línea]. *Dark Reading*. [Consulta: 2 de marzo de 2024]. Disponible en: https://www.darkreading.com/threat-intelligence/-isoon-contractor-helps-the-prc-hack-foreign-governments-companies

Presidencia del Gobierno. (2021). *Estrategia de Seguridad Nacional 2021* [en línea]. [Consulta: 2 de febrero de 2024]. Disponible en: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

Radauskas, G. (2022). OpZero's modus operandi: opportunity hunter, front for Kremlin, or both? [en línea]. *Cybernews*. [Consulta: 28 de febrero de 2024]. Disponible en: https://cybernews.com/editorial/opzero-exploit-hunter-kremlin/

Report of the Panel of Experts established pursuant to resolution 1874 (2009) S/2019/691 [en línea]. (2019). United Nations Security Council. [Consulta: 14 de febrero de 2024]. Disponible en https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

Starym (2020). Blizzard DDoSed After Announcing Shadowlands Delay [en línea]. *Foro Icy Veins*. [Consulta: 24 de enero de 2024]. Disponible

en https://www.icy-veins.com/forums/topic/52568-blizzard-ddosed-after-announcing-shadowlands-delay/

The Cult of the Dead Cow [en línea]. (2019). [Consulta: 8 de febrero de 2024]. Disponible en: https://cultdeadcow.com/about.html.

The New Era of hacktivism – State-mobilized hacktivism proliferates to the west and beyond [en línea]. (2022). *Check-Point Research*. [Consulta: 28 de febrero de 2024]. Disponible en: https://research.checkpoint.com/2022/the-new-era-of-hacktivism/

The Pall Mall Process declaration: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities [en línea]. (2024). Pall Mall Process. [Consulta: 20 de febrero de 2024]. Disponible en https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

The White House. (2024). *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware* [en línea]. [Consulta: 3 de septiembre de 2024]. Disponible en: https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

US Department of Defense. (2013). *Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat (2012)* [en línea]. [Consulta: 11 de febrero de 2024]. Disponible en: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf.

La necesidad de la Inteligencia en las operaciones del SOC

Iván Portillo Morales

Resumen

Ante el creciente riesgo de ciberataques en diversos sectores, es imperativo adoptar un enfoque proactivo en lugar de reaccionar solo después de un incidente forense. Se sugiere analizar de manera proactiva las tendencias de ataques de actores conocidos que afecten al sector profesional, investigando su *modus operandi*, el *malware* utilizado, vulnerabilidades más explotadas y los métodos de exfiltración de información, por poner unos ejemplos. Para abordar estos desafíos, se propone la implementación de inteligencia de amenazas, con el objetivo de reducir la incertidumbre ante posibles incidentes futuros. Este enfoque busca brindar información accionable para tomadores de decisiones en todos los niveles, ya sea estratégico, táctico u operativo.

En el ámbito de la ciberseguridad, las unidades de inteligencia de amenazas desempeñan un papel fundamental al proporcionar una perspectiva global de las amenazas. Este conocimiento aporta un contexto significativo a las operaciones de un Centro de Operaciones de Seguridad (SOC), permitiendo tomar decisiones anticipadas y responder de manera efectiva a posibles ataques. En resumen, la inteligencia de amenazas se presenta como una herramienta esencial para fortalecer la preparación y la capacidad de respuesta frente a ciberamenazas.

Palabras clave

Ciberinteligencia, Amenazas, CTI, *Cyber threat intelligence*, Ciberseguridad.

The need of Intelligence in SOC Operations

Abstract

With the increasing risk of cyberattacks in various sectors, it is imperative to take a proactive approach rather than reacting only after a forensic incident. It is suggested to proactively analyze attack trends of known actors affecting the professional sector by investigating their modus operandi, malware used, most exploited vulnerabilities and information exfiltration methods, to give a few examples. To address these challenges, the implementation of threat intelligence is proposed, with the aim of reducing uncertainty about possible future incidents. This

approach seeks to provide actionable information for decision-makers at all levels, whether strategic, tactical or operational.

In cybersecurity, threat intelligence units play a critical role in providing a global perspective on threats. This knowledge brings significant context to the operations of a Security Operations Center (SOC), enabling early decisions to be made and effective responses to potential attacks. In short, threat intelligence is presented as an essential tool for strengthening preparedness and responsiveness to cyber threats.

Keywords

Cyber intelligence, Cyber threat intelligence, CTI, Threats, Cybersecurity.

1 Introducción

Cada vez es más común escuchar en las noticias que una organización, organismo o empresa, de cualquier sector profesional, ha sido víctima de un ataque cibernético. Este hecho en sí genera un problema a resolver con una serie de preguntas que sin ser analizadas no tienen respuesta alguna:

- ¿Cuánto tiempo ha estado expuesta la empresa, organización u organismo ante dicho ataque?
- ¿Únicamente han accedido a los sistemas que tienen públicamente expuestos en internet o han conseguido acceder a sistemas internos?
- ¿Se trata de un 0-day[1] o es una vulnerabilidad ya conocida?
- ¿Han robado información confidencial de la empresa? ¿Han filtrado información de la empresa en internet?
- ¿Quién y porqué ha atacado a la empresa?
- ¿Cómo han accedido a la empresa? ¿Hay un insider[2] en la compañía? ¿Es necesario mejorar las defensas?
- ¿El ataque producirá a la empresa un daño reputacional?

Estas son algunas de las preguntas que puede plantearse cualquier empresa, organización u organismo ante un ataque. Frente a esta situación y con la idea de proteger mejor los activos digitales y/o sistemas, es posible utilizar la inteligencia con el objetivo de reducir la incertidumbre ante una situación en particular y tomar las mejores decisiones.

La inteligencia se define como «producto obtenido tras aplicar a la información técnicas de análisis, de forma que resulte útil al decisor a la hora de tomar sus decisiones con el menor nivel de incertidumbre posible, siguiendo el ciclo de inteligencia» (Díaz et *al.*, 2013).

Lo primero que hay que tener en cuenta en inteligencia es esa necesidad real a la que se enfrenta el decisor y ahí es donde la propia inteligencia puede ayudarle a tomar la mejor decisión que se adecue a su negocio. Por un lado, ese decisor puede ser el jefe, cliente, proveedor o un compañero de otro departamento. Por otro lado, la necesidad mencionada hace referencia a la información requerida para abordar un problema al que hay que dar respuesta.

Gracias a las técnicas de análisis mencionadas anteriormente en la definición de inteligencia se puede transformar ese dato recolectado de

[1] Un *0-day*, también conocido como *zero day*, se trata de una tipología de vulnerabilidad que no ha sido descubierta con anterioridad y sin un parche de seguridad asociado que lo mitigue.

[2] Persona que, por diversas motivaciones, extrae información confidencial de la empresa, ya sea de forma intencionada, negligente o bajo chantaje.

internet, ya sea de manera manual o automática, a inteligencia, pasando por un proceso de elaboración mediante el ciclo de inteligencia.

En un primer momento se parte de un dato recolectado por alguna herramienta, descubierto de manera manual o facilitado por algún compañero con el objetivo de su investigación. Dicho dato hace referencia a esa unidad mínima que,por sí sola no indicará nada, ya que será necesario un procesamiento y un tratamiento de este para convertirlo en información ya tratada. En este caso, dicha información seguiría siendo un material sin evaluar, ya sí estaría dirigido hacia un objetivo en particular, pero faltaría aún aplicarle un análisis para separar el grano de la paja y conseguir una información de valor. Con esto último se tendría un conocimiento sobre un suceso o actividad en el que se contaría con una visión general del mismo junto con un contexto de la situación.

Para acabar todo el proceso de generación de inteligencia sería necesario adaptar dicho conocimiento resultante al decisor idóneo, plasmarlo en un informe y añadir unos planes de acción que le ayuden a tomar decisiones. Sin esto último no se estaría hablando de un producto de inteligencia.

Al extrapolar esta definición de inteligencia clásica al ámbito del ciberespacio, se observa que el objetivo, aunque ha cambiado de escenario, permanece inalterado. La finalidad de la inteligencia es que el decisor tome sus decisiones fundamentadas en la contextualización de sucesos asociados a una amenaza, permitiendo elaborar un conocimiento global sobre el entorno analizado.

La disciplina encargada de hacer frente a las ciberamenazas conocida como Cyber Threat Intelligence (CTI) o inteligencia de amenazas en el contexto español, posibilita la adquisición de conocimientos acerca de las amenazas a través de evidencias concretas que incluyen capacidades, infraestructura, motivación, objetivos y recursos del atacante. En este sentido, la inteligencia de amenazas facilita la detección de indicadores relacionados con ciberamenazas, la extracción de información sobre los métodos de ataque, la identificación de amenazas de seguridad y la toma anticipada de decisiones. Este enfoque permite responder de manera precisa y contundente ante posibles ataques.

2 El valor de la inteligencia de amenazas en el ecosistema de la ciberseguridad

En el contexto de la ciberseguridad, la inteligencia de amenazas emerge como una herramienta sumamente eficaz al brindar una visión integral de las ciberamenazas en todos los niveles de una empresa, organización u organismo, abordando tanto aspectos estratégicos como tácticos y operativos, a

un nivel técnico más profundo. Es esencial conocer y comprender las amenazas para desentrañar su funcionamiento técnico y establecer, de manera proactiva, los mecanismos necesarios para una defensa efectiva.

Anualmente, ENISA[3] publica un informe global (European Union Agency for Cybersecurity, 2023) que analiza las principales amenazas y las posibles tendencias asociadas. Según los datos recolectados por ENISA a lo largo de diversos incidentes de ciberseguridad entre julio de 2022 y junio de 2023, se destaca que el *ransomware*[4] ha sido la principal amenaza, representando el 31,32 % de los incidentes. En segundo lugar, se encuentran los ataques DDoS[5], con un 21,4 %, seguidos por las brechas de seguridad en tercer lugar, con un 20,09 %, y los ataques de *malware*[6] en cuarto lugar, con un 8,24 %.

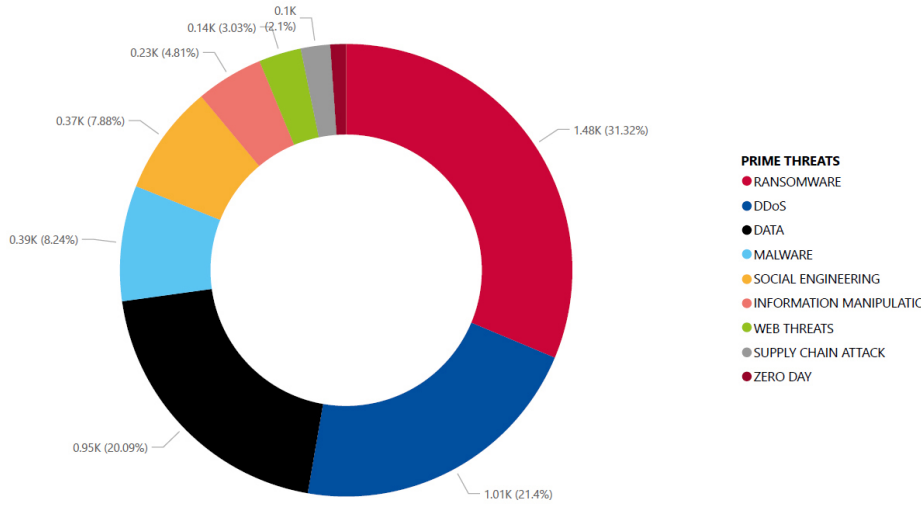

Figura 1. Incidentes de ciberseguridad divididos por tipos (datos entre julio 2022-junio 2023). Fuente: ENISA

[3] Agencia de Ciberseguridad de la Unión Europea (ENISA).

[4] El *ransomware* es una forma de *software* malicioso (*malware*) que restringe o impide el acceso de los usuarios a su sistema. Esto puede lograrse bloqueando la pantalla de acceso al sistema o cifrando los archivos de los usuarios, exigiendo un rescate para restaurar el acceso o proporcionar la clave de cifrado.

[5] El ataque de denegación de servicio distribuido (DDoS) constituye una táctica maliciosa en la cual diversos sistemas informáticos, generalmente comprometidos y dirigidos por un atacante, saturan el objetivo con un exceso de tráfico de datos que supera su capacidad de gestión. El propósito de esta acción es dejar inoperativos los sistemas del objetivo, generando una pérdida de disponibilidad significativa.

[6] El *malware* consiste en un código malicioso capaz de afectar tanto el *hardware* como el *software*, así como los datos, en cualquier tipo de dispositivo.

Las ciberamenazas no conocen límites sectoriales específicos, más bien, ejercen su influencia en diversos ámbitos. Este fenómeno es un reflejo de la omnipresencia de la interconectividad digital en la actualidad. Los datos proporcionados en el mencionado informe de ENISA corroboran de manera concluyente que los actores de amenazas no discriminan entre sectores, reforzando la idea de que ninguna industria queda excluida de sus intentos de ataque. Según estos datos, los incidentes de ciberseguridad se centran en la administración pública con un 19 %, seguido por el sector de la salud con un 8 %, las infraestructuras críticas con un 7 % y los proveedores de servicios digitales en cuarto lugar con un 6 %. Asimismo, se ha identificado que en el 11 % de los ataques, los actores de amenazas han dirigido sus esfuerzos hacia la sociedad civil, sin centrarse en ningún sector específico.

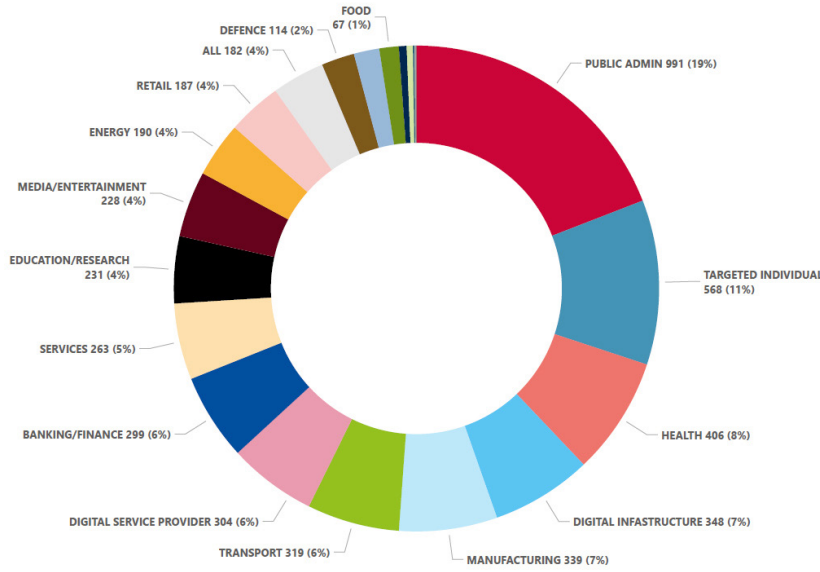

Figura 2. Incidentes de ciberseguridad por sector (datos entre julio 2022-junio 2023). Fuente: ENISA

La inteligencia de amenazas se erige como un activo valioso en diversas áreas profesionales, donde la interacción con amenazas es una constante diaria. La figura del analista se vuelve esencial en cualquier disciplina de inteligencia, desempeñando un papel crucial para analizar de manera eficaz cualquier amenaza.

La gestión de vulnerabilidades, *Red Team*, análisis de riesgos y *threat hunting* representan solo algunos ejemplos de la amplia gama de opciones disponibles para un analista de inteligencia, quien se sumerge en el análisis de amenazas desde diversas perspectivas y entornos. La capacidad del

analista para adaptarse a distintos escenarios de amenazas resulta esencial para comprender y gestionar incidentes que puedan escapar de las tareas cotidianas en momentos particulares.

2.1 *Centro de Operaciones de Seguridad (SOC)*

Un Centro de Operaciones de Seguridad, comúnmente conocido como SOC (por sus siglas en inglés), representa una unidad organizativa dedicada a la vigilancia y gestión de la ciberseguridad en una organización. Su cometido fundamental radica en la identificación, análisis, respuesta y mitigación de amenazas en tiempo real.

La abrumadora cantidad de alertas de seguridad generadas en la mayoría de los SOC a menudo resulta en que muchas no se gestionen adecuadamente, sin dedicarles el tiempo necesario para realizar un análisis exhaustivo del incidente correspondiente. La experiencia y las aportaciones del analista de inteligencia de amenazas, con una perspectiva global, permiten comprender cómo un incidente puede afectar a una empresa desde diversas perspectivas y enfoques, más allá de la parte técnica. Esto facilita la elaboración de planes de acción estratégicos y tácticos para afrontar un incidente con una visión a largo y medio plazo. La distinción crucial radica en que, desde la perspectiva de un forense, se puede comprender lo que ha ocurrido a nivel técnico, pero esto representa más un análisis *post mortem* del incidente. En cambio, la inteligencia de amenazas permite analizar el conjunto completo y desarrollar planes proactivos para evitar que incidentes similares tengan un impacto significativo en la empresa en el futuro.

Figura 3. Sinergias del SOC de BeDisruptive. Fuente: Elaboración interna de BeDisruptive

Un SOC se compone de diversas áreas que deben colaborar de manera sinérgica, creando una interacción efectiva para abordar las diferentes necesidades que puedan surgir. En los subpuntos siguientes, se detallan estas áreas.

2.1.1 Detección y respuesta

Para identificar amenazas en la infraestructura de la organización, es imperativo realizar una monitorización exhaustiva de todos los sistemas que la conforman, con el propósito de detectar comportamientos anómalos o cualquier indicio de actividad maliciosa. Esta vigilancia constante genera diversos tipos de información, los cuales alimentan de datos al Sistema de Gestión de Eventos e Información de Seguridad (SIEM), permitiendo la correlación efectiva entre los datos recopilados.

Es esencial examinar minuciosamente el comportamiento de la red interna, interactuando directamente con los activos de la organización. No obstante, para potenciar la generación de una inteligencia de amenazas más sólida, resulta vital incorporar datos provenientes de fuentes externas. Este enfoque no solo amplía la perspectiva, sino que también facilita la verificación de posibles actividades maliciosas vinculadas a los activos de la compañía. En síntesis, la conjunción del monitoreo interno y la integración de inteligencia externa refuerzan la capacidad del sistema de seguridad para identificar y responder de manera eficaz ante posibles amenazas.

El equipo de respuesta a incidentes asume la responsabilidad de analizar los eventos, evaluando si constituyen amenazas y elaborando estrategias de acción para su mitigación.

Una metodología de respuesta a incidentes clara y ampliamente reconocida en el ámbito de la ciberseguridad es el estándar establecido por el Instituto Nacional de Estándares y Tecnología (NIST[7]). Siguiendo el estándar SP 800-61 del NIST (Computer Security Resource Center, 2012), se pueden definir una serie de fases:

— Preparación: esta fase aborda la necesidad de que toda la entidad esté debidamente preparada para cualquier eventualidad. Una anticipación y entrenamiento adecuados pueden marcar la diferencia entre una gestión eficiente de un incidente y un desastre absoluto. Para lograrlo, es esencial contar con tres pilares fundamentales: personal capacitado, procedimientos bien definidos y tecnología adecuada.

[7] Agencia del Departamento de Comercio de los Estados Unidos que desarrolla y promueve estándares y pautas para mejorar la seguridad, eficiencia e interoperabilidad de sistemas y tecnologías.

— Detección y análisis: esta fase comienza con la recepción de alertas tras la detección de alguna anomalía en forma de posible incidente. Estas alertas son identificadas por los agentes desplegados en la arquitectura organizativa, los cuales proporcionan retroalimentación de manera centralizada al SIEM a través de dispositivos defensivos como firewall, DLP[8], EDR[9], entre otros.
  El siguiente paso en esta fase implica analizar el incidente para determinar si está relacionado con amenazas conocidas. En ausencia de indicadores de compromiso (IoC), se lleva a cabo una consulta en fuentes externas. Posteriormente, se analizan los registros de los sistemas afectados para identificar posibles patrones y similitudes con las técnicas, tácticas y procedimientos (TTPs) asociados a actores o grupos criminales.
— Contención, erradicación y recuperación: durante esta fase, se realiza una evaluación exhaustiva del impacto y la gravedad reales del incidente, estableciendo las acciones necesarias para mitigar la amenaza y minimizar los daños. Además, se ejecutan las acciones previamente delineadas para eliminar cualquier rastro de la amenaza en los sistemas internos afectados. En resumen, se implementan medidas esenciales para contener, erradicar y recuperarse del incidente.
— Post incidente: esta etapa representa la fase final del incidente, una vez que se ha recopilado toda la información relevante y se han implementado medidas para erradicar o remediar el incidente. En este punto, se genera un informe exhaustivo que recopile todos los detalles sobre el incidente y las acciones tomadas durante su remedición. Además, se incorporan lecciones aprendidas que se utilizarán para prevenir futuros incidentes similares, contribuyendo así a fortalecer las medidas de seguridad de la organización.

Al examinar el proceso utilizado para abordar los incidentes, se evidencia que es bastante reactivo. En respuesta a esta dinámica, han surgido la inteligencia de amenazas y la caza de amenazas (*threat hunting*), enfoques que analizan las amenazas de manera proactiva con el objetivo de proteger a las organizaciones de futuros riesgos. Cada empresa tiende a adaptar este proceso según sus necesidades, lo que implica variaciones en la denominación de cada fase. El conocimiento sobre ciberamenazas puede desempeñar un papel crucial para acelerar los tiempos de respuesta ante incidentes. Asimismo, contribuye a mejorar la capacidad para procesar

[8] Solución de seguridad diseñada para prevenir la fuga, perdida o filtración de información confidencial o sensible de una organización.
[9] Sistema integral de protección para los equipos e infraestructura de la empresa. Combina el antivirus tradicional con herramientas avanzadas de monitorización e inteligencia artificial, proporcionando una respuesta ágil y eficiente frente a las amenazas más sofisticadas.

información sobre amenazas de manera eficiente, permitiendo tomar decisiones más informadas y rápidas. Algunos ejemplos de lo mencionado son los siguientes:

- Identificación de amenazas probables: la inteligencia puede ayudar a identificar las amenazas más comunes, permitiendo resolver incidencias que utilicen patrones similares. Contar con una perspectiva global de las amenazas y mantener información actualizada sobre las TTPs más empleadas por actores o grupos criminales es de vital importancia para desarrollar una inteligencia de amenazas proactiva.
- Priorización de las incidencias: la capacidad de un analista de inteligencia de amenazas para evaluar el grado de importancia y la severidad de una amenaza resulta fundamental al momento de asignar prioridades a aquellos incidentes que son más críticos y tienen un impacto significativo.
- Clasificación de las amenazas: catalogar las amenazas en función de un sistema de puntuación de acuerdo con las características de cada una de ellas como, por ejemplo, el impacto, riesgo, severidad, vector de ataque, TTPs, entre otros Este proceso permite la creación interna de una base de datos exhaustiva sobre amenazas y sus riesgos asociados.

En líneas generales, la inteligencia de amenazas permite al SOC enriquecer las alertas recibidas por los agentes distribuidos en las máquinas de la arquitectura interna de la organización con información de amenazas obtenidas desde fuentes externas. Este proceso de enriquecimiento proporciona contexto en torno a la amenaza, lo que permite una evaluación más efectiva del alcance del incidente y la aplicación de medidas de contención. Un analista de seguridad que carezca de conocimientos en inteligencia podría enfrentar dificultades para comprender el contexto de la amenaza, incluso si cuenta con datos externos de fuentes relacionadas con amenazas. Por lo tanto, se destaca la importancia del valor que aporta el analista de inteligencia de amenazas en el análisis de los incidentes recibidos por el SOC.

2.1.2 *Threat hunting*

Es una práctica enfocada en la búsqueda y el análisis proactivo de amenazas dentro de la red interna de una organización.

En lugar de depender exclusivamente de las medidas de seguridad actuales, como SIEM, *firewall* y EDR, que informan de anomalías mediante alertas de manera reactiva después de que las amenazas ya hayan interactuado con los sistemas de la organización, el *threat hunting* adopta un enfoque proactivo. Este método implica la investigación activa de amenazas antes de que los sistemas se vean comprometidos o antes de su

detección. La efectividad del *threat hunting* no solo radica en su enfoque proactivo, sino también en la combinación con tecnología innovadora, un robusto repositorio de conocimiento sobre amenazas y, especialmente, en la presencia de personal altamente cualificado para llevar a cabo esta tarea.

El enfoque del *threat hunting* parte de la premisa de que el adversario ya ha logrado infiltrarse en la red corporativa, observando de cerca todas las comunicaciones y operaciones internas. Bajo esta premisa, el actor de amenazas puede haber permanecido infiltrado durante meses, habiendo obtenido un acceso inicial sin despertar sospechas en los sistemas de detección de amenazas.

El *threat hunting* desempeña un papel crucial en la detención de estos ataques al buscar indicadores de compromiso encubiertos, permitiendo su mitigación antes de que los objetivos del ataque se vean comprometidos.

La identificación de estos IoC implica el análisis minucioso de las actividades diarias en todos los sistemas, incluyendo servidores y equipos de trabajo de los empleados, así como el tráfico de la red. El objetivo es descubrir patrones que puedan indicar cualquier actividad maliciosa que haya pasado desapercibida para las medidas de seguridad lógica. El *threat hunting* se sustenta en cuatro componentes clave, que son:

- Metodología: es esencial que la empresa cuente con mecanismos y procedimientos diseñados para realizar un análisis proactivo de las amenazas. La clave radica en la aplicación constante y la evolución continua de esta metodología para asegurar una respuesta efectiva frente a posibles riesgos y vulnerabilidades en constante cambio.
- Tecnología: además de contar con soluciones integradas de seguridad como EDR, SIEM y firewall, es crucial disponer de sistemas especializados para la detección de anomalías, patrones o actividad maliciosa en todos los sistemas y equipos de la compañía. Asimismo, se hace necesario contar con sistemas capaces de capturar y analizar grandes volúmenes de datos.
- Profesionales especializados: contar con personal altamente cualificado en investigación de amenazas es de suma importancia, siendo la figura del threat hunter esencial en este contexto. Estos profesionales altamente proactivos, gracias a su combinación de conocimientos sobre amenazas actuales y habilidades en áreas como análisis forense o hacking, logran comprender a la perfección el comportamiento de las amenazas con una visión global. Este perfil tiene la capacidad de analizar eventos y actividades generados por los sistemas, identificando patrones que permiten descubrir amenazas ocultas e indetectables hasta ese momento.
- Conocimiento sobre inteligencia de amenazas: el componente final implica contar con un repositorio interno sobre amenazas o, alternativamente, acceder a fuentes confiables que proporcionen

información de calidad sobre amenazas. Estos recursos son fundamentales para obtener información relevante acerca de IoC, TTP o vectores de ataque asociados a amenazas específicas.

El proceso de investigación en *threat hunting*, integrado en la metodología previamente mencionada, abarca diversas fases. En la primera etapa, se formula una hipótesis centrada en identificar posibles amenazas a partir de TTP de actores o grupos criminales conocidos, o mediante patrones maliciosos no clasificados. En la segunda fase, se lleva a cabo una validación de la hipótesis, contrastando los datos establecidos en la misma para garantizar su capacidad de detectar amenazas.

En caso de que la hipótesis sea confirmada, durante los resultados de la prueba en la fase anterior, se busca evidencias de la existencia de la amenaza. En este punto, se descartan los falsos positivos y se conservan únicamente los resultados válidos, siempre y cuando la hipótesis siga siendo válida. En la fase cuatro, se realiza un ataque simulado para emular la amenaza detectada, con el objetivo de identificar nuevos patrones que permitan descubrir TTP no considerados anteriormente. En la última fase, los datos generados en la investigación se utilizan para enriquecer el conocimiento sobre amenazas, mejorando así las medidas de seguridad de la organización.

2.1.3 Gestión de vulnerabilidades

Se emplea como un proceso para identificar posibles brechas de seguridad en los sistemas y aplicaciones de la organización, con el objetivo de evaluar su grado de criticidad y abordar su corrección. La evaluación de la criticidad es fundamental para clasificar todas las vulnerabilidades vinculadas a los sistemas de la organización y para priorizar la atención en aquellos activos en los que el riesgo es significativamente mayor.

Un error común al priorizar vulnerabilidades es enfocarse únicamente en la clasificación de su severidad[10] y tomar decisiones basadas exclusivamente en los valores resultantes. Las métricas empleadas para evaluar esta severidad incluyen el *Common Vulnerabilities and Exposures* (CVE[11]) y el *Common Vulnerability Scoring System* (CVSS[12]).

Al incorporar la inteligencia de amenazas en la gestión de vulnerabilidades, se logra generar un conocimiento global acerca de las amenazas, permitiendo tomar decisiones de manera más eficaz. Un ejemplo de ello sería el siguiente: si hay conocimiento de que un grupo criminal, que ha estado atacando a empresas del sector, tiene como objetivo una tecnología

[10] Grado de impacto que tiene un defecto en el *software* o sistema.
[11] Estándar encargado de identificar las vulnerabilidades. La asignación es gestionada por MITRE.
[12] Estándar que calcula la severidad a partir de fórmulas establecidas.

específica que es vulnerable y resulta que esta tecnología está integrada en la infraestructura, aumenta la probabilidad de sufrir posibles ataques por parte de dicho actor, debido a la vulnerabilidad de España.

Este conocimiento sobre las amenazas permite asignar prioridad a las vulnerabilidades que potencialmente tendrían un impacto más crítico. En lugar de depender únicamente de la clasificación del CVSS mencionado previamente, se evalúa si la vulnerabilidad podría ser aprovechada por un actor de amenazas y si la tecnología disponible estaría más expuesta al éxito de un posible ataque.

2.1.4 Seguridad ofensiva

Dentro del ámbito de la seguridad ofensiva, diversas actividades se benefician significativamente de la inteligencia de amenazas. Una de ellas es la fase OSINT dentro de las pruebas de penetración (*pentest*[13]). En esta fase, se lleva a cabo la recolección de información tecnológica de la empresa a partir de fuentes abiertas. La inteligencia de amenazas desempeña un papel crucial al identificar la verdadera superficie de exposición de la compañía, basándose en la infraestructura directamente expuesta en internet y la tecnología específica empleada.

En función de esta tecnología, el equipo de inteligencia puede proporcionar datos sobre vulnerabilidades conocidas que podrían ser explotadas en dicha tecnología, así como vectores de ataque con una probabilidad elevada de éxito, basándose en tácticas empleadas por actores maliciosos con características similares.

El equipo de seguridad ofensiva también realiza actividades conocidas como *Red Team*, un ejercicio diseñado para simular ataques sofisticados, imitando las tácticas de un actor de amenazas real. En términos generales, este ejercicio busca acceder a los sistemas internos de la compañía con el propósito de eludir todas sus defensas, llevando a cabo operaciones específicas para evaluar la efectividad de las medidas de seguridad establecidas. Estas operaciones pueden incluir la extracción de información sensible fuera de la compañía o la modificación de archivos, entre otras acciones.

En el contexto del ejercicio de *Red Team*, la inteligencia de amenazas desempeña un papel fundamental al proporcionar información relevante sobre nuevos *exploits* (0days), vectores de ataque y TTP utilizados por actores de amenazas. Además, contribuye a la creación de escenarios específicos, adaptados tanto al sector de la organización como a sus sistemas críticos.

[13] Evaluación de seguridad de los sistemas informáticos, por medio de ataques controlados, con el objetivo de detectar y explotar vulnerabilidades. La finalidad primordial es verificar la efectividad de las medidas de seguridad implementadas por la compañía.

Por otra parte, la inteligencia de amenazas, al monitorear diversos foros *underground*, grupos y canales de Telegram, puede suministrar información relacionada con credenciales recientemente comprometidas o la venta de accesos robados, ya sean remotos o internos de la compañía, que los actores de amenazas estén comercializando.

2.2 *Ciberseguridad global*

Más allá de la operativa del SOC, la integración de inteligencia de amenazas puede extenderse a diversas áreas, con un enfoque más centrado en la consultoría. Dos ejemplos destacados donde la inteligencia de amenazas puede agregar valor son el análisis de riesgos y las actividades dentro del ámbito político.

2.2.1 Análisis de riesgos

El análisis de riesgos cumple la función de evaluar y estimar de manera objetiva el riesgo actual, pero actualmente enfrenta varios desafíos. En primer lugar, se encuentra la cuestión de los resultados no cuantificados, provenientes de diversas fuentes y expresados a través de niveles de amenazas representados por colores. Aunque se entiende que el color rojo indica un riesgo muy alto, en muchas ocasiones carece de un valor numérico que precise el grado de severidad. Otro problema se relaciona con la obtención de información de manera parcial e incompleta. Estos inconvenientes pueden dar lugar a un producto de análisis que, aunque aparenta ser preciso, en realidad carece de la acción necesaria debido a la falta de información detallada y cuantificada.

Existen modelos de riesgos que calculan el riesgo propio a través de un análisis cuantitativo, siendo uno de ellos el modelo de análisis de factores de riesgo de información (FAIR). Este modelo posibilita la evaluación del riesgo mediante la simulación de diversos escenarios afectados por amenazas específicas. En el marco del FAIR, el primer paso implica la creación de una lista de amenazas que podrían impactar directamente en el negocio, seguido por el segundo paso que consiste en estimar las probabilidades de éxito de los ataques.

En este contexto, la posesión de fuentes de información confiables es crucial para realizar un análisis de riesgos preciso, y contar con datos actualizados sobre amenazas actuales se vuelve esencial. Por esta razón, la aplicación de conocimientos de inteligencia de amenazas al análisis de riesgos puede proporcionar información adicional sobre una amenaza específica. La inteligencia de amenazas puede ofrecer respuestas a preguntas como:

— ¿Qué actores o grupos criminales están utilizando el mismo ataque?
— ¿El sector está siendo afectado por la amenaza?

— ¿Qué TTP utiliza la amenaza? ¿Se aprovecha de alguna vulnerabilidad conocida?
— ¿Provocan daños en los sistemas únicamente o también afecta al negocio?

2.2.2 Ámbito político

En el ámbito político, la geopolítica emerge como una herramienta fundamental, siendo su esencia el estudio de las relaciones entre países desde una perspectiva geográfica y política. Definida como la investigación de cómo la geografía y otros elementos influyen en la dinámica mundial, la geopolítica busca comprender cómo los cambios pueden afectar las relaciones nacionales e internacionales, así como los conflictos y alianzas entre países. Su propósito es influir en las decisiones estratégicas de los Estados, analizando de cerca cómo la ubicación geográfica y otros factores moldean las estrategias políticas a nivel global.

Históricamente, la geopolítica y la ciberseguridad se percibían como áreas separadas, sin una conexión directa. Sin embargo, los recientes conflictos internacionales, manifestados en guerras, han demostrado que las acciones en el ámbito físico tienen repercusiones directas en el ciberespacio. Se ha observado la participación de actores de amenazas con motivaciones claramente ideológicas y políticas en diversos bandos de los conflictos bélicos. En este contexto político, se han intensificado los ataques cibernéticos, destacando tanto los ataques DDoS como los dirigidos estratégicamente a infraestructuras críticas en los últimos años.

3 Elementos clave de la inteligencia de amenazas

La información recopilada de diversas fuentes sobre amenazas se clasifica según su naturaleza y la información asociada, categorizándola en grupos específicos. Estos datos recopilados se emplean para la detección proactiva o reactiva de actividades maliciosas llevadas a cabo por actores de amenazas, con el fin de salvaguardar a la organización de posibles amenazas tanto internas como externas. Los principales tipos de información incluyen: observables, indicadores de compromiso, indicador de ataque (IoA), técnicas, tácticas y procedimientos, *cyber kill chain* y actores de amenazas. A continuación, se proporcionarán definiciones y explicaciones detalladas de cada uno de estos tipos de información mencionados.

3.1 Observable

Los observables representan el nivel más básico de información utilizado para la identificación de amenazas. Este tipo de información analiza todos los eventos medibles o propiedades de estado que pueden ser detectados

en el ciberespacio. En el caso de observables basados en eventos, se refieren a cualquier cambio registrado en un archivo o cualquier activación de reglas en un Sistema de Detección de Intrusiones (IDS). Por otro lado, los observables basados en propiedades de estado están vinculados a modificaciones en el valor de una clave de registro, variable del sistema o valor *hash* de un archivo de sistema.

La clasificación de un observable como evento o propiedad de estado generalmente no proporciona conclusiones sobre si se trata de una acción maliciosa. Un conjunto de observables es simplemente una agrupación de aspectos generados en un sistema, que pueden medirse o detectarse. Aquí radica la diferencia fundamental entre un observable y un indicador de compromiso.

3.2 *Indicador de compromiso (IoC)*

Un indicador de compromiso se define como «un artefacto técnico u observable que sugiere que un ataque es inminente, está en curso o que ha podido ocurrir ya» (Johnson, et *al.*, 2016). Algunos ejemplos de indicadores son: URL, dirección IP, rango IP, *hash*, dominio, registro DNS como MX, NS, SOA y CNAME.

La premisa fundamental de los IoC radica en la detección de patrones tanto de forma reactiva como proactiva, con el objetivo de identificar indicadores vinculados a posibles amenazas que puedan afectar a la organización. Estos indicadores pueden manifestarse en registros de *logs* de sistemas internos. Además, permiten tomar medidas preventivas para defenderse de futuras amenazas, como la inclusión en listas negras de direcciones IP asociadas a *botnets*, por ejemplo.

Los IoCs son fundamentales por dos razones destacadas. En primer lugar, posibilitan la documentación precisa de una amenaza, proporcionando datos específicos y utilizando una terminología compartida. Esta uniformidad en el lenguaje facilita la comunicación interna en el equipo y la colaboración con otras organizaciones. En segundo lugar, ofrecen a los equipos técnicos una herramienta eficaz para gestionar datos de manera automatizada, permitiendo la identificación rápida de la presencia de indicadores externos en los sistemas internos de la organización.

Un IoC engloba cualquier observable que esté asociado con una amenaza. Al analizar estos observables, se pueden identificar patrones similares de amenazas en diferentes instancias. Aunque la variedad de IoCs es extensa y depende del tipo de amenaza, algunos de los más utilizados y reconocidos incluyen:

— URL.
— Dirección IP Origen.

- Dirección IP Destino.
- Dirección MAC Origen.
- Dirección MAC destino.
- Puerto.
- Nombre servicio.
- Protocolo.
- Rango IP.
- Dominio.
- Registro DNS como MX, NS, SOA, CNAME.
- Hostname.
- Hash (MD5, SHA1, SHA224, SHA256, SHA512).
- Fecha del incidente.
- Correo electrónico.
- Nombre de procesos y archivos afectados.
- Muestra de fichero malicioso.
- Funciones utilizadas por el archivo malicioso.
- Clave de registro.
- Librerías importadas.
- Username.
- Cookie: son archivos generados por los navegadores web. Incluye información relativa a la autenticación o sesión del usuario, pudiendo incluso suplantar la identidad del propio usuario en el caso de que esté autenticado en algún servicio de terceros.
- CVE (Common Vulnerabilities and Exposures), CPE (Common Platform Enumeration).
- IBAN, BIN (número de identificación bancario), BIC (Código de identificación bancario).
- BTC, ETH (direcciones de criptomonedas: Bitcoin y Ethereum).

Es importante considerar que los IoCs pueden tener una fecha de vencimiento, que depende de su vigencia o desuso. Por esta razón, en el ámbito de la inteligencia de amenazas, se hace referencia al ciclo de vida de un IoC. En este ciclo, los IoC pasan de un estado a otro según su madurez. Inicialmente, un indicador se encuentra en el estado de revelación, surgido a partir de un análisis interno mediante la detección en la red interna de la empresa o durante una investigación forense para un cliente. Alternativamente, puede originarse a través de un análisis externo, ya sea de un proveedor de inteligencia, una organización con la que se tenga una federación, o mediante un *feed* de fuentes públicas.

Para clasificar un IoC como maduro, es esencial someterlo previamente a un análisis exhaustivo en un entorno controlado específico. Este proceso tiene como objetivo verificar la fiabilidad del indicador en cuanto a la detección de actividades maliciosas.

Una vez que el análisis sea concluyente y el indicador se haya contrastado de manera efectiva, estará listo para su uso e integración en los sistemas de detección. Cuando este IoC esté implementado y sea reconocido como coincidencia con actividad maliciosa a través de una regla de detección en algún sistema defensivo, el indicador será etiquetado como útil.

El final de la vida útil de un IoC será determinado por el actor de amenazas en función de si decide dejar de utilizar dicho indicador en sus campañas y ataques. En caso de que el indicador no vuelva a ser empleado, se considerará obsoleto, lo cual es común en situaciones que involucran direcciones IP y URL altamente específicas.

3.3 *Indicador de ataque (IoA)*

«Los indicadores de ataque (IoA) se centran en detectar la intención de lo que pretende lograr el adversario, independientemente de la muestra de malware o exploit empleado en el ataque» (Guerra Soto, 2023). En otras palabras, su enfoque se centra en identificar patrones y actividades que indiquen la existencia de un ataque en curso o de un intento de comprometer la seguridad de un sistema.

Los IoA se especializan en analizar las acciones que un adversario debe llevar a cabo durante un compromiso, evaluando sus intenciones y objetivos mediante el análisis de comportamientos anómalos, actividades sospechosas o patrones de ataque específicos. Este tipo de indicador se revela como un componente esencial en una estrategia proactiva, desempeñando un papel valioso en la anticipación y detección temprana de ataques antes de que se concreten en incidentes reales.

Una distinción fundamental entre un IoC y un IoA radica en que los primeros son indicadores reactivos, como direcciones IP, *hashes* de *malware*, firmas, *exploits* y vulnerabilidades. Por otro lado, los IoA, a diferencia de centrarse en las herramientas utilizadas por los adversarios, se fundamentan en el comportamiento de estos. Por ejemplo, si llevan a cabo movimientos laterales, establecen persistencia, se conectan a un servidor de comando y control o realizan la filtración de información.

3.4 *Actores de amenaza*

Los actores de amenaza, también referidos como adversarios, pueden ser individuos o grupos vinculados a un ataque específico. La información que se puede recopilar en relación con un actor incluye:

- Afiliación a un colectivo especifico, como algún servicio vinculado a un estado-nación o grupos hacktivistas, entre otros.
- Identidad del atacante.

— Motivación del ataque.
— Sector en los que opera.
— Vulnerabilidades y tecnologías que suele explotar.
— Relación con otros actores de amenazas.
— Modus operandi y TTP relacionados.

Los actores de amenaza pueden categorizarse según su motivación. En base a esta premisa, se obtiene la siguiente clasificación de actores:

— Ciberespionaje: el espionaje cibernético se enfoca en la explotación de sistemas y redes de manera paciente, persistente y creativa con el objetivo de obtener ventajas estratégicas en ámbitos económicos, políticos y/o militares. Una de las principales amenazas utilizadas en el ciberespionaje son las amenazas persistentes avanzadas (APT). Los actores que operan bajo esta motivación incluyen:
  • Estado-Nación: actividades de recolección de inteligencia patrocinadas por el gobierno y/o fuerzas militares de un país para cumplir con objetivos específicos.
  • Corporativo o empresarial: actividades centradas en obtener ventajas competitivas desleales dentro de una industria, donde los *insiders* desempeñan un papel crucial.
— Cibercrimen: se trata de una evolución de la actividad delictiva tradicional trasladada al ciberespacio. Su enfoque principal es el robo de información personal y de cuentas, así como la ejecución de campañas de influencia con objetivos monetarios. Dentro de esta categoría, existen diversos subtipos de actores que llevan a cabo actividades vinculadas al fraude online, phishing, ataques mediante ransomware, robo de identidad y exfiltración de información. La mayoría de los ataques se concentran en la ingeniería social, buscando engañar a las víctimas para que compartan información confidencial o ejecuten código malicioso en sus dispositivos.
— Hacktivismo: se refiere a actividades llevadas a cabo por activistas que buscan influir en la opinión y/o reputación de organizaciones, afiliaciones o causas específicas basándose en sus creencias. Un ejemplo de esto es el grupo Anonymous en sus inicios, que operaba como colectivos independientes en función de sus ideales, objetivos y, especialmente, su país o región de origen. Este colectivo solía carecer de una jerarquía formal de liderazgo, en gran parte debido a su dispersión geográfica y a la diversidad de intereses entre sus miembros.
  Por otro lado, hay grupos de actores con la misma motivación, pero con un liderazgo más cohesionado y estructurado, como es el caso de NoName057(16). Estos suelen mostrar apoyo político a algún partido o gobierno específico, actuando bajo sus directrices. Entre los ataques más comunes asociados a esta motivación se encuentran

los DDoS, la filtración de información confidencial y la manipulación del contenido en perfiles sociales y páginas web para respaldar causas específicas.

— Ciberterrorismo: esta manifestación implica la convergencia del ciberespacio con el terrorismo, donde diversas operaciones de sabotaje o ciberataques buscan obtener acceso no autorizado a información sensible. Estos actos ocasionan pérdidas económicas, perturban y dañan infraestructuras críticas, y difunden propaganda con el objetivo de generar miedo y pánico en la sociedad. Las motivaciones detrás de estos actores suelen incluir la interrupción de bienes o servicios para las víctimas, así como la intimidación de la población para ejercer una influencia específica sobre ella.
— Guerra híbrida o ciberguerra: estas operaciones buscan eliminar o degradar las capacidades de un objetivo, enfocándose específicamente en un estado-nación. Pueden actuar como complemento a actividades militares o ser llevadas a cabo por motivaciones propias. Los objetivos de estas acciones ejecutadas por los actores incluyen la interrupción de las operaciones de los estados-nación enemigos, la degradación y manipulación de las capacidades subyacentes de estos y la destrucción de objetivos físicos pertenecientes a los estados-nación adversarios.

Esta información se emplea para obtener una comprensión más profunda del adversario y para implementar contramedidas más efectivas destinadas a salvaguardar los sistemas de la organización. Este proceso se lleva a cabo mediante un análisis exhaustivo de cada táctica, técnica y procedimiento (TTP). Los niveles de atribución resultan invaluables para identificar la autoría de un determinado ataque, permitiendo relacionar TTP que no pueden ser atribuidas a ningún actor conocido. A través de la similitud en las técnicas o tácticas empleadas, es posible vincular estos ataques a actores específicos. Contar con un repositorio que almacene las capacidades principales de los actores es esencial para atribuir ciertos ataques que inicialmente no han sido identificados.

Los distintos niveles de atribución para clasificar a cada adversario se describen de la siguiente manera:

— High-Level Motivation: eepresenta las motivaciones de alto nivel. Las amenazas resultan más fácilmente atribuibles, ya que generalmente se agrupan en alguna de las 5 motivaciones mencionadas anteriormente.
— Qualifiers: la amenaza se clasifica según ciertos aspectos, como el objetivo preferido (sector, afiliación, tipo de información, etc.), actividades patrocinadas (financiación) y la detección de posibles relaciones con otros grupos criminales o actores a través de operaciones similares, la misma ideología política o intereses comunes.

— Group: Incluye la identificación a través de TTP, categorización por herramientas y malware utilizados, infraestructura empleada en el ataque y el grado de cohesión del grupo.
— Individual: este nivel resulta particularmente desafiante de identificar, principalmente porque los adversarios operan en un nivel altamente avanzado, utilizando técnicas extremadamente sofisticadas e innovadoras. Suelen llevar a cabo ataques muy específicos y dirigidos

3.5 Tácticas, técnicas y procedimientos (TTP)

Constituyen un conjunto que describe el comportamiento de un actor malicioso. Estos elementos son cruciales para comprender las operaciones ejecutadas por los adversarios, abarcando el objetivo perseguido, la manera en la que llevan a cabo sus acciones y las razones detrás de la elección de métodos específicos. Además, los TTP son esenciales para simular escenarios de ataque de manera controlada, particularmente en proyectos de *threat hunting* y *red teaming*. A continuación, se detallan cada uno de los términos que integran un TTP:

— Táctica: engloba la descripción del comportamiento a alto nivel. Se puede definir, de manera más precisa, como el proceso que sigue un adversario para alcanzar un objetivo determinado, apoyándose en diversas técnicas para lograr dicho fin. Esto implica que la táctica analiza las acciones llevadas a cabo por un adversario para entender que está intentando conseguir y el porqué de su operativa.
— Técnica proporciona una descripción más detallada dentro del marco de la misma táctica. Se define como una actividad que utiliza un patrón conocido para ejecutar los movimientos delineados en la táctica y así cumplir con el objetivo establecido. A través de la técnica, se es capaz de comprender cómo un adversario ha logrado sus objetivos, adquiriendo conocimiento sobre los métodos empleados para ello.
— Procedimiento: ofrece una descripción aún más detallada, pero dentro del contexto de la técnica y a un nivel más bajo. El procedimiento se define como una guía paso a paso que contiene todas las pautas o acciones oficiales a realizar, las cuales deben cumplir el objetivo de obtener el resultado deseado en la parte técnica.

Los TTP constituyen un recurso invaluable para la detección de nuevas amenazas, ya que, al analizar las técnicas empleadas en un ataque, es posible identificar la táctica asociada y, por ende, descubrir qué actor o grupo criminal está detrás de la amenaza. El *framework* ATT&CK[14] de MITRE se destaca como una de las referencias globales en cuanto a TTP. Originado en 2010 para categorizar el comportamiento del adversario durante ejercicios

[14] Disponible en: https://attack.mitre.org/

estructurados de emulación en una investigación interna llamada Fort Meade Experiment (FMX), ATT&CK presenta una base de conocimiento que modela el comportamiento de los adversarios. El proyecto ATT&CK ha evolucionado significativamente, abarcando tácticas, técnicas y procedimientos que preceden al ataque, y ampliándose para incluir dominios tecnológicos como sistemas Linux y MacOS, además de dispositivos móviles.

ATT&CK ofrece un modelo de comportamiento de adversarios con los siguientes componentes:

— Tácticas vinculadas a los adversarios. Dentro del framework ATT&CK, las tácticas se organizan en columnas que incluyen las siguientes opciones: acceso inicial, ejecución, persistencia, escalada de privilegios, evasión defensiva, acceso a credenciales, descubrimiento, movimiento lateral, recopilación, comando y control, exfiltración e impacto.
— Técnicas que posibilitan la realización de ejercicios prácticos basados en cada táctica. Dentro del framework ATT&CK, estas técnicas se representan en las celdas divididas por filas, agrupadas en cada columna correspondiente a la táctica asociada.
— Procedimientos en forma de documentos que recogen las técnicas individuales utilizadas por cada adversario.

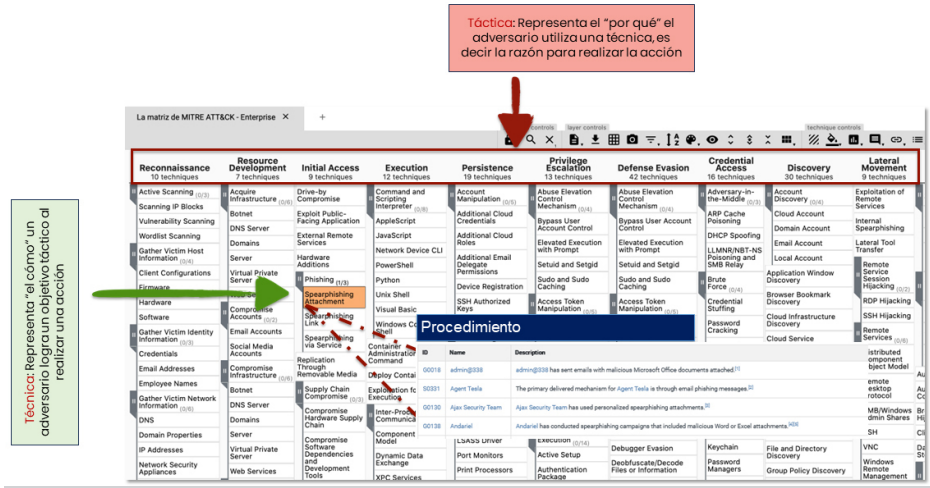

Figura 4. Representación de TTPs. Fuente: Elaboración propia

MITRE publicó en julio de 2018 un documento (Strom et *al.*, 2020) que explica el diseño y la filosofía desarrollada por MITRE ATT&CK. En su interior se describe el comportamiento en forma de TTP utilizados por los adversarios, además de proporcionar una taxonomía seguida tanto para el ataque como para la defensa. Marco muy utilizado por los analistas para analizar

información sobre amenazas, ya sea para defenderse de estas o simular ejercicios de *Red Team* aprovechando algún TTP de algún actor conocido.

3.6 *Cyber kill chain*

Los ataques perpetrados por adversarios están experimentando un aumento en escala, alcance, complejidad y frecuencia. En numerosas organizaciones, se implementan estrategias defensivas reactivas, lo que significa que solo se actúa en defensa cuando la amenaza ya ha ingresado a los sistemas internos. Por lo tanto, es crucial adoptar medidas proactivas para hacer frente a las amenazas más avanzadas y recientemente emergentes.

Predecir el comportamiento de un adversario no es tarea sencilla, lo cual dio origen a lo que se conoce como *kill chain*. Este modelo, creado por Lockheed Martin, ofrece una abstracción de la amenaza a lo largo de su ciclo de vida. La metodología de *kill chain* se centra en recopilar información de fuentes internas y externas relacionadas con una amenaza, con el objetivo de planificar estrategias proactivas para bloquear o analizar el comportamiento del adversario. Aunque múltiples actores y grupos criminales emplean este *kill chain*, la intención española en este caso es reaprovechar las mismas técnicas para simular un comportamiento similar al de un ataque real en los sistemas de la propia organización. A continuación, se describirán cada una de estas fases desde la perspectiva de un adversario, con el propósito de identificar posibles puntos de entrada a la organización.

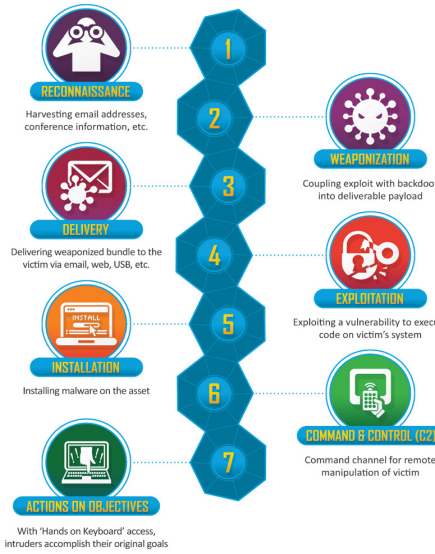

Figura 5. Fases del Cyber Kill Chain.
Fuente: Lockheed Martin

3.6.1 Reconocimiento

En esta fase inicial, el objetivo es recopilar información exhaustiva sobre posibles vulnerabilidades en la red y sistemas de la organización. Los puntos primordiales de acceso a una entidad son:

— Explorando servicios o tecnologías desactualizados que presenten vulnerabilidades desconocidas (0-day) en la infraestructura externa de la compañía, particularmente aquellos expuestos en internet.
— Accediendo desde dentro de la compañía mediante la colaboración de un insider.

En esta etapa, la ingeniería social adquiere una relevancia significativa, siendo una de las tácticas más empleadas para manipular a las víctimas y engañarlas con el objetivo de acceder a la red interna. En este contexto, resulta crucial recopilar información sobre todos los empleados potenciales de la organización e identificar un punto de entrada mediante una persona específica o un grupo de personas, según su perfil. En última instancia, el adversario busca responder a las siguientes preguntas:

¿Qué métodos de ataque funcionaran con el mayor grado de éxito? ¿Cuáles son los ataques más fáciles de ejecutar según los recursos que disponemos? Las medidas proactivas para esta fase incluyen:

— Realizar escaneos internos y externos regulares, así como ejercicios de Red Team, para descubrir vulnerabilidades y puntos de entrada no controlados en la organización.
— Utilizar motores de búsqueda para identificar información almacenada en caché que pueda representar una amenaza, especialmente en combinación con exploits específicos.
— Realizar búsquedas y análisis a través de la inteligencia de amenazas para descubrir credenciales, tarjetas de crédito, BINs, vulnerabilidades, código de software corporativo, información sobre directivos, fraudes, entre otros.
— Garantizar que los controles perimetrales y servicios expuestos a internet sigan el principio de mínimo privilegio y estén debidamente fortificados.
— Implementar honeypots para analizar la actividad maliciosa dirigida a la organización con el fin de detectar nuevos TTP.

3.6.2 Preparación

En esta etapa los adversarios analizan minuciosamente los datos recopilados sobre sus objetivos para determinar las técnicas de ataque más adecuadas. Planifican y desarrollan las estrategias necesarias basándose en la información obtenida en la fase anterior. Como vectores de ataque, pueden

prepararse diversas modalidades, como la creación de *malware* personalizado, aprovechando vulnerabilidades asociadas a los servicios expuestos en internet, la utilización de documentos ofimáticos con macros maliciosas o la explotación de vulnerabilidades 0-*day*, entre otros. Las medidas proactivas para esta fase son las siguientes:

- Mantenerse actualizado sobre las nuevas vulnerabilidades mediante el acceso a datos recientes sobre exploits utilizados para acceder a sistemas. Realizar la correlación de información sobre vulnerabilidades, comparándola con los sistemas internos de la organización para identificar aquellos que están afectados. Asimismo, es esencial priorizar la aplicación de parches o la implementación de medidas de mitigación en las vulnerabilidades que representen un mayor riesgo.
- Conducir investigaciones sobre amenazas inminentes, especialmente aquellas relacionadas con ataques dirigidos a organizaciones del mismo sector, mediante el análisis de fuentes sobre inteligencia de amenazas.
- Examinar y analizar TTP empleados por los adversarios, tanto contra la organización como contra otras entidades del mismo sector.

3.6.3 Entrega

El ataque previamente planificado y preparado en la fase anterior se ejecuta a través de la vía establecida para llevar a cabo la ofensiva. La entrega puede realizarse mediante un dispositivo USB, un archivo malicioso enviado mediante *phishing*, sitios web comprometidos, inyecciones en servicios web de la organización o en bases de datos, o aprovechando alguna vulnerabilidad detectada. Las medidas proactivas para esta fase son las siguientes:

- Disponer de firewalls que permitan controlar el tráfico de red incluyendo la detección avanzada de amenazas (ATD) como el sandboxing u otros métodos de detección de malware.
- Implementar medidas de seguridad en el servidor de correo electrónico mediante la aplicación de diversas técnicas de inspección de contenido malicioso.
- Contar con dispositivos y software específicos para prevenir ataques DDoS.
- Análisis de comportamiento de la red (NBA) y análisis de comportamiento de la entidad de usuario (UEBA) para detectar patrones de actividades maliciosas y sospechosas.
- Formación a los empleados para concienciar sobre las amenazas de Ingeniería Social y puedan identificarlas.
- Seguridad DNS.

3.6.4 Explotación

Después de distribuir al usuario, según lo planteado en la fase de preparación, con la entrega establecida para su correspondiente fase, la ejecución del ataque logrará su éxito comprometiendo así al objetivo. En esta etapa se logra la explotación de la vulnerabilidad planificada, lo cual posibilitará el acceso al sistema deseado dentro de la red de la organización. En este punto el atacante ya habría logrado infiltrarse en la organización. Las medidas proactivas para esta fase son las siguientes:

- Disponer de un SIEM que realice la correlación de eventos y registros provenientes de diversos elementos de seguridad, dispositivos e identidades de usuarios, con el objetivo de detectar posibles patrones y actividades maliciosas.
- Implementar dispositivos de prevención de amenazas, como firewalls, plataformas de protección de endpoints (EPP), sistemas de prevención de intrusiones de última generación (NGIPS) y soluciones de seguridad en el correo electrónico.
- Contar con un web application firewall (WAF) para prevenir posibles ataques a los sistemas web de la organización.
- Examinar APT conocidas y correlacionar TTP utilizados por estos, con el objetivo de detectar nuevas amenazas de este tipo.

3.6.5 Instalación

En esta etapa, se busca instalar un *backdoor* u otro tipo de *software* malicioso para lograr persistencia en la máquina víctima, permitiendo así el acceso remoto de manera sigilosa y sin levantar sospechas. Las medidas proactivas para esta fase son las siguientes:

- La implementación de una plataforma de protección de endpoints (EPP) puede contribuir a prevenir actividades maliciosas, garantizar la seguridad en el navegador y gestionar una lista blanca de aplicaciones.
- La utilización de una solución de detección y respuesta en endpoints (EDR) puede ser efectiva para la búsqueda proactiva de nuevas amenazas desconocidas y la detección de aquellas que aún no están presentes en los activos de la organización.
- A través del uso de un gestor de movilidad empresarial (EMM), es posible controlar y denegar la ejecución de aplicaciones no deseadas en los dispositivos gestionados por la organización, incluidos los dispositivos conocidos como BYOD[15]. El EMM evita que las aplica-

[15] *Bring your own device*. Utilizar el ordenador personal, pero de manera oficial y con control de la organización.

ciones instaladas por los usuarios accedan a datos confidenciales de la organización.
— La implementación de filtrado DNS, junto con el uso de listas blancas y la correlación de fuentes de inteligencia de amenazas, permite controlar que los dispositivos, tanto internos como externos, resuelvan las solicitudes DNS sin amenazas relacionadas.

3.6.6 Comando y Control (C&C)

En esta etapa, los adversarios han logrado el control de los activos dentro de la organización mediante métodos de control reconocidos, como DNS, ICMP, sitios web o redes sociales. A través de estos paneles de control, el adversario puede emitir órdenes para llevar a cabo operaciones en los activos comprometidos, desde recopilar contenido de la organización hasta obtener capturas de pantalla de los escritorios de los usuarios o robar credenciales. Las medidas proactivas para esta fase son las siguientes:

— Implementar herramientas con capacidades de filtrado de reputación por DNS e IP, herramientas forenses, firewalls, IPS, entre otros.
— Ofrecer seguridad DNS con capacidades de inteligencia de amenazas para bloquear resoluciones DNS de hosts maliciosos que intenten comunicarse con los DNS de la organización. Es recomendable que los registros de las actividades realizadas por los servidores de DNS se analicen mediante un SIEM.
— Monitorizar la red utilizando datos de flujo de red, como NetFlow, para detectar comportamientos anómalos.
— Contar con un SIEM que integre múltiples fuentes de inteligencia de amenazas para detectar comportamientos y actividades maliciosas dentro de la red interna de la organización o conexiones hacia el exterior.

3.6.7 Objetivos de la acción

En esta etapa, se materializa el propósito original del ataque, ya sea la extracción de información o el daño a los activos de la organización. La duración del acceso al mando y control influye directamente en la magnitud del impacto, siendo mayor a medida que el adversario mantiene un acceso prolongado.

Las medidas proactivas para esta fase son las siguientes:

— Para prevenir la actividad de exfiltración de información, es crucial contar con características específicas en el SIEM, UEBA o software de prevención de pérdida de datos (DLP) que salvaguarden la información confidencial, evitando su salida de la organización incluso cuando un activo ha sido comprometido.

— Analizar el comportamiento de la red, identificando dispositivos que exhiban actividades inusuales, como la generación de tráfico con un volumen excesivo de solicitudes DNS hacia un DNS externo, o protocolos que estén activos, pero no funcionen correctamente, según las políticas internas establecidas
— Implementar firewalls de próxima generación (NGFW) e IPS que puedan identificar actividades maliciosas de usuarios con permisos para ejecutar ciertas aplicaciones, pero que las utilicen de manera no convencional o inapropiada.

4 Ecosistema tecnológico para la inteligencia de amenazas

Para gestionar de manera efectiva la información sobre amenazas, resulta fundamental contar con un ecosistema tecnológico bien integrado y comunicado. Cada componente tecnológico en este entorno debe cumplir una función específica y contribuir de manera coordinada al conjunto. En este sentido, la presencia tanto de un SIEM como de una plataforma de inteligencia de amenazas se vuelve crucial. A continuación, se enumeran diversas tecnologías y plataformas que pueden implementarse para llevar a cabo la monitorización de todos los dispositivos conectados a la red, tanto interna como externa de la organización, estableciendo políticas eficientes de detección y respuesta ante amenazas.

4.1 SIEM

Este sistema de seguridad tiene como objetivo proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza que pueda afectar a sus sistemas informáticos.

Las funciones principales del SIEM comprenden el almacenamiento e interpretación de registros, llevadas a cabo en tiempo real para garantizar una respuesta eficiente ante incidentes de seguridad. Este sistema centraliza toda la información en una base de datos, posibilitando un análisis exhaustivo para identificar tendencias y patrones de comportamiento, distinguiendo aquellos que no son habituales. Las alertas generadas por el SIEM se transmiten al SOAR[16] para su enriquecimiento con otros sistemas en una etapa posterior.

Mantener un catálogo de alertas de correlación resulta crucial, permitiéndolo evolucionar constantemente gracias a la colaboración entre las diversas áreas del SOC. Estas áreas contribuyen con información sobre

[16] SOAR engloba un conjunto de servicios y herramientas diseñados para automatizar la prevención y respuesta ante ciberataques. Se ve en mayor detalle en el punto 4.3 del documento.

nuevas tendencias de ataques, vulnerabilidades, grupos de atacantes, IOCs, entre otros aspectos relevantes.

Es importante destacar que todas las reglas, como por ejemplo SIGMA[17], se construyen en un lenguaje agnóstico[18] respecto a la tecnología SIEM. Esto se hace para evitar la necesidad de reconstruir las reglas en caso de utilizar otro fabricante. El catálogo de reglas de correlación se integra con la plataforma de inteligencia de amenazas para mantener actualizados los enriquecimientos de datos sobre IOC.

4.2 Plataformas de inteligencia de amenazas

Centralizar y contextualizar los datos recopilados de diversas fuentes y herramientas en un repositorio compartido es esencial para cualquier organización. Esta consolidación de información permite realizar investigaciones proactivas sobre amenazas, proporcionando una visión integral de datos relacionados con actores y grupos criminales vinculados a los indicadores de compromiso (IoC). Este enfoque facilita la detección de patrones utilizados por dichos actores, fortaleciendo así la capacidad de defensa ante posibles amenazas futuras.

Una plataforma de inteligencia de amenazas representa una herramienta tecnológica que permite a las organizaciones recopilar, correlacionar y analizar datos sobre amenazas provenientes de diversas fuentes, tanto internas como externas, en tiempo real. Su función principal es fortalecer las defensas contra actividades maliciosas. Esta plataforma centraliza y enriquece los datos, facilitando la comunicación con sistemas como el SIEM y otros dispositivos perimetrales de seguridad para detectar patrones maliciosos.

Las plataformas de inteligencia de amenazas más ampliamente utilizadas en la actualidad son MISP y OpenCTI. A continuación, se proporcionará una descripción detallada de ambas.

4.2.1 MISP

Es una plataforma diseñada para la recopilación, compartición y correlación de Indicadores de Compromiso (IoC) relacionados con ataques

[17] Formato que simplifica la descripción de eventos sobre actividad maliciosa en base a su comportamiento. El principal objetivo de SIGMA es ofrecer una forma estructurada para que los profesionales describan sus métodos de detección y los compartan con otros, facilitando así la colaboración y el intercambio de conocimientos en el campo de la ciberseguridad.

[18] El objetivo principal del lenguaje agnóstico es escribir código o desarrollar soluciones que no dependan de una tecnología específica, lo que permite que el *software* sea más flexible, escalable y fácil de mantener a lo largo del tiempo.

dirigidos, APT, información de fraude financiero, vulnerabilidades y antiterrorismo, entre otras amenazas. Esta herramienta facilita el análisis de un indicador específico y revela cómo se relaciona con otros, proporcionando así una visión global de un ataque al vincular IoC entre sí. Además, MISP posibilita el análisis de eventos y amenazas, como identificar qué actores pueden estar vinculados a un ataque particular o qué TTP podría estar utilizando un grupo criminal. Algunas de las características principales incluyen:

- Cuenta con una base de datos de indicadores que posibilita almacenar información técnica y no técnica relacionada con muestras de malware, incidentes y actores, además de ofrecer una contextualización detallada.
- Ofrece correlación automática entre atributos e indicadores de malware, campañas de ataques o TTP, facilitando la identificación de patrones y relaciones entre diferentes elementos.
- Dispone de un modelo de datos flexible en el que se pueden enlazar objetos complejos para expresar información sobre amenazas, incidentes o elementos conectados.
- Cuenta con una funcionalidad que permite la compartición de datos, utilizando diferentes modelos de distribución. MISP puede sincronizar automáticamente eventos y atributos entre diferentes instancias.
- Facilita el intercambio y sincronización automática con otros grupos de confianza mediante MISP.
- Herramienta flexible para integrar fuentes de cualquier amenaza o mediante fuentes públicas.
- API flexible que permite la integración de MISP con otras soluciones. Utilizando la librería de Python, PyMISP, puedes recuperar, añadir o actualizar atributos de eventos, gestionar muestras de malware y buscar atributos de manera eficiente.

MISP cuenta con una taxonomía adaptable que permite la clasificación y etiquetado de eventos mediante esquemas de clasificación propios o taxonomías existentes. Esta taxonomía puede ser local para la instancia de MISP en cuestión, pero también puede ser compartida con otras instancias. La herramienta incluye un conjunto predeterminado de taxonomías y esquemas de clasificación reconocidos para respaldar la clasificación estándar utilizada por organizaciones como ENISA, Europol, DHS, CSIRT, entre otras.

Por otro lado, MISP emplea un diccionario denominado galaxias que contiene palabras clave relacionadas con la inteligencia. Este enfoque permite agrupar y vincular eventos o sucesos con actores de amenazas, *malware*, RAT, ransomware o el marco MITRE ATT&CK.

MISP es la plataforma líder en inteligencia de amenazas, siendo ampliamente adoptada por los principales Centros de Operaciones de Seguridad (SOC) a nivel mundial mediante sistemas federados para el intercambio de información sobre amenazas. En España, por ejemplo, se cuenta con la Red Nacional de SOC (RNS), establecida y dirigida por el CCN-CERT, donde entidades públicas, proveedoras e invitadas colaboran en el intercambio de información sobre amenazas con el objetivo de fortalecer las capacidades de protección de sus miembros dentro del ámbito español.

4.2.2 OpenCTI

Es una plataforma de código abierto diseñada para que las organizaciones gestionen su inteligencia de amenazas. Su propósito es estructurar, almacenar, organizar y visualizar información tanto técnica como no técnica relacionada con las ciberamenazas.

En OpenCTI los datos se organizan según el estándar STIX2, un lenguaje estandarizado para estructurar la información sobre amenazas. STIX2 tiene como objetivo facilitar el intercambio de información de inteligencia de amenazas entre organizaciones, con la finalidad de crear un conocimiento compartido sobre amenazas. Esto capacita a la comunidad para detectar y responder de manera más rápida y eficiente ante posibles amenazas con un estándar común. Además, facilita la integración de herramientas y conjuntos de datos como por ejemplo MISP y MITRE ATT&CK.

Además, OpenCTI brinda la capacidad de centralizar todo el conocimiento relacionado con las investigaciones de amenazas realizadas internamente. Si una investigación resulta relevante, se puede conectar con la plataforma MISP para transformar dicha investigación en un evento que pueda compartirse con organizaciones externas con las que esté sincronizado, como la Red Nacional de SOCs (RNS), por ejemplo.

Finalmente, esta plataforma ofrece la capacidad de contar con un repositorio para almacenar internamente el conocimiento adquirido a través de investigaciones sobre *malware*, ransomware, APT, así como mantener una base de datos relacionada con herramientas, *malware*, TTP y actores de amenazas vinculados a las investigaciones realizadas. Este conocimiento aporta valor al desarrollo de casos de uso, reglas de detección y *playbooks* que pueden ser utilizados en la detección y respuesta de incidentes.

4.3 SOAR

Engloba un conjunto integral de servicios y herramientas diseñadas para automatizar y optimizar tanto la prevención como la respuesta a ciberataques. Este enfoque implica la unificación de integraciones, la definición de

procesos para la ejecución de tareas y la creación de un plan de respuesta a incidentes adaptado a las necesidades específicas de la organización. La automatización simplifica la ejecución de tareas de seguridad, mientras que la orquestación conecta de manera eficiente diversas herramientas para lograr una respuesta coordinada y efectiva.

Las integraciones que se desarrollen pueden contar con la capacidad de bloquear amenazas identificadas y verificadas en los *firewalls* mediante diversas fuentes de información. Esto establece una sinergia efectiva entre el intercambio de inteligencia de amenazas de MISP y la implementación de medidas de seguridad reactivas y proactivas a través de sus integraciones. Esta colaboración entre ambos componentes de SOAR contribuye a formar un sistema más cohesionado, maximizando la eficacia desde el principio hasta el final.

Además, el SOAR tiene la capacidad de orquestar y automatizar no solo alertas de SIEM y EDR, sino también tareas relacionadas con sistemas de gestión de vulnerabilidades, indicadores de compromiso, TTP, y diversas funciones adicionales.

5 Conclusión

Es fundamental comprender las necesidades de información específicas del decisor, ya sea un cliente, jefe o alguien que busca ayuda, y ajustarlas a su contexto. La inteligencia debe estar orientada al destinatario, ya sea a nivel estratégico, táctico u operativo, alineándose con los cinco objetivos clave de un producto de inteligencia: ser oportuno, preciso, procesable, relevante y predictivo.

Es crucial seleccionar, adaptar y aplicar las técnicas de análisis de inteligencia más adecuadas para cubrir las necesidades de información identificadas. Esto implica un conocimiento profundo de las amenazas dirigidas al sector y al país en el que operan los adversarios, siendo ideal contar con un panorama de amenazas adaptado a cada organización.

Para una defensa efectiva, es esencial comprender al adversario en todos los niveles, analizando a fondo las tácticas, técnicas y procedimientos que emplean. Además, se recomienda elaborar escenarios de ataque realistas que se adapten a las características únicas de cada negocio, teniendo en cuenta las amenazas más actuales y peligrosas.

Para concluir, es esencial contar con un ecosistema tecnológico apropiado y trabajar en el desarrollo de madurez en términos de procesos, procedimientos, así como capacidades técnicas y analíticas de los analistas. Además, la automatización de *playbooks* específicos sobre amenazas desempeña un papel crucial en este proceso para evolucionar como SOC.

Bibliografía

Computer Security Resource Center. (2012). *Computer Security Incident Handling Guide* [en línea]. National Institute of Standards and Technology. [Consulta: 2024]. Disponible en: https://csrc.nist.gov/pubs/sp/800/61/r2/final.

Díaz *et al*. (2013). *Diccionario LID Inteligencia y Seguridad*. España, LID Editorial Empresarial. 329. Colección Diccionarios LID. ISBN: 978-84-8356-760-9.

European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023* [en línea]. [Consulta: 25 de febrero de 2024]. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Guerra Soto, M. (2023). *Ciberinteligencia de la amenaza en entornos corporativos*. Madrid, Ra-Ma. 773. ISBN: 978-84-19857-45-3.

Johnson, C. *et al*. (2016). *Guide to Cyber Threat Information Sharing* [en línea]. *National Institute of Standards and Technology*. [Consulta: 2024]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

Strom, B. E. *et al*. (2020). MITRE ATT&CK: Design and Philosophy [en línea]. *MITRE*. [Consulta: 2024]. Disponible en: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

Enigmas o misterios, cuando la amenaza está en la interpretación (centrada en el escenario del Sahel)

David Cuesta Vallina

Resumen

Fue en 2009, cuando un experto en política exterior e inteligencia, Gregory F. Treverton, que estuvo al frente del Consejo de Seguridad Nacional *(National Security Council* o NSC), directamente dependiente del presidente de los Estados Unidos, cuestionó la estructura de los órganos de inteligencia, partiendo de unos conceptos tanto simples como abstractos. Su solución, organizar los problemas de inteligencia con un enfoque desde los enigmas o desde los misterios.

El Sahel, organización regional que en sus inicios contaba con Burkina Faso, Chad, Malí, Mauritania y Níger, comprende una de las regiones más inestables del planeta y representa una fuente de amenazas latente para el entorno europeo. Desde una perspectiva de enigmas y misterios se pretende progresar en el entendimiento de la situación actual, con una diferenciación conceptual que puede ser interesante para la resolución de problemas y reducir la permanente incertidumbre.

Palabras clave

Inteligencia, Enigma, Pensamiento, Misterio, Sahel.

Enigmas or mysteries, when the threat is in the interpretation (focused in the scenario of the Sahel)

Abstract

In 2009, Gregory F. Treverton, an intelligence expert who headed the National Security Council (NSC) that reports directly to the president of the United States, questioned the structure of the security and intelligence national organizations based on both simple and abstract concepts. Its solution is to reorganize intelligence problems with a focus on enigmas or mysteries.

The Sahel, a regional organization that included Burkina Faso, Chad, Mali, Mauritania and Niger, comprises one of the most unstable regions on the planet. From a perspective of enigmas and mysteries, the aim

is to progress in understanding the current situation, with a conceptual differentiation that can be interesting for solving problems and reducing permanent uncertainty.

Keywords

Intelligence, Enigma, Thinking, Mystery, Sahel.

1 Ajustando el enfoque

Tras los atentados del 11 de septiembre de 2001, Osama Bin Laden fue considerado la principal amenaza para el mundo, lo que derivó en la realización muchos esfuerzos de la comunidad de inteligencia para lograr su búsqueda y captura. Además de convertirse en un nuevo enemigo público, el paradero del jefe de Al-Qaeda fue considerado como un enigma, no se le podía encontrar porque no se disponía de suficiente información.

Poco después, en 2003, en el escenario iraquí, las fuerzas de la coalición disponían de mucha información de todo tipo, se estaba en el terreno, pero saber lo que pasaría tras la derrota del dictador chiita Sadam Hussein no resultaba fácil, se trataba de todo un misterio, todo el mundo tenía una visión justificada y fundamentada basada en infinidad de fuentes, las valoraciones crecían sin parar con protagonistas de la CIA, de expertos en inteligencia o incluso el tertuliano de turno.

Fue Gregory Treverton[1], quien, en 2009, realizó una distinción formal entre enigmas y misterios que posteriormente ha sido empleada como referencia para tratar aspectos organizativos en los sistemas de inteligencia y en el modo de tratar las necesidades informativas frente a nuevas amenazas. Esta distinción fue cuestionada, pero con el tiempo llevó a modificar la estructura de determinados servicios y quizá permita aportar una perspectiva diferente sobre las nuevas amenazas a la Seguridad Nacional, los enigmas y misterios podrían ayudar a comprender, a pensar, puesto que con la realidad actual ya no es suficiente informarse.

Para resolver la primera situación, el enigma, se recomendaba esperar a tener una fuente cercana al propio Ben Laden, había que esperar, la paciencia era clave, frente a esta situación, aumentar los servicios de inteligencia era parte de la solución que acabaría por llegar. La segunda situación, el misterio, requería de un buen juicio y análisis, pero la incertidumbre siempre estaría presente, la respuesta a la pregunta sobre qué pasaría después, no era simple o incluso podría no llegar.

Para el enigma los esfuerzos realizados pueden llevar a encontrar una respuesta concreta, es lo que buscan los servicios de inteligencia. En el misterio la cosa se complica, no se puede encontrar una respuesta definitiva, aunque si se podría tener una aproximación basándose en determinados indicadores.

En el Sahel, considerada una de las zonas geográficas más particulares del planeta, contemplar el problema desde una perspectiva de enigmas o misterios, puede hacer pensar, más si está en juego parte de la credibilidad

[1] El experto en Seguridad Nacional norteamericana y autor del libro *Intelligence for an Age of Terror*, publicado por Cambridge University Press.

de la Unión Europea y se mantienen fuerzas desplegadas allí. Ante un enigma, se podrían aumentar los esfuerzos de inteligencia, desplegar elementos de obtención e incrementar la cantidad de información. Por el contrario, si se considera como un misterio será más beneficioso mejorar el análisis profundo dentro de la comunidad inteligencia, asegurar la calidad de la información, los lazos y las relaciones adquieren especial valor para comprender.

2 Un escenario particular, una amenaza real

Si se dice que nueve de los diez últimos golpes de Estado sucedidos en el mundo, y que hayan obtenido cierto éxito, se han originado en África se puede aceptar que se está hablando de un continente inestable, además de ser el más pobre del planeta[2]. En la misma línea, cuando se habla del Sahel, palabra de origen árabe que significa «costa» o «borde», es fácil encontrar referencias con enfoque negativo que aumentan la imagen de desastre que se vive en esta zona geográfica: «una tormenta perfecta[3]», «el cinturón africano de la miseria[4]» o un «cóctel de problemas[5]».

En febrero de 2014, los mandatarios de cinco países de la región se reunían para formar una nueva organización, denominada el G5 Sahel. En los inicios de esa alianza, el presidente mauritano Abdel Aziz decía «no hay un desarrollo duradero sin seguridad ni una seguridad perdurable sin un desarrollo efectivo». Con los países del Sahel Occidental —Mauritania, Malí, Burkina Faso, Níger y Chad[6]— se promovían medidas para asegurar la zona y evitar la inestabilidad regional, todo un reto para una región que comprende tanta inestabilidad, violencia o diversidad que de alguna manera suponen la convivencia de enigmas y misterios.

La falta de una solución internacional eficaz tras la finalización de la guerra en Libia, ha producido la aparición de numerosas variables, desde el extremismo político o religioso al cambio climático, desde la lucha por los recursos naturales al crimen organizado o terrorismo, todo un coctel de amenazas que hacen muy complejo cualquier análisis de inteligencia o previsión. Todos pueden encontrar argumentos para justificar su visión, la Unión Europa para retirarse de Malí y buscar otro país cercano para

[2] Disponible en: https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEOWORLD

[3] Véase: https://www.europapress.es/internacional/noticia-ue-habla-tormenta-perfecta-sahel-dice-region-parte-poligono-crisis-20201018093035.html

[4] Disponible en: https://www.consumer.es/solidaridad/sahel-el-cinturon-del-hambre-africano.html

[5] Véase en: https://www.cubahora.cu/del-mundo/el-sahel-bajo-amenaza

[6] Malí se retiró de este grupo en 2022. Disponible en: https://www.jeuneafrique.com/1346607/politique/le-mali-se-retire-du-g5-sahel/

mantener su influencia, la Unión Africana para aplicar medidas favorables a unos y de castigo a otros, o los propios países de la región que buscan abrir alianzas para asegurar su supervivencia mientras las amenazas como el yihadismo[7] o el crimen organizado siguen al alza al no conocer fronteras.

Si bien estos factores están presentes, los países sahelianos siguen trayectorias políticas distintas, parece que el mundo de las certezas está quedando atrás en el mundo de las nuevas amenazas, lo que aumenta la incertidumbre y la posibilidad de aparición de enigmas y misterios que pueden tener su eco en Europa.

3 Un enfoque geográfico

El Sahel, como zona geográfica del norte del continente africano que se extiende desde el océano Atlántico hasta el mar Rojo, representa una zona de transición entre el desierto del Sahara y la sabana sudanesa al sur. En esas extensiones de terreno, aparecen fronteras caracterizadas por un diseño humano que podrían recordar al empleo de escuadra y cartabón, y donde algunas podrían pasar incluso por ilógicas. La historia ha mostrado que una frontera establecida por el hombre, que no corresponde con una zona fronteriza natural, es especialmente vulnerable.

El auge colonialista que se estaba viviendo en África, se sofocó en parte por el papel de Bismarck y la Conferencia de Berlín en 1884. Se establecía de alguna manera unos límites para la adquisición de territorio[8]. Poco después, se acordó la distribución de la tarta territorial africana con unas fronteras que permanecieron prácticamente inamovibles durante décadas, limitándose a algunos cambios en las dependencias producidas por las dos guerras mundiales. Las posesiones alemanas eran repartidas entre Francia, Reino Unido y la, por aquel entonces, Unión Sudafricana. Fue en 1963, con la creación de la Organización para la Unidad Africana (OUA), que los estados africanos independientes de ese momento decidieron respetar las fronteras heredadas aunque permanecía la ambición de muchos líderes en promover la unificación y el panafricanismo superando ese diseño artificial de fronteras[9]; la solución africana tampoco parecía firme y había diferentes visiones.

La realidad es que pocos países en esta región tienen fronteras estables, lo normal es tener unos límites discutidos o desconocidos entre la población por su falta de utilidad, lo que ha favorecido disputas y descontrol,

[7] Véase: https://elordenmundial.com/boko-haram-de-la-predicacion-al-terrorismo/

[8] Se mantuvo una perspectiva europea al no participar los dos únicos países africanos independientes, Liberia y Abisinia.

[9] Disponible en: https://elordenmundial.com/los-caprichos-fronterizos-de-africa/

facilitando que transiten con impunidad toda clase de actividades ilícitas[10]. Para comprender la situación de lo que supone esta amenaza, se hace necesario el conocimiento de la historia, evitando la tendencia a simplificar en exceso. La dificultad de encontrar respuestas definitivas se mantiene porque cuesta comprender las interrelaciones y lo complejo predispone a rechazar lo que no confirma las creencias derivadas del pensamiento lineal o de lo aceptado en la visión occidental, de hecho, el pensamiento grupal es una de las raíces de los fallos de inteligencia ante la interpretación de nuevas amenazas.

Es la combinación del aspecto geográfico definido por el hombre, la aparición de estados independientes y el efecto de la historia de los países del Sahel, que propician la formación de enigmas para la población. Los límites fronterizos existen, aunque podrían no influir de forma determinante en la población que no las siente como suyas.

4 Factor demográfico

Cuando se observan las pirámides de población de estos países africanos se puede apreciar que difieren en su forma a las europeas. Además de reflejar un crecimiento demográfico explosivo, están caracterizadas por tener una base ancha, lo que se traduce en una población joven muy numerosa que, además, sigue creciendo por encima de las medias mundiales. La región del Sahel es considerada como una de las más jóvenes del planeta, ya que según Naciones Unidas, el 64,5 % de la población es menor de veinticinco años.

Los índices demográficos son de los más altos del mundo, Malí o Níger presentan excepcionales tasas de fertilidad, con una media de siete hijos por mujer que les lleva a una población extremadamente joven (quince años de media), que unido a las dificultades educativas generalizadas, favorece el crecimiento del analfabetismo en toda la región.

Esa población joven, unido a una cultura arraigada en el comercio e intercambio como forma de vida, facilita que las personas tengan diferentes ocupaciones y no las mantengan por periodos prolongados, no existe una fuerte división del trabajo como en la sociedad europea y existe cierta pasión por ese comercio que les ha hecho mantener reinos saheliano de gran influencia durante siglos. Esta demografía, combinada con su geografía ha ayudado a generar un estilo de vida que recorre toda la franja del Sahel, con la agricultura y ganadería como complemento de esa cultura del comercio.

[10] *Documento de Trabajo 05/2018*. La estabilidad en el Sahel. Un análisis prospectivo, pp. 17.

Las tendencias pueden fortalecer las previsiones, pero el enigma poblacional se mantiene y, en determinados escenarios, supone incluso una amenaza, ya que el largo plazo siempre está sometido a la incertidumbre y a la volatilidad propia de los entornos de hoy. Además, hoy no se puede descartar la aparición de los conocidos «cisnes negros», que pueden afectar a la percepción de la amenaza como se aprendió con el COVID-19, y que hacen más difícil la comprensión del problema.

Las métricas y estadísticas pueden aclarar indicadores, son útiles para resolver el enigma que suponen las tendencias poblacionales en el corto plazo, pero los índices elevados de desplazamientos internos, la emigración como salida para buscar oportunidades, favorecen esos flujos migratorios donde las expectativas para la juventud son muy limitadas. Está claro que descifrar el enigma del largo plazo no es tarea fácil para la comunidad de inteligencia, incluso la recomendación es aceptar las limitaciones en las prospectivas y tratar el problema poblacional o como un misterio, pero lo importante es tener la sensibilización de la amenaza que podría suponer si se deja a la sorpresa.

5 El terrorismo

Si hasta 2012, Malí era considerada como el «paradigma de la democracia y la estabilidad política» del Sahel Occidental, poco después, las previsiones ya no se daban por válidas y una serie de acciones terroristas provocaron una falta de control físico del país, por parte de los gobiernos establecidos, facilitando ser el epicentro del yihadismo de toda la región y la amenaza principal.

Los Acuerdos de Argel de 2015, como solución acordada enfocada a Malí, pero con influencia en toda la zona, han sido sobrepasados por un aumento de las acciones terroristas y por el número creciente de actores, ya que la violencia yihadista no es la única con influencia en la región. Los choques intercomunitarios, la insurgencia, Al-Qaeda y sus filiales o incluso la presencia del Estado Islámico, forman parte de esas búsquedas de poder constantes que sufren los distintos países caracterizados por la inestabilidad. El JNIM[11] (la filial de Al-Qaeda en Mali) ha conseguido realizar varios atentados con cierto éxito; los míticos tuaregs, que ocupan una zona que transcurre por Malí, Argelia, Libia, Níger, Chad y Nigeria, han sido capaces de retar seriamente al gobierno de Bamako; el puzle se complica, la interpretación de la amenaza se hace más compleja que nunca.

La expansión de los grupos yihadistas ha llegado hasta Burkina Faso y otros grupos como Boko Haram, suníes radicales, ocupan titulares en

[11] El grupo Jamaat Nusrat al Islam wal-Muslimin, se concentra en Mali pero también opera en Burkina Faso y en Níger, se instituyó en marzo de 2017.

las noticias por la brutalidad de sus acciones. Su acción más conocida, el ataque en 2014, cuando secuestraron a 276 niñas en la ciudad de Chibok y que tuvo su repercusión mediática a través del #bringbackourgirls[12]; la información crece exponencialmente.

Si hay un tema que ha mostrado la dificultad en realizar predicciones, es el ámbito de las amenazas y principalmente en lo referido al terrorismo. Esto lleva al misterio que supone el terrorismo, el factor cuantitativo ya no es suficiente. Aunque las estadísticas atraen porque simplifican las cosas y facilitan encontrar atajos que el cerebro busca para conseguir una solución rápida y satisfactoria, en la actualidad compleja se hace necesario algo más. La época de resolver misterios con fórmulas matemáticas, como las empleadas para calcular la capacidad de combate sumando número de divisiones, carros o misiles, ha pasado. Hoy las capacidades de los grupos terroristas son más complejas y asimétricas, los apoyos globales, las técnicas innovadoras, el trasfondo religioso, asociar sus acciones a misterios puede ayudar a interpretar la amenaza con sus complejas interrelaciones y carácter global.

6 El cambio climático

Hace pocos años, en 2020, la primera localidad considerada víctima por el cambio climático fue Beria[13], en el continente africano, en Mozambique, donde, bajo los efectos del ciclón Idai, quedó arrasado más de un 90 % de su territorio. También existe la comparativa de la superficie de agua existente en el lago Chad[14] en 1964 y en la actualidad, donde se calcula una reducción de más de 10 000 km^2, en una zona que reúne el 75 % de la población y donde la vida depende del, cada vez más escaso, recurso natural que es el agua.

ACNUR estima que el 80 % de los cultivos en el Sahel están afectados por elementos del cambio climático, una amenaza ya real que en el Sahara tiene una gran repercusión[15], afectando directamente a las zonas agrícolas de Sudán, Chad y Mauritania. Burkina Faso ha perdido en los últimos diez años casi el 20 % de su territorio fértil por los efectos de la deforestación, aunque sus consecuencias son difíciles de ver en el corto plazo.

Cuando en 2021 la Real Academia Sueca de Ciencias hizo entrega del Premio Nobel de Física expertos en la modelización física del cambio

[12] Véase: https://www.fidh.org/es/temas/derechos-de-las-mujeres/bringbackourgirls-las-escolares-secuestradas-por-boko-haram-siguen
[13] Disponible en: https://ipsnoticias.net/2019/04/primera-ciudad-destruida-cambio-climatico-mozambique/
[14] Véase: https://www.bbc.com/mundo/noticias-internacional-43206097
[15] Disponible en: https://www.publico.es/internacional/superficie-del-desierto-del-sahara.html

climático[16] se reconocía sus contribuciones para comprender mejor los sistemas físicos complejos, se abría un poco de luz al que podría ser el enigma climático. Entre los premiados, un meteorólogo en la Universidad de Princeton que destacaba la idea de que el clima es un sistema extremadamente difícil de comprender, pero se podría mejorar en las predicciones climáticas y ambientales. Aunque se estudian ciclos climáticos, patrones de circulación de la atmósfera, tendencias de temperatura… falta tecnología para conocer cuál será su influencia neta en un futuro próximo, la incertidumbre se mantiene a igual que el misterio de la amenaza climática perdura.

7 Golpes de Estado

Si antes se mencionan que los golpes de Estado se han centrado en África, más aún en la zona del Sahel, son muchos las informaciones que hay. Al menos cinco acciones de este tipo han conseguido su objetivo: Chad (2021), Mali (2020, 2021) y Burkina Faso (enero y septiembre de 2022), aunque seguramente hay otros golpes de Estado que no han conseguido su objetivo, como el de Níger en 2021, por lo que es probable que la amenaza sea mayor considerando los golpes fallidos. Sí que se percibe un cierto gusto por los golpes de Estado[17] y rebeliones en esta región, sin olvidar el interés mostrado por los tuareg para desestabilizar los gobiernos de Bamako y Niamey que dejan un escenario de incertidumbre.

La desconfianza ha crecido de forma general en todo el Sahel, con una clara inestabilidad política que unido al estrecho margen de error ha popularizado la solución del «golpe de estado» que se ve como solución rápida para mejorar la situación en una sociedad que prioriza la justicia y seguridad a su manera.

Se producen también similitudes entre países diferentes, Burkina parece que tiene un efecto diferido respecto en Malí, como ocurre con su gobierno fruto de un golpe de Estado posterior al maliense, o con la presencia yihadista que entró a los pocos años de entrar en Malí o donde las tropas francesas fueron expulsadas también meses más tarde.

Las similitudes pueden hacer pensar que se habla de un enigma y sirven para creer en lo que confirma la propia línea de acción, si bien en esta región se ha visto que la misma causa puede dar resultados diferentes.

Las prospectivas de los golpes de Estado promueven el misterio, ya que se habla de una región donde los modelos de un país no pueden ser

[16] Syukuro Manabe, Klaus Hasselmann y Giorgio Parisi.
[17] Véase: https://www.larazon.es/internacional/20221229/l77uagdtm5f2vh3kuym3l6cr7i.html

exportados a otra situación similar y hacerlo supondría una simplificación excesiva que llevaría a sesgos y errores de interpretación. Se requiere juicios y evaluación de la incertidumbre, considerando todos los datos, el factor psicológico influye y requiere de unos análisis profundos solo al alcance de una comunidad de inteligencia sensible y dedicada.

8 Conclusiones misteriosas o enigmáticas

«Es un acertijo, envuelto en un misterio, dentro de un enigma, pero quizá haya una clave. La clave es el interés nacional de Rusia» (Churchill).

La frase de Churchill, emitida en un programa de radio de 1939, refleja ya un matiz revelador de la interpretación dual de enigma y misterio. No todos los problemas pueden ser clasificados de forma clara desde uno u otro punto de vista, incluso alguno podría ser las dos cosas a la vez, según quien lo enfoque. Un enigma, para los Estados Unidos, con un despliegue descomunal de servicios de inteligencia en un escenario dado, podría ser, al mismo tiempo, un misterio para la Unión Europea, únicamente solucionable con una comunidad de inteligencia colaborativa y con un propósito común frente a la amenaza.

En un continente que es más grande que Europa, China y los Estados Unidos juntos, una región, como la del Sahel, que podría ocupar una mayor atención mediática[18] de la que tiene en la actualidad, presenta una combinación de enigmas y misterios que no hacen fácil la comprensión de los diferentes caminos que está viviendo África hacia la modernización. Con cobertura mediática o no, la relevancia estratégica del Sahel aumentará en las próximas décadas debido, entre otras cosas, a la explosión demográfica, los nuevos actores internacionales como China y Rusia o la necesidad creciente de los recursos naturales por parte de las potencias mundiales.

Las amenazas existen pero existe la dificultad de llegar a «comprender», debido a la complejidad de la región, la ausencia de patrones realistas y la falta de solución clara que tienen los misterios como parte inherente a los nuevos entornos[19].

Resulta importante dar respuestas a las preguntas, por ello se han creado variables e indicadores que facilitan la comprensión y ayudan a entender las pistas que se detectan. De forma inconsciente se trata de dar forma a los misterios, pero los misterios son misterios, no se van a resolver con el conocimiento de hoy. Los países y organizaciones invierten para resolver los enigmas, pero, generalmente, falta tener la información suficiente, es

[18] Disponible en: https://elpais.com/planeta-futuro/2022-06-29/una-exposicion-contra-el-abandono-del-sahel-el-silencio-y-el-olvido-matan.html

[19] Véase: https://www.leadershipcentre.org.uk/artofchangemaking/theory/complexity/

aceptar la realidad, las limitaciones, y adoptar una perspectiva de los misterios y tratarlos como tal.

Frente a las nuevas amenazas se mantendrá necesario el trabajo de los analistas de inteligencia, sacando conclusiones de las declaraciones, prensa, fuentes, contrastando… pero con los misterios se tendrán que seguir revisando las conclusiones, no habrá una causa única, se tendrá que aprender a tener preguntas sin respuesta y a modificar los juicios de inteligencia, el mundo de las certezas ha quedado atrás. El progreso está en saber pensar más sobre las causas y centrarse menos en las recurrentes estadísticas que, aunque son más fáciles de conseguir, pueden llevar a aumentar el distanciamiento con la realidad. Las amenazas de hoy requieren saber moverse de una organización nacida con un enfoque para resolver enigmas como los propios de la Guerra Fría, a hacer lo necesario para sentirse cómodos frente a los misterios.

Los métodos para resolver los enigmas, en esa lucha por tener información de primera mano, realza el valor clásico de la inteligencia humana, fuentes fiables, compartir información, métodos que requieren de presencia en el terreno, compromiso, energía y persistencia, precisamente virtudes cercanas a la juventud. Al enfrentar los misterios los perfiles cambian y la experiencia y perspicacia adquieren especial valor junto esa mentalidad abierta de aceptar diferentes puntos de vista. El Sahel es un reto, la mezcla de enigmas y misterios obligan a pensar en las personas, los factores psicológicos influyen, se deben de tomar, en su justa medida, las tendencias y modelos, y la preparación y el esfuerzo intelectual se hacen necesarios. Se busca movilizar desde el conocimiento, basado en los datos hacia la comprensión entendiendo el entorno y las relaciones. Es la única manera de poder percibir el complejo mundo de las amenazas.

Artículo noveno

Una acotación de la amenaza presente y futura de los drones comerciales letalizados

Juan Luis Chulilla Cano

Resumen

Comprender y acotar la amenaza presente y futura de los drones comerciales letalizados es, a la vez, un reto y una necesidad perentorios. El punto de partida más equilibrado es identificar algunos de los problemas que han impedido hasta 2023 identificar la amenaza, su prioridad y su potencial. Un juguete no puede ser un sistema de armas decisivo, por más que desde el campo llegaran advertencias sobre su uso.

El siguiente paso es abrir la caja negra y observar el interior: comprender, a cierto nivel de detalle técnico, qué se puede lograr con cada uno de los componentes con los que se han creado los drones comerciales y cómo estos sistemas, por separado y juntos, se traducen en un conjunto de capacidades militares disruptivas.

La suma de componentes y la apertura de la caja negra dejan ante una realidad muy diferente a la imaginada durante buena parte de este siglo: en lugar de *killer bots* autónomos o de enjambres autoorganizados que atacan de manera imparable, se encuentran sistemas sencillos, económicos y que alcanzan su verdadero y terrible valor gracias a lo que los operadores humanos logran hacer con ellos. Cuando los combatientes de ambos lados se sirven de sistemas parecidos, solo ellos pueden hacerlos evolucionar para mantener o reducir, según toque, cada ventaja competitiva.

Para maximizar esta carrera de la reina roja dronera[1], un nuevo ecosistema poblado por voluntarios, *war startups* e iniciativas gubernamentales, está reescribiendo el libro de reglas. Aprovechar lo que se pueda de sus ejemplos y monitorizar sus avances son pasos imprescindibles para pivotar el ecosistema de defensa C-UAS, hacer frente a la amenaza y, cuando sea posible, aprovechar la oportunidad.

Palabras clave

Drones comerciales, Drones FPV, Guerra de drones, Conflicto de Ucrania, Masa distribuida, Counter-UAS, Ecosistema de defensa.

[1] La carrera de la reina roja, un concepto derivado de *A través del espejo* de Lewis Carroll, se refiere a la necesidad de continuar avanzando solo para mantenerse en el mismo lugar.

An approach to the present and future threat of lethalized commercial drones

Abstract

Understanding and narrowing down the present and future threat posed by weaponized commercial drones is both a pressing challenge and a pressing need. The most balanced starting point is to identify some of the problems that have prevented identification of the threat, its priority and its potential until 2023. A toy cannot be a decisive weapon system, no matter how many warnings about its use come from the field.

The next step is to open the black box and look inside: to understand at some level of technical detail what can be achieved with each of the components from which commercial drones have been created and how these systems, separately and together, translate into a set of disruptive military capabilities.

The sum of the components and the opening of the black box leaves us with a very different reality from the one imagined for much of this century: instead of autonomous killer bots or self-organising swarms that attack unstoppably, we have systems that are simple, inexpensive and achieve their true and terrible value through what human operators manage to do with them. When combatants on both sides use similar systems, only they can evolve them to maintain or reduce each competitive advantage.

To maximise this red queen drone race, a new ecosystem populated by volunteers, war startups and government initiatives is rewriting the rulebook. Leveraging what we can from their examples and monitoring their progress are essential steps to pivot our C-UAS defence ecosystem, address the threat and, where possible, seize the opportunity.

Keywords

Commercial drones, FPV drones, Drone warfare, Ukraine conflict, Distributed mass, counter-UAS, Defense ecosystem.

1 El fantasma de Port Arthur

Tras más de 120 años, el lugar que ocupa la guerra ruso-japonesa de 1904-1905 en la historiografía militar se debe, en buena medida, a su papel como advertencia inadvertida sobre el papel que algunos avances tecnológicos iban a jugar en los siguientes conflictos de alta intensidad y, sobre todo, en los frentes principales de la Primera Guerra Mundial. La combinación de la ametralladora, el alambre de espino y la madurez de la pieza artillera de retrocarga y pólvora sin humo causó bajas sin precedentes y anunció las dificultades que introduciría para la guerra de movimientos.

Como es sabido, en las batallas de aquel conflicto hicieron acto de presencia observadores militares de las principales potencias del mundo. La gran mayoría de los informes llegaron a las mismas conclusiones sobre el efecto real de las últimas tecnologías desarrolladas. Sin embargo, el choque conceptual era tan profundo que ninguno de los contendientes de la Gran Guerra pudo incorporar a tiempo lo que deberían haber sido lecciones aprendidas.

En la fase de la guerra de Ucrania que arranca el 24 de febrero de 2022, el uso de los drones comerciales letalizados (de ahora en adelante, DCL) no ha sido una novedad. En distintos conflictos previos y, de hecho, en las etapas anteriores del conflicto, ya se habían empleado con éxito creciente, pero con poco impacto en la percepción de sus efectos más allá de algunos artículos precursores. De hecho, los éxitos del SOCOM norteamericano contra el DAESH y otros grupos salafistas y, en particular, la neutralización que lograron de la amenaza dron entre 2017 y 2018 tentó a no pocos a minusvalorar la amenaza e, incluso, a darla por mitigada de manera decisiva.

Una de las diferencias esenciales con la guerra ruso-japonesa estribaría en que, mientras que los altos mandos de comienzos del XX padecieran una ceguera doctrinal parcial y no fueran capaces de dar los últimos pasos conceptuales a los que llevaba la combinación de los nuevos medios industriales, en el caso actual los analistas y altos mandos tuvieron que luchar desde 2014 a 2022 con el aparente contrasentido de que un juguete como es el dron comercial (sobre todo, en comparación con los sistemas militares) pudiera tener un impacto significativo en las operaciones de alta intensidad.

En 2022-2024 apenas hay observadores militares aliados en primera línea, debido a las extraordinarias circunstancias que concurren en la guerra. En su lugar, las omnímodas redes sociales están trasladando imágenes reales del uso de los drones en primera persona (FPV - *First Person View*), abalanzándose sobre sus objetivos. Ahora mismo resulta muchísimo más difícil que en 1906 minusvalorar la amenaza, especialmente cuando se comprueba el impacto decisivo y paralizante que los pequeños drones

están generando en el invierno 2023-2024. Cabe confiar que no se va a repetir una situación comparable a la europea en 1914; sin embargo, hay que admitir que el ritmo de evolución de la amenaza es sustancialmente superior al ritmo de evolución y adquisición de los sistemas C-UAS. Está por ver si la necesaria y enérgica reacción a estas novedades se materializa, y será más probable cuanto mejor entendida sea la amenaza.

Lo que ya no está por ver es la similitud entre el efecto de la ametralladora y el alambre de espino con el efecto de la presencia masiva de los drones comerciales en el campo de batalla. La presencia de miles de ojos en el cielo, día y noche, con la sola y parcial excepción de la lluvia o la niebla densa, imposibilita desde hace meses que la concentración de vehículos previa al avance se ejecute sin ser detectada; perdida la sorpresa, a los efectores convencionales se les suma el dron volando a distancias de más de 10 km con una granada contramaterial o antiblindaje impactando con precisión en puntos desprotegidos. Como consecuencia, el movimiento ha quedado reducido a niveles anteriormente impensables y se lleva a cabo a costa de pérdidas difíciles de asumir. Los drones en su conjunto han frenado en seco la guerra de movimiento, como la suma de ametralladoras, artillería de retrocarga y alambre de espino hace cien años.

2 FPV vs comercial

La diferencia principal entre los drones civiles raya en lo filosófico. Por una parte, drones comerciales (como los de la empresa dominante DJI y de otras marcas como Autel, Parrot, Yuneek, Hubsan) se basan en el mismo principio: un producto cerrado, de muy difícil modificación y centrado en facilitar al máximo el manejo a los usuarios. Si desde el primer momento la interfaz y experiencia de usuario logró reducir decisivamente la barrera de entrada, en los últimos años los fabricantes líderes del mercado han añadido sucesivas mejoras orientadas a la evitación automática de obstáculos, la programación de rutas y un manejo cada vez más despreocupado, que permita al usuario centrarse en la grabación de tomas con fines personales o profesionales. Más una *appliance* que un dispositivo de vuelo, estos sistemas son productos diseñados para ser usados, no para ser modificados o mucho menos creados. Su enlace radio es sobradamente conocido por las FCSE occidentales, de manera que tal y como vienen de serie[2] son detectables en segundos por los sistemas C-UAS en uso.

Por otra parte, hay drones FPV. Son lo contrario a los drones comerciales en dimensiones muy diferentes. Hasta hace meses han sido por

[2] Tal y como vienen de serie. Si se modifica o sustituye su sistema operativo, su *firmware*, se pueden saltar las protecciones definidas de fábrica: límite de altura, límite de velocidad, zonas *no-go* y, sobre todo, anonimizarlos: evitar su detección por medios policiales.

completo minoritarios porque su curva de acceso era opuesta: elevadísima y con *show stoppers*[3] de compleja solución. La mayoría de los drones FPV se han adquirido por piezas, de manera que el dronero **y** *maker*[4] escoge los componentes que mejor encajan con el problema que quiere solucionar, con sus preferencias, etc. Una vez se adquieren los componentes físicos, electrónicos y de soporte el dronero-maker procede a montarlos en una cadena de pasos que lleva su tiempo y que demanda un importante set de conocimientos. Al acabar de montarlos, se instala y configura el *firmware open source* de la elección del dronero (betaflight, INAV, ardupilot, etc.). Después probar y finalmente volar, lo que a su vez exige un conjunto de destrezas completamente alejadas de las necesarias para usar un dron comercial - para que el dron pueda seguir trayectorias imposibles y recorrer al límite un circuito de carreras, o filmar instalaciones como nunca antes, su manejo está en las antípodas del mencionado uso despreocupado. El *eterno retorno* dronero de FPV sigue estos pasos: diseñar, montar, configurar, probar, volar, estrellar, empezar de nuevo.

No hay simetría: el usuario de drones comerciales no puede volar un FPV sin dotarse del conjunto de conocimientos y habilidades. El dronero FPV puede volar un DJI sin problemas.

Finalmente, hay que entender que el aeromodelismo clásico se vuela en tercera persona y tan lejos como el operador pueda distinguir con claridad la actitud de su aparato. Las cámaras FPV rompen esa barrera y colocan el límite teórico (que no el legal) en la distancia en la que se pueden seguir recibiendo imágenes del dron. Además, el set de habilidades y la experiencia es completamente distinta: el operador ve lo mismo que el dron y puede maniobrar de forma imposible para un vuelo en tercera persona. Muchos de los droneros FPV no iniciaron su camino en el aeromodelismo, sino que entraron desde la electrónica y el *software*: al fin y al cabo, un dron es un ladrillo lleno de electrónica, cables, cámaras y radios, que vuela.

3 One-way attack y ojo en el cielo

En la guerra, como desgraciadamente se está comprobando a diario, ambos tipos de drones se complementan: el dron comercial anonimizado (nota 1 a pie de página) se mantiene alejado de la línea de contacto y se aprovecha sus estupendas cámaras estabilizadas en tres ejes para obtener inteligencia a un nivel orgánico inéditamente bajo.

---

[3] Obstáculo crítico que detiene o retrasa significativamente la adopción generalizada de una tecnología.

[4] Mientras que «dronero» se refiere a una persona muy vinculada con drones de fabricación propia, que las mayoría de las veces los vuela y fabrica, «maker» es aquella persona que principalmente fabrica y modifica drones civiles a título particular.

En los cielos de Ucrania se asume que drones DJI Mavic y equivalentes son prácticamente desechables y se van a perder por efecto de la guerra electrónica. Sin embargo, las pocas horas que logren estar en el cielo son un recurso de inteligencia completamente inédito, que ha cambiado para siempre la historia de la guerra hasta el punto de ser uno de los componentes más importantes de las nuevas fuentes de inteligencia junto a los satélites comerciales para lograr el campo de batalla transparente (Taylor, 2024).

No se trata de una eliminación completa de la niebla de la guerra, tanto por motivos ambientales (niebla densa y lluvia intensa) como humanos (camuflaje aumentado y envenenamiento de computer vision); sin embargo, el hecho de que unidades de entidad sección o piezas de artillería individuales posean medios de reconocimiento aéreo orgánico y en tiempo real no tiene precedentes, como tampoco lo tiene que la información que generan esos medios alimenten distintos sistemas de gestión del campo de batalla.

La pura acumulación de cámaras volando día y noche dificulta no solo la concentración previa al movimiento, sino que reduce los fuegos de contrabatería a plazos inéditos de bastante menos de un minuto, reduce la movilidad cerca de la línea de contacto a muy pequeños grupos de infantes desmontados, y como se expresa en el manual de protección de infantería contra drones de las Fuerzas de Defensa Territorial de Ucrania: «La basura te puede matar. Si tiras una bolsa, una botella, un envoltorio, un papel al suelo, te has traicionado a ti mismo. Si no la limpias, el enemigo lo detectará. Recógela o entiérrala»[5].

Hasta hace algunos meses, los drones comerciales también se empleaban para lanzar granadas y otras cargas letales volando en estacionario. Para ello se desarrolló una pequeña industria que fabricaba lanzadores activados mediante una célula fotoeléctrica activada por la linterna cenital del dron y un servomotor. Sin embargo, es una práctica que ha perdido mucho predicamento debido a lo conocido que es el radioenlace de DJI (Ocusync). Como quiera que en los drones DJI Ocusync se emplea tanto para control como para vídeo, resulta especialmente vulnerable a los sistemas de inhibición; además, su papel actual como vector de obtención de inteligencia es demasiado valioso como para arriesgarlos aún más en misiones tras las líneas enemigas. Es sencillo constatar cómo los ataques con lanzamiento de granada en estacionario y con interfaz de DJI han disminuido sustancialmente en el último semestre, a tenor de lo que se publica en redes sociales.

Los primeros drones de ataque creados por los droneros ucranianos se retrotraen a 2016. En otras piezas (en un artículo de la *Revista General de Marina* (Chulilla Cano, 2023) y en La guerra de Ucrania III (Murillo, López y

[5] *HOW TO PROTECT YOURSELF FROM THE ENEMY DRONES. TIPS FOR INFANTRY.* Fuerzas de Defensa Territorial de Ucrania.

Piella, 2024) se cubre cómo grupos pioneros como Aerorozvidka desarrollaron los primeros multicópteros dedicados a observación y ataque nocturnos como el R-18. Estos drones pesados escapan del ámbito principal de este artículo, al tratarse de drones industriales que emplean componentes diferentes y presentan un coste y huella logística más elevados. Además, por más que jugaran un papel importante en los primeros compases de esta fase de la guerra de Ucrania (de febrero del 22 a la primavera del 23), su coste y complejidad impidieron que se consiguiera un factor crítico: la masa.

El problema no es solo que por cada dron pesado se pueden llegar a montar una decena de drones FPV o más, sino que las habilidades necesarias para hacerlo son aún más especializadas. Los drones FPV nacieron y evolucionaron por y para los aficionados y las empresas chinas que les sirven: una sola persona, en su dormitorio, con un soldador, un par de destornilladores y un PC puede montar un dron FPV.

El ecosistema FPV carece de precedentes militares. Grupos independientes aplicaron sus métodos de iteración (construcción, prueba, vuelo, repetir) al caso del dron FPV letalizado. En ciclos realmente cortos resolvieron los principales escollos que les separaban para poner en producción un dron que transportara de manera fiable una granada PG-7V contracarro o una mina direccional MON-50 a algunos kilómetros. Aprovecharon los desarrollos civiles para vuelos *Long Range* (pasar a baterías de ión de litio y mejorar la transmisión y recepción de los dos enlaces de radio), desarrollaron modificaciones de las cargas letales para poder ser empleadas sin sus medios originales y, sobre todo, mejoraron el *fieldcraft*[6] partiendo de la metodología del tirador de precisión heredada de la URSS y adaptándola al enorme salto que supone no necesitar línea de visión con el blanco.

Un dron FPV de ataque es un efector sin precedentes. Puede torcer una esquina, quedarse en estacionario, dar media vuelta y reintentar la aproximación hasta que logra acertar a su blanco. Puede entrar por ventanas, troneras y cualquier rendija por la que quepa, y hacerlo a una velocidad tan lenta que resulta manejable para el piloto. La lenta velocidad de los drones FPV, comparada con la de un misil CC, ha supuesto otra ventaja sorprendente más: es mucho más manejable y permite esquivar obstáculos o cambiar la trayectoria mientras haya carga en la batería. Por si fuera poco, nunca antes se dispuso de esta suma de capacidades a un coste también sin precedentes: menos de 2000 € para un dron básico, probado y capaz de portar una carga útil de más de 2 kg.

[6] El conjunto de habilidades del tirador de precisión relativos al camuflaje, observación y movimiento en entornos hostiles para tomar posición, identificar y neutralizar objetivos mientras se evita ser detectado.

Y con semejante ausencia de precedentes, no resulta sencillo acotar sus consecuencias. Solo hay una consecuencia evidente e indiscutible: los drones comerciales letalizados son la gran caja de Pandora de esta guerra. Han venido para quedarse, y ya han transformado las operaciones militares en un enorme abanico de aspectos. Además, la experiencia se está replicando de manera directa: el tsunami de innovación dronero ha llegado ya a Sudán, a Siria (esta vez en manos de las fuerzas del régimen de el-'Assad (Suleiman y Hezaber, 2024) y a cada vez más lugares de conflicto presente o potencial. A no mucho tardar, los DCL dejarán de ser opcionales, mientras que las Fuerzas Armadas de cada nación tendrán que priorizar más y más la integración y evolución de sistemas de sistemas C-UAS[7]. Aquellas naciones que apuesten con decisión por su ecosistema de fabricantes y proveedores de servicios C-UAS y por los campeones nacionales a cargo de la integración del conjunto de sistemas no solo protegerán antes y mejor sus recursos vitales, sino que apoyarán el crecimiento de este sector vía exportación.

4 El juguete y el teléfono volador

Se ha mencionado antes el freno conceptual que supone el juguete para valorar la amenaza que suponen los drones comerciales letalizados. Es un reto también sin precedentes: ¿Cómo han podido transformarse los protagonistas de las carreras de drones de la década pasada y los juguetes de navidad en un vector y efector con impacto significativo en las operaciones militares? No se habla del tamaño, o no solo: hay pocos drones comerciales tan pequeños como el Black Hornet de Teledyne y, desde luego, ninguno con esos 33 g de peso que se mantenga tantos minutos emitiendo vídeo a muchos cientos de metros.

De lo que se habla, fundamentalmente, es de aparatos voladores construidos por aficionados en unos casos, y siempre operados por aficionados o, en casos contados, por profesionales en dominios por completo alejados de la milicia. Se trata de volar con drones FPV en pequeños circuitos de velocidad, de hacer acrobacias sobre ruinas o, bordeando la normativa aeronáutica, de volar más allá del alcance visual poniendo al límite habilidades y enlaces de radio. Todo, por algunos cientos o muy pocos miles de euros. Por el precio de un Black Hornet se pueden llegar a adquirir cerca de cien drones comerciales de distintas características. Otro precio que se paga en algunos casos son las horas de aprendizaje: mientras que un Black Hornet ofrece a su operador elevados automatismos, en el caso del dron FPV la curva de aprendizaje sigue siendo elevada y a todos los niveles: la mayoría de los operadores también son *makers* de sus propios drones y,

[7] La inspiración inicial para esta formulación la proporcionó una conversación con Manfredo Monforte Moreno, general de división retirado.

en todos los casos, tienen que dedicar cientos de horas al simulador para adquirir las competencias necesarias para hacer lo que quieran con su dron.

La figura del *maker* merece reflexión aparte. Partir de unas decenas de componentes *hardware* y un *software* por configurar para llegar a un dron FPV en condiciones de vuelo es un camino largo y complejo que solo se puede construir en comunidad.

Sin embargo, no se habría dado ni el primer paso si la industria civil no hubiera generado los componentes necesarios. La explosión del *smartphone* no solo ofreció componentes imposibles de prever, como unidades de medición inercial que registran con precisión inclinación en tres ejes, aceleración y presión atmosférica, sino a un precio tan imposible como menos de 15 €. Hace no demasiados años, sus equivalentes subían de precio y, sobre todo, masa en varios órdenes de magnitud. Los drones FPV de cuatro motores, los famosos quads o cuadricópteros, pueden mantenerse en vuelo gracias a que la CPU recibe a amiles de veces por segundo datos precisos de inclinación y aceleración y, con ellos y las lógicas de su programación, puede traducir los comandos del operador en cambios de actitud y aceleración controlables. Si el operador tuviera que mantener la velocidad de cada uno de los cuatro motores por separado, sería imposible un vuelo controlado.

No es el único ejemplo del imperativo de la electrónica de consumo sobre los drones comerciales. Se puede hablar de protocolos de radio definida por *software*, de gran alcance y de bajo consumo, que, emitiendo a menos de 2 W, alcanzan muchos kilómetros en condiciones óptimas, ofrecen salto de

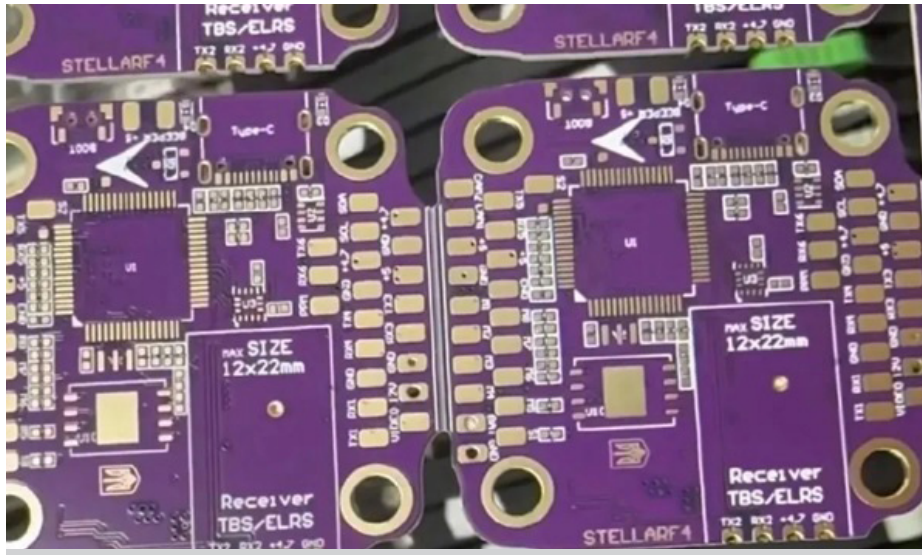

Figura 1. Placas controladoras de vuelo del grupo ucraniano Wild Hornets.
© Forbes

frecuencia encriptado dentro de las frecuencias legales[8], de *firmware* (sistema operativo embebido) libre, gratuito y de enorme capacidad y adaptabilidad, o incluso de diseños de *hardware* libres y disponibles para ser implementados con recursos realmente reducidos. De hecho, a principios de 2024 se ha cerrado el círculo y pequeños grupos ucranianos como Dyki Shershni (Wild Hornets) han empezado a fabricar (*In Ukraine flight controllers for drones have been developed*, 2024) placas de controladoras de vuelo integrando sus componentes principales gracias a que los diseños y esquemas estaban disponibles en su totalidad.

En este sentido, el miedo a un *shadow ban* (prohibición encubierta y no declarada) de componentes chinos a Ucrania es cada vez mayor, y con ello crece la presión —y la oportunidad— para que distintos fabricantes ucranianos y occidentales disminuyan la dependencia de los componentes chinos, especialmente electrónicos.

5 *Software* libre, componentes abiertos, comunidad

Este conocimiento libre y acumulado en comunidades de práctica *online* nacionales e internacionales, es esencial para que el dron FPV haya evolucionado primero como dispositivo civil y ahora como vector y efector militar. En las manos y mentes más talentosas posibles, el conjunto de componentes necesarios para construir un dron se puede escoger, modificar e incluso fabricar para optimizar la respuesta a una necesidad dada. Por ejemplo, desde antes de febrero del 2022 los voluntarios ucranianos habían seguido la tendencia dronera internacional a sustituir las baterías de polímero de litio por otras de ion de litio... construidas por ellos mismos. Las baterías, basadas en baratas celdas estándar de ion de litio (18650, 21700, etc.), ofrecen una mayor densidad de carga que resulta crítica para mantener el aparato en vuelo durante más minutos. Las conocidas y también comunitarias impresoras 3D permiten modificar los marcos o frames de los drones para optimizar su rendimiento (por ejemplo, asegurando posición de antena GNSS para evitar la interferencia con otros componentes eléctricos), o aportarles nuevas funcionalidades, como sistemas de suelta de carga basados en servomotores y piezas creadas *ad hoc*.

Mención especial merece el uso de las impresoras 3D para modificar las cargas útiles letales. De las granadas de 30 y 40 mm modificadas crudamente para permitir su detonación sin haber sido disparadas y con aletas impresas para mejorar su comportamiento lanzadas desde un dron, se ha pasado a generar distintas municiones de fragmentación optimizadas

[8] O desde hace unos meses fuera de la legislación internacional, que han logrado tanto ucranianos como rusos al modificar los emisores y receptores ELRS para emitir desde 720 MHz hasta casi 1000 MHz partiendo del set inicial en 868 / 915 MHz.

para las dimensiones de un dron. No hay que explicar el efecto que una Claymore o una MON-50 pueden crear si detonan en ángulo en lugar de detonar a ras de suelo.

Figura 2. Granadas VOG modificadas con aletas impresas en 3D para su uso con drones. © Getty Images

Los drones FPV nacieron y pudieron madurar gracias a las comunidades de entusiastas. Ingenieros, *hackers* y personas de las profesiones más variadas se unieron a foros, primero, y grupos en RRSS, después, para compartir conocimientos y aprender juntos. Comparados con las comunidades de Linux, hay que señalar que la cordialidad y la cooperación son superiores y, por motivos muy prácticos, solo se puede mandar a *Read The Fucking Manual* cuando hay un manual que leer. Una vez más, nadie podía imaginar que esas comunidades se reconvertirían en una forma completamente

Figura 3. Makers Ukranianos montando un dron para la guerra. © Aleksey Filippov/AFP

nueva de innovar en la guerra: el ecosistema de grupos voluntarios y *war startups* ucranianos, imitado en cierta medida por sus adversarios rusos.

No se puede acabar la revisión del *software* sin mencionar los simuladores. Se trata de piezas críticas para el aprendizaje de los futuros pilotos. Por menos de 50 € (o completamente gratis en algunos casos de *software* libre), y empleando un PC con windows y una tarjeta gráfica que no sea nada del otro mundo, un usuario puede conectar la emisora que luego empleará para operar su dron y aprender a pilotar. Pese a esta ayuda decisiva de la controladora y sus sensores, la operación de un dron FPV no es sencilla... porque sus creadores originales no desarrollaron el *software* para que fuera cómodo, sino para extremar la agilidad y velocidad de respuesta.

Los simuladores en PC ofrecen al operador un entorno de vuelo crecientemente realista en el que adquirir y mejorar habilidades de vuelo sin importar las miles de veces que acaban estampando su dron simulado contra el suelo o un obstáculo. Desde el primer momento, los simuladores de vuelo han resultado ser un recurso indispensable: es básicamente imposible volar un FPV a la primera, y a poco brusco que sea el choque se van a partir hélices, o patas, o dañar los componentes electrónicos. De hecho, el aprendizaje en simulador se ha integrado en los *curricula* de pilotos ucranianos y rusos como elemento esencial en el que formar primero a decenas, luego a cientos y ahora mismo a decenas de miles de pilotos que saquen partido a la montaña de drones FPV que se está poniendo en servicio en 2024.

El simulador ha ganado valor con la guerra, porque permite al aspirante a dronero de combate entrenar miles de veces hasta perfeccionar su arte. De hecho, en fecha muy reciente se ha liberado en Steam un juego llamado «FPV Kamikaze» que ha dado el salto a la simulación de operación de combate de drones en entornos comparables a los de la guerra de Ucrania, empleando los drones de manera comparable a cómo se emplean en el conflicto. Hay que señalar que la física del dron no es tan precisa como los productos estrella (Lift Off, Velocidrone) y, sobre todo, el origen del *software* desaconseja su instalación en un ordenador de uso cotidiano.

6 La radio voladora

Las radios analógicas permitieron que los aeromodelistas tomaran el control de sus creaciones sin recurrir a cables. De hecho, los primeros drones FPV heredaron ese recurso crítico que permitía emitir comandos desde la emisora hasta el receptor de radio (RX) montado en el dron. Al igual que ha ocurrido en el caso de los *smartphones* y del resto del monstruoso ecosistema digital inalámbrico, la introducción de la radio definida por *software* ha permitido un salto disruptivo. Un RX digital pesa 0,7 g (10 g sumando antena y conector) y garantiza la recepción de la señal procedente de la emisora desde no

pocos kilómetros para una potencia de no demasiados miliwatios. Además, el enlace le permite devolver datos de telemetría a unos hercios respetables.

Los protocolos más populares en 2024 (Crossfire y ELRS) no difieren ni en frecuencias ni en tecnologías empleadas de manera decisiva. Ambos ofrecen una bajísima latencia y permiten un salto de frecuencia dentro de la banda empleada al emplear tecnologías FHSS (*Frequency Hopping Spread Spectrum*). La diferencia más importante es que Crossfire es un protocolo privativo y cerrado, mientras que ELRS es abierto. Esto se traduce en que un RX crossfire cuesta menos de 50 €, mientras que uno ELRS cuesta menos de 20.

Como se ha comentado líneas arriba, el hecho de que la licencia de ELRS sea *open source* ha permitido emplear otros protocolos igualmente libres (concretamente, LoRa) y adaptarlos del propósito original de enlazar nodos con poco ancho de banda pero muy largo alcance en una red Mesh a una red punto a punto (entre el TX y el RX) de bajísima latencia. Tanto el enlazado (*bind*) entre emisora y receptor como los pasos de frecuencia se emplean encriptados para evitar que un tercero tome control del dron mientras está en vuelo. El origen del salto de frecuencia se debe a las carreras: como quiera que los pilotos van a emplear un número reducido de bandas de frecuencia (868/915 ó 2.4, fundamentalmente) era crítico que no se interfirieran para volar con muy pocos metros de separación. Claro está, esta característica le pone las cosas más difíciles al defensor que emplee sistemas de inhibición, al tener que cubrir bandas más amplias.

Estos protocolos y sus frecuencias se diseñaron y escogieron para lograr una buena penetración. Los pioneros de la dronería FPV enseguida le cogieron el gusto a volar en el interior de edificios abandonados, esquivando obstáculos y entrando y saliendo por sus aperturas. Una vez más, estas características inocuas han sido reaprovechadas para superar los obstáculos entre el emisor y el receptor y, por ejemplo, lograr penetrar en el interior de instalaciones con fuerte componente metálico hasta alcanzar sus objetivos.

El radioenlace que terminó por permitir el vuelo en primera persona fue el que transmitía una señal de vídeo con latencia mínima y a distancia.

7 La cámara voladora

Los drones FPV (*First Person View*) transformaron tanto el aeromodelismo como el uso profesional e industrial de los drones de categoría I y peso inferior a 25 kg. o, según normativa europea, todos los drones de categorías C0 a C3. Una vez que se solucionó el problema de la miniaturización de los emisores de vídeo por radiofrecuencia (VTX) haciéndolos ligeros, de poco volumen y baratos, nació una afición y luego una profesión netamente distinta. De hecho, es el secreto del éxito inicial de la dominante DJI:

levantar un dron con una cámara (el primer Phantom) que pudiera enviar un *feed* de vídeo a su receptor a cierta distancia y en tiempo real.

Desde sus inicios, las cámaras montadas en dron han dado lugar a un rango creciente de usos profesionales civiles. La base es el control del dron: gracias a la cámara, el operador puede controlar su dron fuera del alcance visual y sin necesidad de preprogramar su trayectoria. Si la cámara ofrece resolución suficiente, permite emplear al dron para todo tipo de tareas de inspección y observación. Si no es el caso (por ejemplo, casi todas las cámaras de señal analógica), hasta hace no mucho se montaba una cámara de acción solidaria a la cámara FPV para grabar secuencias de alta calidad. Ese problema se ha solucionado en fecha reciente gracias a los sistemas VTX digitales, que ofrecen tomas sin pérdidas y de alta calidad para todo tipo de grabaciones publicitarias.

Anteriormente a las cámaras FPV, los aparatos de aeromodelismo (que no se denominaban drones) tenían que controlarse en alcance visual, lo que limitaba mucho su uso para aparatos de tamaño reducido. Sumando estos primeros y primitivos emisores de vídeo a drones con una relación empuje/peso excelente, nacieron las principales modalidades de vuelo FPV: enloquecidas carreras de obstáculos, vuelos *freestyle* acrobáticos en todo tipo de entornos, y vuelos *long range* mientras fueron legales o al menos no despertaron la alarma de las autoridades competentes. El factor de diversión y competición entre aficionados es de tal magnitud que, de hecho, para estos talentosos jóvenes, y no tan jóvenes, era realmente difícil de imaginar el uso hostil y malintencionado de sus preciados drones.

Los aficionados, y ahora algunos profesionales, han pasado a pilotar sus drones con gafas FPV en lugar de con monitor externo. En vuelos con muy poco margen para el error, las gafas permiten concentrar por completo al piloto en el *feed* de vídeo que recibe en tiempo real mientras maneja una emisora cuyos mandos conoce por memoria muscular. La sensación de estar en el dron llega a ser completa y resulta crucial para arrancar al rival unas décimas de segundo o para ejecutar una maniobra imposible, entrando y saliendo por una chimenea de una fábrica abandonada.

El vídeo puede derivarse a otros dispositivos. De hecho, muchos binomios en la guerra de Ucrania operan así: mientras el piloto se concentra en su misión, su binomio obtiene inteligencia del *feed* de vídeo y ayuda al piloto a la navegación y a evitar amenazas.

Nadie pudo prever, hasta que ha sido evidente para todos, el valor del *feed* de vídeo generado durante el vuelo. Es tanto un recurso de *battle damage assessment* que además se combina con las imágenes a distancia de los drones comerciales como un recurso adicional de inteligencia general. Conviene detenerse en este punto como un todo.

En el cambio de siglo, la introducción generalizada de drones tácticos, MALE y de categorías intermedias produjo un interesante cuello de botella: la IMINT de los *feed* de vídeo de los drones. En algunos momentos de la guerra global contra el terror, una proporción muy significativa de los *feeds* de los drones no llegaba a ser aprovechado. De la misma manera, el valor de los *feeds* de los drones tácticos mayoritariamente quedaba concentrado en la unidad para la que eran recurso orgánico. Con este panorama, parece claro que el cuello de botella aumentaría de forma proporcional al número de ojos en el cielo de forma simultánea.

Si hubiera ocurrido así, los drones comerciales no habrían ganado la preponderancia que han logrado. Sucede, para empezar, que el aumento de drones ha llevado aparejado un aumento del ancho de banda humano. El mencionado binomio, y otros miembros de la unidad, aportan capacidad de IMINT distribuida, interpretando el *feed*, detectando objetos de interés adicionales y generando *battle damage assessment*. La aportación decisiva de los drones al campo de batalla transparente se completa cuando toda esta inteligencia se canaliza y suma empleando los distintos sistemas de gestión del campo de batalla (BMS).

En la medida en la que lo permiten las comunicaciones de una zona (fundamentalmente starlink, pero no solo), el *feed* de vídeo o al menos fragmentos significativos ascienden a escalones superiores; sin embargo, lo importante es que la información operacionalizada consume un ancho de banda despreciable y puede ser mantenido empleando distintos sistemas de comunicación (incluso civiles en circunstancias puntuales). Esta capacidad aumentará más aún conforme se incorpore más y más el tratamiento multimodal de la información en bruto y los modelos de IA detecten objetos de interés; con todo, conviene poner en valor lo conseguido aquí y ahora combinando miles de ojos en el cielo, miles de mentes humanas, varios sistemas de gestión del campo de batalla y sistemas de comunicación redundantes. Sobre todo porque, saliéndonos del actual conflicto, se trata de una capacidad al alcance de algunos actores no estatales.

El vídeo producido por los drones comerciales se ha revelado como un recurso de propaganda sin precedentes. Los vídeos de los ataques con drones FPV y comerciales comenzaron a llegar en fecha temprana a redes sociales y constituyeron un éxito instantáneo. Estas secuencias siempre llamativas las emplean los grupos droneros independientes para algo tan mundano como conseguir visitas para sus canales. La batalla por la economía de la atención era y sigue siendo completamente crítica, los grupos droneros necesitan la atención de su público para conseguir donaciones que les permitan comprar todo tipo de componentes y equipos.

La publicación recurrente de los vídeos de ataque de los droneros ha tenido un impacto muy significativo en el público general y hasta

especializado. Los datos OSINT han pasado a depender cada vez más de los vídeos de los grupos droneros, y, por lo tanto, es razonable asumir un sesgo FPV importante en la causa de las bajas rusas de vehículos constatadas y, en menor grado, en las ucranianas.

8 El dron NLOS

Se comenzó esta fase de la guerra con una experiencia limitada con drones FPV letalizados. Eso ya se había traducido en alcances de hasta 4 km, empleando antenas direccionales de alta ganancia montadas sobre mástil portátil y los mejores componentes VTX y RX disponibles. Esto permitió, a su vez, separar la antena del operador. Esto ha ganado una importancia capital para el *fieldwork* de los operadores y es un aspecto muy importante en la formación de los droneros de guerra en las academias: los operadores, como los tiradores de precisión, aprenden a moverse y ocultarse. Al contrario que los tiradores, los droneros de combate no necesitan línea de visión directa a blanco alguno. Esto les permite emplear ruinas, búnkeres a cierta profundidad o cualquier otro escondite discreto desde el que sacar sus cables.

Este principio se ha extendido en fecha reciente al uso de drones relé o repeaters: un dron se sitúa en estacionario a más de 100 m de altura, recibe la señal de vídeo del dron FPV y la transmite al dronero en tierra. La señal de control sigue el camino inverso, de la antena del dronero al dron relé y

Figura 4. Sistema de relé ucraniano instalado sobre DJI mavic. https://twitter.com/front_ukrainian/status/1745906821871612023

de este al FPV. El resultado es que el máximo tiempo posible se mantiene línea de visión sin obstáculos entre el FPV y el relé, y con ello ambas señales se degradan lo menos posible.

Además, este sistema se ha empleado junto con modificaciones por *hardware* y *software* para alterar las bandas de frecuencia de las parejas de emisor y receptor. *Hackers* RF ucranianos y rusos han modificado el *firmware* de los sistemas ELRS para emplear bandas diferentes a la de 868 y 915 MHz, llegando a 1015 MHz y bajando hasta 740 MHz, y, en algunos casos, han modificado los emisores con amplificadores de señal y/o empleando placas de relé que permiten un cambio de la banda de frecuencia empleada. El resultado de todas estas innovaciones combinadas es que se ha pasado de 4-6 km, en el mejor de los casos, a récords de 22 km y alcances relativamente habituales de 10-12 km. Hasta fecha reciente, la limitación para la autonomía del dron FPV de ataque había sido el alcance de sus radios. Con un relé se puede aprovechar las baterías de ion de litio para alcanzar esos 22 km en algo menos de quince minutos, y ofreciendo inteligencia durante todo el trayecto.

No se debe olvidar que el dron relé va a operar en zona amiga, razonablemente lejos de la línea de contacto y en estacionario. Será relativamente raro que se pierda. El coste de cada misión será el del dron FPV creado y testado con componentes de la máxima calidad a la que se tenga acceso. Ahora imagine el lector lo que implica llevar a 22 km un dron contra carro, que va a poder atacar a un MBT por detrás y desde arriba. Por el coste de un Spike NLOS se pueden adquirir y poner en servicio aproximadamente cien de estos drones. Y por el coste de un T-90M, se pueden adquirir más de mil de estos drones. Las distancias que se están logrando permiten ya el fuego de contrabatería contra morteros y, en casos excepcionales, contra piezas de artillería. Sin embargo, la amenaza principal de estos drones FPV de alcance extendido se cierne sobre los medios logísticos. Efectivamente, los últimos kilómetros hasta las posiciones defensivas están ya completamente dentro del alcance de estos drones, más baratos que cualquier blindado, camión, 4 x 4 o incluso UGV (*Unmanned Ground Vehicle*). En la reciente batalla de Avdiivka (culminada en febrero de 2024) se comprobó cómo los drones FPV rusos resultaron críticos para estrangular el suministro a los defensores y provocar que la retirada no se llevara a cabo en las mejores condiciones posibles.

9 La IA voladora

La IA es, en parte, producto de una narrativa cultural industrial, el paso de Pygmalion al Gólem, la creación independiente que se vuelve contra su creador y contra la sociedad, y que acaba en HAL-9000 y Terminator. Esta visión ha contaminado el análisis del estado del arte de la IA, aplicada a vectores y efectores del campo de batalla. Queda fuera de este análisis su aplicación crítica a los sistemas de gestión del campo de batalla.

En el imaginario de Defensa, y, por supuesto, en el del gran público, los drones son uno de los sistemas que se conectan con más asiduidad al concepto inicial de IA. De hecho, las campañas políticas norteamericanas (tan bien financiadas y sostenidas en el tiempo como mal justificadas) han iterado en la última década y media en torno al *Killer bot*, *Slaughterbot* o al concepto de *Autonomous killing*[9]. Uno de los ejemplos de ficción que se pretende aviso sobre el futuro es, precisamente, *Slaughterbots*, un vídeo corto del Future of Life Institute[10], una organización sin fines de lucro dedicada a prevenir las amenazas existenciales y, concretamente, la que presuntamente supone la IA avanzada. Probablemente hayan visto el vídeo en youtube y se habrán percatado de que no es un vídeo de youtuber, sino una producción profesional y con recursos significativos.

No cabe aquí extenderse sobre los sistemas de armas que, desde hace años, son necesariamente autónomos en su *kill chain*. Desde los *Active Protection Systems* de los blindados a los sistemas AEGIS, hay un rango de sistemas de defensa para los que los tiempos humanos no son compatibles con la misión encomendada. De la misma manera, el salto tecnológico final de la Guerra Fría propició la aparición de una amplia diversidad de efectores contra carro de guía terminal autónoma. Muy acertadamente, se estimaba que la forma de gripar el rodillo blindado PACVAR[11] residía en emplear en masa una combinación de efectores NLOS[12] que detectaran y atacaran por sí mismos a los blindados.

El dron convertido en *killer bot* es un animal completamente distinto. Los activistas los presentan como pequeños drones que no solo navegan por sí solos, sino sobre todo que deciden y ejecutan el empleo de la fuerza letal contra seres humanos. El problema principal que genera esta visión es que al militar al cargo de la decisión se le priva del mando y el control, de la decisión de qué y cuándo, pero no de la responsabilidad. Además de esta perspectiva tan poco halagüeña, el problema conceptual más grave es el de sustitución en vez de aumentación: la inteligencia artificial se plantea

[9] *Killer bot* y *slaughterbot* son términos sinónimos creados mayoritariamente desde fuera del dominio de defensa y que apuntan a dispositivos no tripulados, mayoritariamente drones, que actúan con entera independencia de la decisión humana. *Autonomous killing* sería un uso de la fuerza letal con independencia de la decisión humana y con el énfasis puesto en el peligro para la humanidad en su conjunto.

[10] Véase: www.futureoflife.org

[11] Recuérdese el escenario más temido y visibilizado de conflicto convencional en Europa durante los setenta y ochenta. La masa blindada del Pacto de Varsovia, cerca de un orden de magnitud superior a la disponible para OTAN, tendría capacidad para romper las sucesivas defensas y llegar a sus objetivos en muy pocos días a menos que se empleara una cantidad aún más masiva de efectores contra carro.

[12] *Non Line of Sight*. Efectores que no necesitan que, en todo momento, el operador observe de manera directa a su blanco, sino que poseen algún tipo de sensorización o guía que les permite guiarse una vez lanzados, sobre todo en la fase terminal.

como sustituta en lugar de como aumentadora de la humana, despreciando la flexibilidad, adaptabilidad y juicio humanos cuando el individuo dispone de tiempo para decidir.

Matar personas es propio de asesinos o de proyecto de genocidas, no de las operaciones militares. En las operaciones militares el uso de la fuerza letal es un medio al servicio de los objetivos planteados, sometido a las reglas de enfrentamiento y al criterio personal del mando al cargo; además, dichos medios van a ser por definición limitados, y una decisión no humana va a ser siempre inferior al juicio humano sobre cuándo y qué.

El problema de los *killer bots* es que se trata de artefactos de la imaginación. Trasladados al terreno de lo real, se hablaría de montar en un dron de pocos cientos de gramos dos unidades de procesamiento: una TPU o unidad de procesamiento de tensores, en la que ejecutar el o los modelos de machine learning, y una companion computer que le haga peticiones a la TPU y convierta sus resultados en órdenes para la controladora de vuelo del dron. Este montaje no solo sería más grande que un dron pequeño, sino que consumiría una potencia muy importante comparada con la que consume un motor trifásico de dron. El resultado de esto es que el film *slaughterbots* es y seguirá siendo fantasía malintencionada y en conflicto con lo que en el futuro a medio plazo va a poder miniaturizar la electrónica.

La visión del Golem fuera de control es muy eficaz para arrebatar la atención a lo inmediato y posible. La aplicación más avanzada, pero real, de los sistemas de IA es la navegación por seguimiento de terreno empleando una cámara y computer vision. En entornos de navegación vía GNSS imposible o denegada, el sistema puede reconocer los hitos del entorno que le permitan completar un circuito. En la actualidad es una capacidad restringida a los UAS más avanzados, sobre todo militares. Pero los avances en los componentes necesarios acercan una solución de coste contenido y licencia libre, aunque con limitaciones de peso y tamaño.

Por otra parte, existe la guía terminal autónoma. Como se ha comentado antes, el dron que cerrara la fase terminal de su vuelo con una *kill chain* completa no necesita inteligencia artificial para hacerlo… de forma probabilística. La detección de un blindado dentro de un área autorizada para hacerlo es un problema resuelto hace décadas (submuniciones como las Skeet o la BAT, por ejemplo), siempre que se acepte cierto margen de fallo (incluyendo empeñar un blanco ya destruido) y que no se busque un punto de impacto específico del carro.

En los años ochenta surgen sistemas CC más allá de la línea visual que ofrecen al tirador un *feed* de vídeo en tiempo real con el que mantenerse en el *loop* y decidir: dónde exactamente, y si hacerlo. En 2023 y 2024 se aplica el mismo principio de uso de un Spike NLOS, solo que rebajando más de

dos órdenes de magnitud su precio. El operador pilota el dron FPV gracias a su *feed* de vídeo y decide exactamente dónde y si hacerlo.

En este momento pivotal de la historia de la tecnología, el mencionado dilema entre sustitución y aumentación del hombre puede tentar a algunos a minusvalorar las capacidades de una mente humana entrenada, desde el juicio humano pasando por la flexibilidad y la improvisación. El dron *killer bot*, así, pasa por alto lo que una persona motivada y preparada puede llegar a hacer con un dron en las manos.

Es cierto que la inhibición de los enlaces radio, y especialmente el de control, supone un grave problema para el piloto humano de un dron FPV. Ahí es donde ya está entrando la guía terminal autónoma, pero no como IA avanzada sino como recurso más probado y sencillo: cuando el piloto quiere o tiene la oportunidad, y a distancia prudencial, coloca el punto de mira de su cámara donde quiere que impacte el dron. A continuación, pulsa uno de los controles de su emisora para transmitir al dron la orden de que se dirija en línea recta a ese objetivo. Para cumplir esa orden no hace falta una IA avanzada ni una TPU enorme: recursos plenamente maduros como el *optical flow* (comparable a las guías de munición por TV de los sesenta, pero miniaturizado) hacen perfectamente el trabajo. A fecha de febrero de 2024 no se ha alcanzado un grado de madurez suficiente que permita la generalización de esta capacidad, pero cada vez le queda menos.

10 Enjambre y masa

Más allá del aquí y el ahora, está una capacidad muchas veces anunciada y hasta ahora no concretada: los enjambres. Hay que destacar la asombrosa dificultad del problema: un enjambre propiamente dicho es un conjunto de drones que comparte información proveniente de sus sensores y coordina entre sí sus acciones individuales y en grupo «votando» sobre el curso de acción más apropiado según evolucionan las circunstancias para lograr el mayor éxito posible de una misión. Por ejemplo, si un enjambre pierde parte de sus integrantes durante el transcurso de una misión, los supervivientes conocerían este hecho y adaptarían sus perfiles de vuelo y misiones particulares para que la misión general se cumpliera lo mejor posible.

Dificultades: ancho de banda, comunicación segura (futuro: lumínica), capacidad de cálculo in situ y, sobre todo, complejidad *software*. No hay nada ni remotamente similar en la definición de agentes en los repositorios libres. Las compañías más avanzadas dan pasos hacia la implementación de sistemas de comunicación altamente resistentes (incluyendo la comunicación vía láser, así como redes mesh de baja latencia y gran ancho de banda), y sobre todo *software* que genere para todo el enjambre una

common operational picture y acerque la adaptabilidad colectiva a la puesta en servicio.

En cualquier caso, hay que insistir en que se lleva décadas debatiendo y avisando sobre una tecnología que no acaba de ser puesta en producción. Tanto espacio ocupó en las discusiones que hizo todavía más invisible al juguete, al dron construido a base de piezas estándar y *software* libre y, sobre todo, a las mentes que los conciben, los fabrican y los vuelan. Un efector aparentemente menos rupturista que el imaginado enjambre gestionado por agentes de inteligencia artificial, ha acabado resultando completamente disruptivo. En lugar de una masa de drones atacando simultáneamente y por sí mismos, lo que ha traído esta guerra es un goteo continuo de vuelos, de día y de noche, sobre amplios sectores de la línea de contacto que se transforma en un todo continuo de vuelos sobre cualquier blanco posible.

El verdadero peligro en 2024, el concepto central respecto a la letalización de los drones comerciales y FPV es la masa distribuida. Una realidad que, sin ser enjambre, se adapta en mil direcciones y a un ritmo más que preocupante. Como decía Koba el Terrible, alias Iosif Stalin, la cantidad tiene su propia calidad. No es sencillo definir un momento preciso o una cantidad en la que el uso de los drones cambia de fase. De hecho, en mayo de 2023 el británico RUSI publica *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine* (Watling y Reynolds, 2023). En este informe se señala cómo Ucrania estaba *perdiendo* 10 000 drones al mes. Dejando aparte lo redondo y, por lo tanto, grueso de la cifra, lo importante es que en aquellos días no se acababa de visualizar el cambio que estaba teniendo lugar: la gran mayoría de las pérdidas no eran tales, sino el resultado inevitable del uso de los OWA (*One-Way Attack*) drones, mal llamados entonces y aún ahora *Drones kamikaze*. Todavía no se había establecido en Ucrania una cadena de suministro que permitiera consumir ese número de drones, pero a no mucho tardar la cadena logística y de producción escaló a lo que acabaron siendo las cifras estables: cientos de miles al finalizar el año, millones en 2024 y sucesivos. Y otro tanto ocurría y ocurrió con los pilotos: de cientos se pasó a miles y luego a decenas de miles.

La masa, así, no es la imagen de una bandada de drones en un render publicitario, por más que hasta hoy una parte significativa de los sistemas C-UAS se ilustren actuando contra esas formaciones aún inexistentes. La masa es un producto del empleo de drones comerciales y FPV durante enormes períodos de tiempo. En un evento de alta intensidad sobre los cielos de Zaporizhzhia o Jersón podrán estar volando a la vez menos de diez drones[13] en una distancia de pocos cientos de metros. Sin embargo,

[13] La mayoría de las veces el límite lo marcarán el número de emisores de vídeo que puedan operar en las cercanías de forma simultánea.

en el transcurso de unas horas seguirán apareciendo más y más drones, individualmente o en pequeños grupos, conforme se detecten nuevos blancos. La masa no va a ser instantánea, sino acumulada y distribuida, y muy probablemente los efectos son peores de lo que cabría esperar de un imaginado enjambre de cientos de drones volando durante unos minutos sobre un área.

11 Chimple vs expenplex: economía del dron

Las cifras mencionadas son una de las disrupciones principales de los drones comerciales letalizados. El final de la Guerra Fría y la era de los dividendos de la paz marcaron una clara tendencia a los productos exclusivamente de defensa, barrocos (Kaldor, 1983) y expenplex: *expensive and complex*. Sistemas magníficos, en lo posible multirrol y avanzando decisivamente las capacidades respecto a la generación de sistemas anteriores, fueron la norma por tierra, mar y aire. El dron comercial es uno de los abanderados de la era de los sistemas chimple: *cheap and simple*. La concentración de roles y capacidades se desacopla hasta donde es posible, y la reducción de costes en varios órdenes de magnitud deriva del empleo de tecnologías civiles, que en el caso de las digitales no solo son suficientemente baratas, sino que superan en capacidad a sistemas puramente militares que no han evolucionado al ritmo frenético de las tecnologías civiles, debido al peso en la economía de escala de estas últimas.

La economía del dron también se conecta con un factor aún más importante: la industria militar tiene acceso a un pool de técnicos creativos y talentosos muy reducida en comparación con el sector civil, tanto empresarial como comunitario - open source. Si el empresarial ha sido decisivo para poner en servicio sistemas críticos, sobre todo de *hardware* exótico, capaz y barato (los *Systems on a Chip* que mueven los *smartphones* o los drones), el mundo *open source* aporta algo igualmente valioso, especialmente en los tiempos de una guerra existencial: miles de jóvenes, y no tan jóvenes, con talento y la máxima motivación posible.

A los jóvenes que han puesto en marcha decenas de grupos voluntarios primero, y ahora *war startups*, nadie les explicó que no se podía iterar en semanas y poner productos en servicio invirtiendo decenas de miles de dólares. Como no lo sabían, y como contaban con el conocimiento comunitario acumulado por sus predecesores en los distintos dominios, lo hicieron. Migraron los sistemas de Github[14] a la guerra.

[14] El mayor repositorio o almacén de *software* libre del mundo. Disponible en: www.github.com

12 *War Startups*, academias, iniciativas gubernamentales: reinventar la guerra para salvar la patria

En esta década, y con tal de tener acceso a internet, cualquier persona con un mínimo de talento y persistencia puede adquirir conocimientos sobre tecnología a un nivel inaudito. Todo el conocimiento necesario está disponible en una cantidad básicamente ilimitada de recursos de aprendizaje. Además, todos aprenden de todos, en el mundo del *software* libre las personas se saben parte de una cadena que aprende primero y enseña después.

Posiblemente uno de los factores más críticos para la supervivencia de Ucrania ha sido traducir este espíritu a amplios ámbitos de la defensa nacional. Es sabido que una parte importante de los desarrollos de *hardware* y *software* no se mantienen en secreto empresarial, sino que se comparten en un modo de comunidad *open source* abierta a todos los que pasan los filtros de seguridad pertinentes. La ventaja que proporciona este esquema es decisiva: el conocimiento adquirido y el *software* desarrollado se comparte para no reinventar la rueda y para trabajar a partir del arte previo, entendiéndose previo como aquello publicado hace más de 48 horas.

Sobre todo en el caso ucraniano, hay que señalar que han llevado el espíritu de las licencias libres del *open source* a su máxima expresión, de manera que cada innovación en *software*, en *hardware*, en combinatoria de componentes y en operativa, se difunde sobre todo en los espacios autorizados y, hasta donde se puede, en espacios cuya única puerta es hablar ucraniano.

En los mencionados artículos de la RGM y capítulo sobre drones del III libro de la guerra de Ucrania, se relata la transición del espíritu organizativo del Maidán a las organizaciones de voluntarios. En los primeros años, la carencia de medios impidió que madurara en Ucrania un ecosistema nacional como el mencionado. Pero la amenaza existencial y el apoyo interno y externo se combinaron para dar el paso de forma colectiva. Por ejemplo, a lo largo y ancho del país han surgido decenas de academias y pequeños centros de enseñanza en los que diseminar el conocimiento. Miles y miles de makers han adquirido en dichos centros, o simplemente por el boca a boca, conocimientos para seleccionar e integrar componentes en drones que respondan a distintas necesidades, y para reparar o canibalizar los drones dañados. Además, los veteranos de un rol particularmente peligroso vuelven del frente para formar a miles y miles de pilotos en el conjunto de habilidades que necesita un joven para trasladar su memoria muscular del gamepad de una consola a la emisora de un dron (como se explica, empleando simuladores civiles) y adquirir los también mencionados conocimientos y habilidades de fieldcraft para minimizar el riesgo al entrar y salir de posición.

Los grupos voluntarios han evolucionado con la guerra. Algunos han buscado apoyo financiero a través de la publicación de vídeos de todo tipo: sus creaciones, entrevistas, acciones exitosas, etc. Esto les ha generado un flujo constante de ayuda voluntaria, en especie y mediante servicios de donación tipo Patreon[15]. Al mismo tiempo, esta misma visibilidad les ha permitido lanzar eventos puntuales de *crowdfunding* para sufragar gastos extraordinarios, desde un 4 x 4 hasta cámaras infrarrojas. Esta actividad continuada en redes sociales, además, ha permitido al gran público conocer la guerra de los droneros contada por ellos mismos, y se puede afirmar que su contribución al mantenimiento de la visibilidad de la causa ucraniana ha sido significativa. De cualquier forma, la mayoría de ellos han cedido el testigo de la innovación tecnológica a las *war startups*, las empresas con fondos y recursos humanos para trabajar en los siguientes pasos evolutivos de los drones. Ahora mismo, el papel principal de los grupos voluntarios está tanto en las operaciones militares como en la construcción de distintos modelos de drones FPV, como sobre todo en la transmisión de sus conocimientos y experiencias de valor incalculable.

El siguiente paso evolutivo han sido las *war startups*. Hacia febrero de 2022 la industria de defensa ucraniana se encontraba en plena transición entre la industria heredada de la URSS y que perseveraba en adaptarse a la demanda del mercado internacional, por un lado, y un grupo creciente de pequeñas empresas rupturistas que hacían lo posible por mantenerse a flote, por otro, antes de esa fecha, la percepción de amenaza era muy limitada, y de ahí que no recibieran un apoyo suficiente del capital nacional o internacional o del propio Estado. Pese a eso, algunos de sus desarrollos en drones militares se unían a los desarrollos de los grupos de voluntarios como cimientos de lo que iba a venir.

Las *war startups* están destilando el conocimiento nacido de la experiencia de combate y de los requisitos de los combatientes y lo combinan con los recursos de los *hackers*, desarrolladores e ingenieros que están culminando la conversión en industria de guerra, como se decía antes. Si en la segunda guerra mundial el fabricante de automóviles o de maquinaria agrícola pasó a fabricar máquinas de guerra de todo tipo, ahora las compañías IT y de ingeniería electrónica y electromecánica están migrando sus esfuerzos al desarrollo de *software* que aumente las capacidades de otros sistemas militares y al desarrollo de un abanico de sistemas no tripulados que crece sin cesar.

Además de los más visibles UAS, existe un sector que finalmente toma velocidad de crucero: los UGV. Los vehículos terrestres no tripulados, hasta la guerra, eran sistemas de industria de defensa pura. Su desarrollo en todo el

[15] La mayor plataforma de patronazgo del mundo. Los seguidores de un creador de contenidos, artista, personas afines a una causa... pueden donar la cantidad periódica que prefieran empleando la plataforma.

mundo ha sido más lento que el de los UAS por la dificultad que conlleva la navegación por distintos entornos terrestres. De hecho, se tenía a la industria rusa como una de las líderes mundiales, hasta que la guerra ha demostrado que sus flamantes blindados no tripulados eran la versión UGV de los pueblos de Potemkin[16]. Por más que la industria puramente militar rusa o ucraniana de UGV no haya acabado de despegar, pequeñas *startups* están haciendo lo que saben hacer mejor: ser ágiles y desarrollar sistemas simples y económicos para tareas que ahora se revelan esenciales: el transporte, suministro y evacuación de heridos en los últimos kilómetros antes de la línea de contacto. Hasta que los UAS de carga se adquieran en número suficiente, para determinadas posiciones defensivas estos vehículos salvan vidas.

Existen, además, los USV (*Unmanned Surface Vehicles*, buques no tripulados de superficie). Una de las mayores sorpresas tecnológicas de la guerra y esta vez carentes de precedentes. En la más pura línea *chimple*, se trata de diseños que posiblemente no lleven ni un año en pruebas. Completamente desconectados de la tendencia previa mundial en USV —navíos de mayor porte, en ocasiones opcionalmente tripulados y por supuesto *expenplex* y poco aptos para el uso en masa— estos sistemas han combinado la simplicidad con la comunicación satelital para lograr éxitos que habrían hecho las delicias de los integrantes de la 10.ª Flotiglia MAS original. Han protagonizado el éxito individual más apabullante de los sistemas no tripulados en la guerra, al derrotar a la mayor Armada del Mar Negro, y suponen por sí mismos otra caja de pandora más: la letalización de productos civiles aún más económicos es una amenaza para instalaciones litorales y aún buques en aguas marrones que necesita de respuesta urgente, sobre todo dado que está al alcance de actores no estatales.

Una de las reacciones más decididas en esta línea vino de fuera de Defensa. Concretamente, del Ministerio de Transformación Digital, con Mijailo Fedorov a la cabeza. Antes de la guerra habían impulsado iniciativas de alto impacto para la e-administración y el desarrollo digital del país. Pero a la hora de la verdad actuaron con decisión y rapidez. Tras sacar en tiempo récord los servicios digitales esenciales a una nube securizada en el exterior y apoyar al recepcionado de los servicios prestados por Palantir en esos momentos críticos, el Ministerio puso en marcha una serie de iniciativas, una detrás de otra, con las que apoyar sin descanso el crecimiento del ecosistema de drones (entre otros). Aprovechando las experiencias previas de su equipo en el Ministerio, las iniciativas de Fedorov facilitaron, entre otros:

— United24, la iniciativa de búsqueda de solidaridad internacional más importante. Dentro de ella destaca Army of drones, un llamado

[16] Grigori Potemkin erigió pueblos falsos con fachadas elaboradas para impresionar a la emperatriz Catalina II durante su viaje por Crimea en 1787, ocultando la pobreza de la región.

a la solidaridad internacional focalizada en los drones, dirigida al gran público occidental y de gran éxito. Con figuras de talla mundial poniendo literalmente la cara, lograron que los drones simbolizaran la resistencia y el apoyo a la causa ucraniana
- People's drones, iniciativa para diseminar por todo el país el montaje de drones FPV.
- Brave1, clúster de war startups creado en conjunción con el Ministerio de Defensa y otros ministerios para apoyar multidimensionalmente la actividad y el crecimiento de las startups.

La suma de estos actores genera un ecosistema de innovación sin precedentes y que merece mucha atención, ahora y en el futuro. Hay que asumir que, de momento, falta una pieza importante: uno o varios campeones nacionales o aún midcaps que vehiculen toda esta ebullición creativa y la ayuden a escalar. Si las *war startups* están para quedarse y ahora mismo juegan un papel crítico en la carrera de innovación que ayuda a mantener a Ucrania en la guerra, también es cierto que presentan obvias limitaciones a la hora de escalar y maximizar la producción de sistemas físicos.

Evidentemente, una industria post-soviética tampoco es la solución salvo en los casos de más inmediata necesidad como la fabricación de munición de todo tipo. Por otra parte, no es inmediato ni baladí poner en marcha una o más plantas de fabricación enfocadas a un modelo productivo 4.0., donde la robótica, la sensorización, el mantenimiento predictivo y la gestión logística avanzada pueden lograr tanto producción como flexibilidad imposible para un modelo taylorista previo. Los recursos de los aliados europeos a este respecto están a la cabeza mundial y probablemente se den decisivas sinergias a no mucho tardar.

13 Modificaciones: materiales, frecuencias

Para fianlziar, se hará una revisión de algunas de las últimas tendencias en el campo de los drones comerciales letalizados.

Por una parte, se extiende el uso de materiales alternativos a la fibra de carbono para la carcasa de los cuadricópteros. Hay que tener en cuenta que la fibra de carbono es un material de manipulación y corte complejos debido al entrelazamiento de las fibras. Esto impide la fabricación en talleres pequeños y de recursos limitados. Como quiera que la mayoría de los filamentos empleados para la impresión 3D no son aptos para los esfuerzos mecánicos que generan los drones FPV, los materiales alternativos que se están ensayando y empleando son:

- Policarbonatos de alta resistencia fabricados por inyección.
- Madera de balsa.
- Aluminio.

Cada uno presenta diferentes ventajas de cara al eco radar, al peso o la economía. Sin embargo, lo más importante en todos los casos es que permite aprovechar infraestructura industrial previa y asegurar que los armazones o *frames* de fibra de carbono nunca sean un cuello de botella para la fabricación. Además, los drones de FPV de mayor tamaño empleados (9 y 10 ") generan semejante empuje que convierten el aumento de peso comparado con la fibra de carbono en algo irrelevante.

Después están las radios. Como se ha venido indicando, su evolución reciente se ha acelerado. A fecha de marzo de 2024, grupos de *hackers* de ambos contendientes han avanzado mucho en la modificación del *firmware* ELRS, de manera que emisores y receptores pueden emplear bandas muy alejadas de las originales. Esto dificulta la detección empleando los escáneres más populares y, por lo tanto, baratos y simples, y saca de la ecuación a aquellos inhibidores no preparados para lidiar con las nuevas bandas.

Este desarrollo es un *stop-gap* a la espera de que maduren algunas de las distintas iniciativas de creación desde cero de radios y protocolos de control basadas en radio definida por *software*. El desafío es mayor que el *hacking* ELRS, pero a cambio el cielo (radioeléctrico) es el límite: por encima del límite de 433 MHz, cualquier frecuencia puede ser empleada para transmitir paquetes con el ancho de banda y la latencia que se necesita para el control de los drones.

Otro desarrollo que madura rápidamente es el de redes *mesh* completas o híbridas. Requieren de *hardware* más complejo, caro y pesado que los pocos gramos de un RX convencional de dron, pero a cambio permiten que muchos más drones (nodos en una red, en este caso) empleen las mismas bandas de frecuencia a la vez. De cara a mantener una latencia y alcance aceptables, se están probando arquitecturas de dron nodriza, por las cuales los drones en la zona de operaciones emplean una red mesh conectada al dron nodriza, quien a su vez retransmite el conjunto total de información a la estación de control en una arquitectura comparable a la antaño popular wifi-wimax. Eso sí, plantea la dificultad de que el derribo de un dron nodriza provocaría la pérdida de control del resto de la formación. Hay que señalar que no se trata de un enjambre al ser cada nodo de la red pilotado por un operador humano.

Para concluir, hasta la fecha los desarrollos más importantes de capacidades autónomas, ya se ha mencionado la navegación con GNSS denegado y la guía terminal autónoma. No hay información en abierto sobre un salto decisivo de capacidades y, además, hay que tener en cuenta que el aquí y el ahora necesita solución, y que miles de mentes enfocadas en ganarle la partida al contrario van a seguir dando más y mejores resultados que sistemas autónomos, caros, complejos y probablemente menos flexibles.

De la misma manera, los «drones antirradiación» que empleen como guía la emisión RF de los inhibidores, están cerca de su puesta en servicio. Se trata de un problema complejo cuando no se pueden emplear antenas suficientemente separadas; con todo, hay indicios suficientes como para dar por bueno un TRL6 o incluso 7, empleando antenas más ligeras y sencillas y discriminando por *software*. Cuando este tipo de efectores se pongan en servicio en número suficiente se producirá una vuelta de tuerca al actual equilibrio del campo de batalla, de consecuencias imposibles de prever.

14 Conclusión

La tozudez de los hechos masivos relacionados con los drones comerciales letalizados no deja alternativa a la hora de considerar su importancia actual y futura. No solo han venido para quedarse y seguir evolucionando, sino que ya se están empleando por zonas cada vez más amplias del mundo. La generalización de su uso va a traer un goteo incesante de nuevas lecciones aprendidas. Ahora mismo los estudiosos de la letalización de drones comerciales viven el sesgo de Ucrania, dado que es en esta desdichada guerra en la que ha explotado el uso de los DCL. Sin embargo, en otros entornos de guerra de todas las intensidades, grises y de seguridad no militar, los DCL y su doctrina de empleo van a variar sustancialmente. Por ejemplo, si sobre los cielos de Ucrania reinan los drones de carga de 7 a 10 ‘’, en otros escenarios los drones más ligeros y pequeños tienen mucho que decir.

El ecosistema de fabricantes de sistemas C-UAS está en plena transformación. Se está abandonando la excesiva fijación en los drones comerciales tipo DJI y tratando de construir sistemas de sistemas, en muchos casos, basados en el protocolo Sapient. Todas las aportaciones van a sumar probabilidad de mitigación mientras se mantengan al día por separado y juntas, y el papel del integrador va a ser crítico durante mucho tiempo.

Cada vez que el autor ha tenido la oportunidad, se ha mostrado optimista respecto a las posibilidades de la industria española de cara a alcanzar la primacía en este sector. Al ecosistema industrial y tecnológico a todos los niveles, desde las *startups* a las PYMES veteranas y midcaps se unen los campeones nacionales y todos ellos se pueden desarrollar en el conjunto único de espacios disponibles en territorio nacional.

Desde las instalaciones del INTA, pasando por los campos de maniobras, hasta llegar a la amplia variedad de espacios disponibles en la España vaciada, dentro de los límites que marca la normativa para pruebas, se dispone de una ventana de oportunidad que puede mantenerse abierta algunos semestres para situar al ecosistema español a la vanguardia de Europa. Cabe ser optimista y confiar en que las decisiones se tomen a todos los niveles y en los tiempos y las formas adecuadas.

Bibliografía

Chulilla Cano, J. L. (2023). Presente y futuro de los drones comerciales letalizados. *Revista General de Marina*. 284, p. 4.

Chulilla Cano, J. L., Román, J. F. y Villanueva, C. (2024). La guerra de drones en Ucrania. En: Murillo, B. C., López, C. D. V. y Piella, G. C. *La guerra de Ucrania III: De la reconquista de Jersón al estancamiento*. Los Libros de la Catarata.

In Ukraine flight controllers for drones have been developed. (2024). *Revista Militarnyi*. [Consulta: 2024]. Disponible en: https://mil.in.ua/en/news/in-ukraine-flight-controllers-for-drones-have-been-developed/

Kaldor, M. (1983). *The Baroque Arsenal*. Londres. Abacus.

Murillo, B. C., López, C. D. V. y Piella, G. C. (2024). *La guerra de Ucrania III: De la reconquista de Jersón al estancamiento*. Los Libros de la Catarata.

Suleiman, A y Hezaber, H. (2024) *The Syrian regime is stepping up its use of suicide drones* [en línea]. Al-Jazeera. [Consulta: 2024]. Disponible en: https://twitter.com/SAMSyria0/status/1758174017855389802

Taylor, C. (2024). *Preparing to Win the First Fight of the Next War*. Modern War Institute at West Point.

Watling, J. y Reynolds, N. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *Royal United Services Institute for Defense and Security Studies*. 19, pp. 18-20.

Contribución de los satélites de observación de la Tierra con capacidades IMINT a la Seguridad Nacional

Fernando Touceda Rodríguez
Antonio José Medina Fuentes
Arturo Rodríguez Torres

Resumen

Los Sistemas Espaciales de Observación de la Tierra (SEOT) son una fuente de obtención de información que permite la elaboración de la inteligencia asociada a la toma de decisiones que dan respuesta a la inmensa mayoría de las amenazas identificadas en la Estrategia de Seguridad Nacional del 2021. Por otro lado, también se han convertido en un elemento esencial para la preparación y conducción de cualquier operación llevada a cabo por las Fuerzas Armadas españolas.

Para poder comprender las capacidades que proporcionan los SEOT actualmente y las que pueden ofrecer en el futuro, se hace necesario describir cómo han ido evolucionando a lo largo de su corta historia, adaptando sus prestaciones a los últimos avances tecnológicos. Resaltar la reciente irrupción de la inteligencia artificial y de la automatización de procesos a través del *machine learning*, con la aplicación de técnicas para analizar una inmensa cantidad de datos proporcionados diariamente por constelaciones de satélites, cada vez más pequeños y más numerosos.

Los cambios en la doctrina espacial y la rápida evolución de las amenazas sobre estas capacidades, sugieren la necesidad de realizar ciertos cambios para mejorar las capacidades espaciales propias, para adaptarse a las amenazas emergentes, mantener ventajas estratégicas y asegurar la resiliencia y efectividad de estas capacidades de potencias mundiales en un entorno espacial cada vez más competitivo y conflictivo.

Palabras clave

SEOT, Inteligencia artificial, *NewSpace*, Constelación, Revisita.

Contribution of Earth observation satellites with IMINT capabilities to National Security

Abstract

The Earth Observing Systems (EOS) are a source to obtain information that allows the development of intelligence associated with

decision-making that responds to the vast majority of threats identified in the 2021 National Security Strategy. On the other hand, they have also become an essential element for the preparation and conduct of any operation carried out by our Armed Forces.

In order to understand the capabilities that EOS currently provide and those they can offer in the future, it is necessary to describe how they have evolved throughout their short history, adapting their features to the latest technological advances. Highlight the recent emergence of artificial intelligence and process automation through «machine learning», with the application of techniques to analyse a vast amount of data provided daily by satellite constellations, increasingly smaller and more numerous.

Changes in space doctrine and the rapid evolution of threats to these capabilities suggest the need to make certain changes to improve our space capabilities, to adapt to emerging threats, maintain strategic advantages and ensure the resilience and effectiveness of these capabilities of world powers in an increasingly competitive and conflictive space environment.

Keywords

SEOS, Artificial intelligence, NewSpace, Constelation, Revisit.

1 Introducción

La industria del cine realiza producciones cinematográficas de gran impacto para el espectador siempre que en ellas aparecen satélites con capacidades IMINT (Inteligencia de Imágenes), a partir ahora se denominarán como SEOT (Sistemas Espaciales de Observación de la Tierra). Los efectos especiales son tan excelentes que el espectador sale del cine con la sensación de que todo lo que ha visto es real: vídeo persistente sobre una zona con resolución espacial milimétrica, imágenes térmicas que permiten ver personas en el interior de edificios, capacidad para cambiar el horario de paso de los satélites por una zona y otras licencias del guionista incluidas con el fin de que el espectador vea una buena película de entretenimiento.

La física y otros factores impiden las maravillas cinematográficas descritas y establecen las capacidades reales que tienen los SEOT y lo que se puede esperar de ellos en el presente y en el futuro a corto plazo.

Se intentará dar respuesta a estas cuestiones sin olvidar el estado de la industria aeroespacial española, dejando presente que, por motivos de clasificación de la información, se omitirán datos con esta consideración. Se puede afirmar que los SEOT son una fuente de obtención de información que permite la elaboración de la inteligencia asociada a la toma de decisiones que dan respuesta a la inmensa mayoría de las amenazas identificadas en la Estrategia de Seguridad Nacional del 2021 (ESN 21).

Es necesario precisar que, como en otros campos, el desarrollo de los SEOT ha corrido en paralelo a los avances tecnológicos de cada momento. Valga como ejemplo la necesidad de disponer de la imagen lo antes posible, por parte del mando, lo que potenció el desarrollo del sensor opto-electrónico. Es decir, la actual tecnología para obtener fotos en un teléfono móvil tiene su origen en la obtención de imágenes desde cientos de kilómetros de la Tierra.

Hay muchos factores a tener en cuenta en un SEOT, aunque para este artículo se pueden utilizar tres que básicamente lo caracterizan: el sensor que obtiene la imagen, la plataforma que proporciona todos los servicios necesarios para que el sensor obtenga las imágenes y se almacenen, y las comunicaciones que permitirán transmitir la imagen a la Tierra para su posterior análisis.

El recorrido de este artículo finalizará con los desafíos de las capacidades espaciales ante las amenazas emergentes y actuales.

2 Limitación orbital. Capacidad de la constelación

Las fórmulas que permiten conocer la velocidad de un satélite alrededor de la Tierra, en función de la altura sobre esta, son sencillas. Hasta los


SISTEMAS ESPACIALES DE OBSERVACION DE LA TIERRA
OPERADOS POR LAS FAS 1995-2024
CUSTODIÆ PACIS
CIFAS
CESAEROB


HELIOS 1A
JUL95-ENE12
HELIOS 1B
DIC99-OCT04
HELIOS 2A
DIC04-DIC21
HELIOS 2B
DIC09-DIC21
PLÈIADES HR-1A
DIC11-FEB13
PLÈIADES HR-1B
DIC12-FEB13
MAXAR
ENE22-DIC22
GEOEYE-1
WORLDVIEW-1
WORLDVIEW-2
WORLDVIEW-3
CSO RECO-1
DIC18-PRESENTE
CSO IDENT
DIC20-PRESENTE
PAZ
FEB18-PRESENTE
CSO RECO-2
DIC24-PRESENTE

estudiantes de la ESO pueden resolver problemas relacionados con órbitas. Indicar fórmulas excede de este artículo, por lo que solo cabría precisar que, un SEOT en órbita polar, a una altura en el entorno de los 600 km, tiene las siguientes características:

- La velocidad del satélite es de 25 000 km/h.
- El tiempo en realizar una vuelta alrededor de la Tierra (una órbita), estaría entorno a los noventa minutos. La mitad de ese tiempo en la Tierra es de día y la otra es de noche, definiéndose, respectivamente, como ciclos diurno y nocturno de la órbita.
- Los satélites no necesitan combustible para mantener la velocidad indicada, su motor son las leyes de Kepler, pero sí que demandan propelente principalmente para mantener la altura, puesto que la fuerza de la gravedad de la Tierra hace que se degrade paulatinamente. Para ello, disponen de propulsores que permiten corregir su altura, realizar otras maniobras menores para minimizar el riesgo de colisiones con otros artefactos o con restos espaciales, así como correcciones de actitud para mantener su orientación con respecto a la Tierra.
- Con la velocidad indicada, los satélites alcanzan, en un día, alrededor de quince órbitas sobre la superficie terrestre. Como bien se sabe, la Tierra no está estática y, como resultado de su movimiento de rotación, la distancia en el Ecuador de dos órbitas consecutivas puede alcanzar unos 2700 km. La rotación y la configuración orbital polar, van a ser los factores que permitan que el satélite pueda acceder a prácticamente toda la superficie terrestre y, en función de la latitud de la zona, ancho de toma, número de satélites y capacidad de balanceo, se podrá cubrir el mismo punto de la superficie terrestre en uno o varios días.
- Hay un parámetro fundamental que se define durante el diseño de la órbita del satélite: la hora del paso por el Ecuador. Los SEOT se diseñan para que en el ciclo diurno de la órbita pasen por un lugar determinado siempre a la misma hora local solar, privilegiando la obtención de un hemisferio. Este tipo de órbitas se denominan «heliosíncronas». De esta manera, imágenes tomadas del mismo punto de la superficie terrestre en diferentes fechas, tendrán las mismas condiciones de iluminación, facilitándose así la labor del fotointérprete. Lo mismo ocurriría en el ciclo nocturno de la órbita.

La principal conclusión que se extrae de las características indicadas es que un solo satélite no permite acceder todos los días a cualquier parte de la superficie terrestre, su resolución temporal es baja y siempre pasa a la misma hora por un lugar determinado. Cómo se obtiene uno o varios accesos diarios a una misma zona: con una constelación compuesta por varios satélites en diferentes órbitas de tal modo que, a mayor número de

satélites, mayor número de accesos diarios. Por tanto, cuando se habla de resolución temporal de Pléiades, CSO, Blacksky, Skysat, entre otros, se hace referencia al acceso diario a una zona que permite la constelación de satélites que lo forman.

3 Capacidades de los SEOT actuales y futuro

Antes de describir el estado actual se darán unas pequeñas pinceladas históricas de los SEOT, recordando que los satélites son un reflejo de la tecnología existente en cada momento.

El 4 de octubre de 1957 la URSS, con el Sputnik, es el primer país que logra lanzar un satélite artificial con una carga útil dedicada a medir diversos parámetros de la atmósfera. Tuvo una vida útil de tres semanas. A los tres meses y tras completar 1440 órbitas, se desintegró en su reentrada a la atmósfera. Este fue el primer hito de la llamada «carrera espacial» de los EE. UU y la URSS, que culminó con el americano Neil Armstrong pisando la superficie lunar el 20 de julio 1969.

Los EE. UU. trabajaron en varios proyectos, todos clasificados, destacando el programa secreto Corona, desarrollado por la CIA. Consistente en un programa de reconocimiento de la Tierra y en el contexto de la Guerra fría, permitió desde 1960 hasta 1972, la obtención de fotografías[1] de zonas de la URSS y de otros potenciales adversarios. El 19 de agosto de 1960 la CIA recuperó las primeras imágenes de este satélite, mediante una cápsula de reentrada en la atmósfera y su posterior captura desde un avión.

Desde finales de los años cincuenta y hasta mediados de los ochenta, la tecnología para obtener imágenes era la fotográfica (procesos químicos) y, atendiendo a los factores principales de un satélite, se consideraban las siguientes características:

- El sensor era un objetivo de alta calidad óptica.
- La plataforma albergaba un contenedor de película con una bobina de acetato de sales de plata que podía llegar hasta los 10 000 m.
- Las comunicaciones consistían en separar la cápsula que albergaba la película ya sensibilizada a la Tierra y, en su fase final, ralentizar su llegada con el despliegue de un paracaídas y la recuperación por un avión, mediante una canasta de recogida diseñada al efecto. Ni que decir tiene, que varias cápsulas nunca fueron recuperadas. Una vez en tierra se realizaba el procesado químico de revelado de la película y su posterior envío a los analistas de imagen.

[1] Sin entrar en definiciones conceptuales, una fotografía es aquella obtenida por procesos químicos, teniendo como material sensible una emulsión de sales de plata sobre un acetato o cristal, mientras que una imagen es la obtenida utilizando dispositivos que transforman la luz en datos digitales que forman la misma.

Con la misión del Discover XIII de los EE. UU, lanzado el 10 de agosto de 1960, se consigue recuperar, por primera vez en la historia, un objeto lanzado al espacio, en este caso la cápsula con la película sensibilizada.

Con el paso de los años, los satélites mejoran sus prestaciones en relación al instrumento óptico, las bandas del espectro electromagnético que adquirían y la resolución espacial. Pero seguía siendo necesario el envío de la película fotográfica a la Tierra, que ralentizaba el acceso a la información por parte de los fotointérpretes. Conscientes de esta limitación, la Fuerza Aérea Americana y la Central de Inteligencia Americana, promueven la investigación de sensores que no utilizasen técnicas fotoquímicas para la formación de la imagen, desarrollando el CCD (dispositivo de carga acoplada) como sustituto de las sales de plata. La cinta magnética regrabable, en lugar de la película fotográfica, como soporte de almacenamiento masivo a bordo del satélite[2]. Todo ello junto con la posterior transmisión de la señal portadora de la imagen a antenas receptoras en tierra. El 19 de diciembre de 1976, con el lanzamiento de un satélite americano denominado KH-11, comienza la era digital de los SEOT.

El estado actual de los SEOT está teniendo un desarrollo que solo puede calificarse como espectacular. Hay SEOT que, al no poder descargar la imagen obtenida inmediatamente a una antena receptora en tierra, la envía a satélites geoestacionarios para su descarga en estaciones terrenas, disminuyendo significativamente la latencia y el tiempo necesario para que la imagen esté a disposición del analista.

Los SEOT convencionales ópticos y radar como son el PAZ, CSO, CosmoSkymed NG y Pléiades, entre otros, se han adaptado al tiempo actual. La mayor parte de ellos son de uso dual (civil/militar) para repartir los altos costes de diseño, fabricación y lanzamiento. Permiten a los países participantes disponer de una soberanía y discreción en el empleo militar del SEOT, fiabilidad de los diferentes subsistemas que lo forman y una alta vida útil.

La irrupción del concepto «NewSpace», consiste en empresas con capital privado que desarrollan, en breve tiempo, necesidades concretas de clientes en plataformas pequeñas (mini satélites). Los costes de puesta en órbita son relativamente pequeños, al asociarse diferentes proyectos de empresas en un solo lanzamiento. Hace quince años el club de los países que tenían un SEOT era muy limitado, ahora, cualquier país tiene la posibilidad de poner en órbita un SEOT aunque esté muy limitada la calidad de la imagen, la recepción y explotación de la información obtenida y el tiempo en órbita (normalmente pocos años).

[2] Actualmente son discos duros de varios TB de almacenamiento.

El «NewSpace» está permitiendo el desarrollo de grandes constelaciones de satélites comerciales pequeños con altas resoluciones espectrales, temporales y espaciales. Valga como ejemplo la constelación Albedo[3] que tiene previsto el lanzamiento de sus primeros satélites (hasta un total de veinticuatro) para la primera mitad de 2025, con una resolución espacial de 10 cm en la banda pancromática, 40 cm en las bandas multiespectrales (rojo, verde, azul e infrarrojo cercano), 2 m en la banda del infrarrojo lejano (térmico) y, con la constelación completa, seis accesos diarios a cualquier parte de la superficie terrestre.

El «NewSpace» podría ser un complemento ideal para los SEOT tradicionales, teniendo presente que la discrecionalidad que ofrece el convencional difícilmente se podrá alcanzar con estas nuevas constelaciones, en su mayoría comerciales.

Otro concepto de actualidad muy relacionado con la información que proporcionan los SEOT, es la inteligencia artificial (IA). Uno de los valores añadidos que proporciona esta tecnología es la entrega de un producto elaborado automáticamente que sirva a las necesidades del cliente (detección de cambios e identificación de materiales, entre otros) utilizando procesos IA en tierra, e incluso a bordo del mismo satélite.

En cuanto al futuro de los SEOT, solo se puede a hablar a corto plazo (cinco a diez años) señalando las siguientes características:

- Miniaturización de componentes, permitiendo satélites más pequeños, menos pesados y más agiles.
- Aumento de la vida útil del SEOT con la sustitución del combustible sólido por propulsión eléctrica para realizar las necesarias correcciones orbitales en altura, evasión de artefactos y actitud del satélite, entre otros.
- Alta calidad en los productos procesados a bordo a partir de las imágenes obtenidas gracias a la evolución de la IA y desarrollos asociados a la misma, como el deep learning.
- Aumento del número de bandas espectrales obtenidas.
- Mayor número de accesos diarios a una zona gracias a constelaciones numerosas de satélites, combinado con diferentes inclinaciones orbitales de los mismos.

4 Capacidades actuales y futuras de los SEOT en las FF. AA.

Las Fuerzas Armadas españolas, conscientes de la necesidad de obtener imágenes con fines de inteligencia militar que permitan al mando realizar una adecuada estimación de los riesgos, firmó con Francia e Italia

[3] Página oficial SEOT Albedo (marzo 2024). Disponible en: https://albedo.com

su adhesión al programa del SEOT óptico Helios 1, lanzándose el primer satélite en 1995. Con posterioridad se participó en el programa del SEOT óptico Helios 2 y el SEOT dual Pléiades HR-1[4]. Con la finalización del programa Helios 2, en diciembre de 2021, y mediante acuerdo bilateral con Francia, se está participando en la actualidad en el SEOT óptico CSO[5]. Por otro lado, al objeto de que las FF. AA tuviesen la capacidad de obtención todo el tiempo, el Ministerio de Defensa firmó, en 2008, un acuerdo marco con la empresa Hisdesat por el que se recibirían diariamente una cuota determinada de imágenes del satélite PAZ, que dispone de un instrumento de radar de apertura sintética (SAR). El lanzamiento del satélite PAZ tuvo lugar en febrero de 2018, desde la Base de Vandenberg (California). Según Hisdesat, las últimas previsiones de vida del sistema hacen indicar que estará operativo hasta 2034.

Los recientes conflictos armados en Ucrania y en la franja de Gaza, en los que existe un gran número de actores con intereses de información sobre estas zonas, han puesto de manifiesto la dificultad que existe a la hora de obtener una imagen satélite sobre áreas en conflicto. Las grandes potencias disponen de contratos con los principales proveedores comerciales, que copan la capacidad de obtención para el resto de usuarios en estas zonas. Por otro lado, en los sistemas multinacionales gubernamentales, el país con el mayor porcentaje de participación actúa de la misma forma, y dificulta la obtención de aquellos gobiernos con menor porcentaje.

El empleo operativo del SEOT PAZ, a través de un modelo de uso dual del sistema (militar-civil), provee a las FF. AA la capacidad de obtener imágenes radar de forma discreta, prioritaria e independientemente de las condiciones atmosféricas.

Considerando lo anterior, solo los SEOT de fabricación y explotación nacional pueden proporcionar la flexibilidad necesaria para apoyar una respuesta autónoma en un escenario de interés prioritario para España y dicha información no tiene que ser conocida o estar controlada por un gobierno extranjero o por una compañía comercial.

Todo parece indicar que la industria nacional está en condiciones de acometer este reto tecnológico. Por tanto, desde el Ministerio de Defensa, se está haciendo lo posible para tratar de impulsar el desarrollo de sistemas nacionales en los espectros visible, infrarrojo y radar, para que en el futuro se pueda dotar a las FF. AA de estas capacidades de una forma autónoma, discreta y prioritaria.

[4] La operación de este sistema, por parte de las FF. AA, finaliza en 2012 por falta de recursos económicos.

[5] El acuerdo técnico con Francia contempla la adhesión al programa CSO por un periodo inicial de cinco años que comenzó en febrero de 2024, más otro opcional de otros cinco años, por lo que la operación del sistema se podría alargar hasta 2034.

Tener este tipo de capacidades nacionales, implicará un incremento considerable de las imágenes que se reciben a diario, pero con similar capacidad de análisis de la información que se dispone actualmente y que se traducirá en que:

— Las herramientas de inteligencia artificial y machine learning jugarán un papel muy importante en el futuro.
— El flujo de trabajo actual tendrá que ir cambiando a un sistema automático de indicadores y alertas[6], que advierta al analista solo de aquellas imágenes en las que se detecte algo relevante que haya sido previamente definido[7].

Todo esto sin olvidarnos de las posibilidades que se puedan ofrecer en el futuro a través del concepto «NewSpace», si la industria nacional es capaz de llegar a resoluciones espaciales por debajo de los 50 cm, con grandes constelaciones de satélites pequeños que mejoren considerablemente la capacidad de revisita, la posibilidad de captura de vídeo y el procesado de las imágenes a bordo con herramientas de IA. Impulsar desde los estamentos públicos los desarrollos de I+D+i de estas capacidades espaciales, se considera fundamental para poder alcanzar este objetivo.

Todo lo anterior conduce a otro concepto denominado «oportunidad en la obtención»[8]. La tecnología está consiguiendo actualmente capacidades de los SEOT inimaginables en el siglo pasado, que junto con la apuesta de la empresa privada por el acceso al espacio, está permitiendo constelaciones de diferentes SEOT, trasvases de imágenes entre los mismos para su descarga en antenas de recepción terrenas y su inmediata puesta a disposición de los analistas de imagen. A corto plazo, no cabe duda que permitirá, con la adecuada y permanente financiación en el tiempo, estar en condiciones de comunicar al mando que su necesidad puede ser cubierta en un plazo de unas horas desde su solicitud.

[6] La Estrategia de Seguridad Nacional 2021 promueve el desarrollo de capacidades nacionales para hacer frente a situaciones de crisis, a través de un sistema de indicadores críticos de los distintos ámbitos de la Seguridad Nacional, cuya monitorización y análisis permitan desplegar acciones preventivas y, llegado el caso, la ejecución de medidas de respuesta y conducción en tiempo oportuno.

[7] Por ejemplo, si se está haciendo el seguimiento de actividad aeronáutica en una determinada base aérea, el sistema de IA debería alertar de forma inmediata al analista de imágenes, si se obtiene una imagen en la que ha variado el número de aeronaves respecto de la obtenida anteriormente.

[8] La oportunidad en la obtención se define como un conjunto de acciones que deben permitir, ante una crisis de cualquier tipo, estar en condiciones de poder satisfacer los requerimientos IMINT del mando o autoridad en el menor tiempo posible, de tal forma que se contribuya a disminuir los tiempos de respuesta a las crisis permanentes y emergentes, tal y como se establece en la ESN 21.

5 Desafíos de las capacidades espaciales ante las amenazas emergentes y actuales

Durante décadas se ha seguido el método de pasar años desarrollando costosos satélites y luego programar lanzamientos para ponerlos en órbita con meses o más tiempo de antelación. Una vez situados, esos satélites permanecen en sus órbitas, preservando la mayor cantidad de combustible posible, porque cuando ese combustible se haya consumido, su vida útil se habrá terminado.

Ante la rápida evolución de las amenazas que se están produciendo sobre las capacidades espaciales, actualmente se está repensando la anterior fórmula mediante la planificación, construcción y el lanzamiento en órbita de grandes constelaciones de satélites mucho más pequeños. Este concepto permite la estrategia de resiliencia del servicio.

Además, se está añadiendo un nuevo reto: operaciones dinámicas. Ya sea entregando satélites en órbita en días, maniobrando los satélites con más frecuencia y de forma activa, o repostándolos en órbita, se está empezando a remodelar los conceptos operativos para responder y mantenerse a la vanguardia en un dominio cada vez más complejo e impredecible.

La rapidez de puesta en órbita y la resiliencia en órbita se han convertido en principios fundamentales que se deben alcanzar para minimizar el impacto que las actuales y futuras amenazas tienen sobre las capacidades espaciales.

La urgencia de estos nuevos requisitos está impulsada por las amenazas que los operadores ven hoy en día, donde China, Rusia y otros tienen la capacidad de destruir satélites cruciales, cegando potencialmente a sus adversarios, principalmente a Estados Unidos, pero también a otras naciones con capacidades espaciales.

La doctrina espacial de Estados Unidos de junio de 2020 incluía la Movilidad Espacial y la Logística (SM&L) entre las cinco competencias básicas que la USSF necesitaba demostrar.

Fundamentalmente, SM&L incluye «el movimiento y el apoyo del equipo y personal militar... a través del dominio espacial», así como la capacidad de sostener, actualizar y recuperar naves espaciales en órbita, según esta doctrina.

Sin embargo, el concepto ha evolucionado con el tiempo. Actualmente se habla de maniobras casi continuamente, de modo que el satélite, ante cualquier detección de amenaza, muestre que está maniobrando y está cambiando constantemente su órbita, preservando la misión, pero cambiando su órbita.

Tal maniobra no es posible con los satélites que los EE. UU. tienen actualmente en órbita, que solo se lanzaron con suficiente propelente para mantenerse en su situación y nunca fueron diseñados para ser reabastecidos.

Uno de los principios de la guerra es la maniobra. Así que ahora en el dominio espacial aparece la necesidad de aplicarlo también. Esto es el futuro y queda un largo camino por recorrer antes de que el reabastecimiento espacial sea rutinario. Pero la industria está dando respuestas a estos conceptos mediante puertos de reabastecimiento en el espacio (*startup* Orbit Fab).

Northrop Grumman está ofreciendo reabastecimiento de combustible en órbita a través de su subsidiaria, SpaceLogistics. El proveedor determinados Blue Origin presentó recientemente su Blue Ring, una nueva nave espacial «enfocada en proporcionar logística y entrega en el espacio», incluido el combustible. Este tipo de capacidades van a complicar el cálculo del adversario. Va a desafiar su pensamiento.

El reabastecimiento de combustible no es el único cambio importante que viene en la forma en la que se hace necesario responder a las nuevas amenazas y requisitos. EE. UU. también está avanzando con su programa Tactically Responsive Space (TacRS), para llevar los satélites a la órbita más rápido que nunca. La capacidad de mover esos satélites y, si es necesario, reemplazarlos rápidamente, cambia los cálculos de costos de cualquier adversario.

Sin embargo, ser más dinámico y receptivo vendrá con posibles desafíos. El mando y el control (C2) en el espacio está a punto de volverse mucho más complejo si los satélites suben más rápido que nunca y se mueven una vez que alcanzan la órbita, especialmente teniendo en cuenta los efectos catastróficos que puede tener una colisión en el espacio. Es necesaria mucha más capacidad C2.

Este enfoque más flexible cambia «la forma de hacer conciencia del dominio espacial». Hacer un seguimiento de un objeto que se mueve dinámicamente es fundamentalmente diferente a cualquier cosa que se hace actualmente. Eso plantea desafíos para una potencia como es EE. UU., pero desafíos aún mayores para los posibles adversarios.

Los cambios en la doctrina espacial y nuevos requisitos, como los mencionados anteriormente, sugieren la necesidad de realizar ciertos cambios para mejorar las capacidades espaciales propias, como lanzar satélites más rápido, tener constelaciones mayores y tener resiliencia en órbita mediante maniobrabilidad, capacidad de repostaje, respuesta dinámica de cambio de posición o de órbita ante una detección de amenaza.

Se pueden identificar algunos cambios requeridos para conseguir la mejora de las capacidades espaciales ante las amenazas potenciales actuales y futuras:

- Lanzamiento de satélites más rápido: para satisfacer la demanda de capacidades de respuesta rápida, simplificar el proceso de lanzamiento de satélites y reducir los tiempos de implementación son esenciales.
- Constelaciones mayores: aumentar el número de elementos que componen las constelaciones de satélites puede mejorar la cobertura, la redundancia y la flexibilidad operativa en las actividades espaciales.
- Resiliencia en órbita:
  - Maniobrabilidad: los satélites con capacidades de maniobra mejoradas pueden evitar amenazas y adaptarse a las dinámicas orbitales cambiantes.
  - Capacidad de repostaje: introducir mecanismos de repostaje puede extender la vida útil de los satélites y mejorar la capacidad operativa de maniobra.
  - Respuesta dinámica a amenazas: implementar sistemas de detección de amenazas en tiempo real y mecanismos de respuesta automatizada rápida pueden garantizar respuestas inmediatas ante potenciales peligros mediante cambios de posición o de órbita.

En conclusión, integrar estos cambios en los Sistemas Espaciales de Observación de la Tierra será fundamental para adaptarse a las amenazas emergentes, mantener ventajas estratégicas y asegurar la resiliencia y efectividad de estas capacidades de las potencias mundiales en un entorno espacial cada vez más competitivo y conflictivo.

Bibliografía

Defense Space Strategy. (2020). Department of Defense of United States of America.

Doctrina de Operaciones en el Ámbito Aeroespacial. (2022). *Publicación Doctrinal Conjunta PDC-3.3*. Estado Mayor de la Defensa.

Gosnold. (2017). Smallsat constellations [en línea]. *SatelliteObservation*. [Consulta: 7 de enero de 2024]. Disponible en: https://satelliteobservation.net/2017/02/11/smallsat-constellations /

Hadley, G. (2024a). Fast & Flexible Space. *Air & Space Forces Magazine*. Vol. 107, N.º 1 y 2. ISSN: 0730-6784. [Consulta: 2024]. Disponible en: https://www.airandspaceforces.com/article/fast-flexible-space/

—. (2024b). SPACECOM Boss: 'It's Time' to Embrace In-Orbit Servicing, Refueling for Satellites. *Air & Space Forces Magazine*. [Consulta: 2024]. Disponible en: https://www.airandspaceforces.com/spacecom-boss-its-time-to-embrace-in-orbit-servicing-refueling-for-satellites/

Lang, S. W. (2016). *Project Corona: America's first photo reconnaissance satellite*. [Consulta: 2024]. Disponible en: https://www.army.mil/article/173155/project_corona_americas_first_photo_reconnaissance_satellite

Martínez Cortés, J. M. (s. f.). *El espacio ultraterrestre. Necesidad de una estrategia de defensa*. Instituto Universitario General Gutiérrez Mellado,UNED. [Consulta: 2024].

Presidencia del Gobierno. (2021). *Estrategia de Seguridad Nacional 2021*. [Consulta: 2024]. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

Secretary of the Air Force Public Affairs. (2023). Remarks by CSO Gen. Chance Saltzman at the Space Force Association Spacepower Conference, Published Dec. 20, 2023. *United States Spaces Force*. ORLANDO, Fla. (AFNS). [Consulta: 2024]. Disponible en: https://www.spaceforce.mil/News/Article-Display/Article/3623358/remarks-by-cso-gen-chance-saltzman-at-the-space-force-association-spacepower-co/

Inteligencia de datos en apoyo a la toma de decisiones para la Seguridad Nacional

Jose Luis Delgado Gamella
Alvaro Alfaro Guillén
Vicente de Ayala Parets

Resumen

La inteligencia de datos es crucial para la Seguridad Nacional, especialmente ante amenazas complejas como la guerra híbrida. Se requiere un enfoque multidominio y contramedidas estratégicas con detección temprana de amenazas. La arquitectura de sistemas debe ser distribuida y resiliente frente a ataques cibernéticos. La evolución hacia la analítica de datos, incluyendo *big data* e inteligencia artificial, permite un análisis profundo y detección temprana de patrones, mejorando la toma de decisiones. La clasificación tradicional de fuentes incluye HUMINT, SIGINT, IMINT, COMINT y OSINT, con fuentes adicionales como la ciberinteligencia y datos financieros.

Se necesitan tecnologías que procesen grandes volúmenes de datos, sean escalables, integren múltiples fuentes y garanticen seguridad y resiliencia. La recopilación de datos implica métodos de extracción, transformación y almacenamiento. Tanto el análisis convencional, con técnicas de *business intelligence*, como el análisis avanzado, que emplea métodos como el análisis de series temporales, la agrupación de datos, el análisis de sentimientos y modelos de lenguaje de gran tamaño, son fundamentales para extraer conocimientos y predecir eventos en Seguridad Nacional. Todos estos aspectos son introducidos en el artículo destacando aplicaciones de la inteligencia de datos en la Seguridad Nacional y resaltando su importancia en la prevención y gestión de amenazas.

Palabras clave

Inteligencia de datos, Seguridad Nacional, Inteligencia artificial, *Big data*, Multidominio.

Data intelligence to support National Security decision-making

Abstract

Data intelligence is crucial for National Security, especially against complex threats such as hybrid warfare. A multidomain approach and strategic countermeasures with early threat detection are required. System architecture must be distributed and resilient against cyber attacks.

The evolution towards data analytics, including big data and artificial intelligence, enables deep analysis and early pattern detection, enhancing decision-making. The traditional classification of sources includes HUMINT, SIGINT, IMINT, COMINT, and OSINT, with additional sources such as cyber intelligence and financial data.

Technologies that process large volumes of data, are scalable, integrate multiple sources, and ensure security and resilience are needed. Data collection involves extraction, transformation, and storage methods. Both conventional analysis, with business intelligence techniques, and advanced analysis, employing methods such as time series analysis, data clustering, sentiment analysis, and large-scale language models, are crucial for extracting insights and predicting events in National Security. All these aspects are introduced in the article, highlighting applications of data intelligence in National Security and emphasizing its importance in threat prevention and management.

Keywords

Data Intelligence, National Security, Artificial intelligence, Big data, Multidomain.

1 Introducción y contexto

El impacto de la inteligencia de datos para la Seguridad Nacional ha sido ampliamente analizado y, debido a la rápida evolución de los sistemas de adquisición de datos de información y el alcance de estos, ha incrementado su importancia en los últimos años. Gobiernos e instituciones deben hacer frente a numerosas amenazas y la identificación de estas se ha convertido en objetivo fundamental para defender los intereses de los ciudadanos.

El panorama, cada vez más complejo, obliga a los gobiernos a analizar las múltiples fuentes de información disponibles a todos los niveles. Los retos más importantes a los que se enfrenta la Seguridad Nacional vienen derivados del contexto multidominio y las amenazas híbridas. El multidominio se podría definir como «Un entorno de actuación muy complejo, que engloba a todos los ámbitos de operación, con una gran interdependencia e interacción entre todos ellos (bien sean físicos o no físicos)». Tradicionalmente solo se tenía en cuenta tres niveles de inteligencia (inteligencia estratégica, operacional y táctica), asumiendo que tienen lugar en ámbitos físicos. Esto está contemplado y plenamente asumido por la doctrina conjunta. Sin embargo, la nueva definición de multidominio requiere la integración de nuevos ámbitos hasta ahora no contemplados como son el cognitivo y ciberespacial.

Por otro lado, en la guerra híbrida, a diferencia de lo que sucede la guerra convencional, el centro de gravedad no se encuentra en el ámbito exclusivamente militar, sino que el enemigo trata de provocar daño usando medios regulares e irregulares (injerencia política, influencia en procesos electorales, desestabilización social, desinformación, etc.). El nivel de intensidad de estas acciones es lo suficientemente alto como para causar el perjuicio, pero a la vez lo suficientemente bajo como para que la mera detección de dichos ataques sea un reto en sí misma.

En este contexto, los avances en la analítica de datos ofrecen a los analistas una herramienta indispensable para poder explotar el número ingente de fuentes de información procedentes de múltiples ámbitos. La inteligencia obtenida en este proceso es esencial para la identificación de amenazas, la prevención y fundamentalmente para la toma de decisiones. Los decisores en materia de Seguridad Nacional deben basar sus acciones, además de en su experiencia y conocimiento, en información sólida y precisa derivada del análisis de datos.

1.1 Operaciones multidominio

Antes de entrar en detalle es importante comprender el origen de los distintos dominios. A la hora de hablar de operaciones tradicionalmente se contemplaba en la doctrina lo que se conoce como operaciones conjuntas,

que son aquellas en las que bajo un mando único intervienen unidades de más de un ejército. Sin embargo, según lo mencionado anteriormente, este concepto no incluye ámbitos relevantes como el ciberespacial. No existe una forma de definir con exactitud un dominio, pero como primera aproximación, puede considerarse la siguiente: «la esfera de influencia en la que se realizan actividades, funciones y operaciones para llevar a cabo misiones para ejercer el control sobre un adversario con el fin de lograr los efectos deseados» (Allen y Gilbert, 2010).

La rápida evolución en las comunicaciones, y la mejora en el manejo de datos que ha supuesto el uso de internet y todo su entorno tecnológico, ha significado un cambio importante en el equilibrio de poder. Ahora la información se ha convertido en un instrumento que garantiza la superioridad, controlar la información es un objetivo fundamental del dominio del ciberespacio.

Si bien las Fuerzas Armadas deben estar preparadas para hacer frente a todo tipo de adversarios, y responder con el grado de intensidad adecuado, se prevé, según el entorno operativo 2035[1], el incremento del «empleo de estrategias no convencionales o híbridas para desestabilizar, deslegitimar o afectar intereses nacionales. Algunas de las acciones empleadas podrían ser las propias de la «zona gris» para dificultar así las posibles respuestas»[2].

Para dar respuesta a estas amenazas se deben considerar los distintos dominios Espacial, Aéreo, Terrestre, Naval, Ciber e incluso cognitivo y, sobre todo, como combinarlos. De este modo las operaciones multidominio son conjuntas, ya que afectan a varios dominios de forma simultánea, complejas debido a la falta de límites tangibles entere los distintos ámbitos, y distribuidas, ya que requerirán la coordinación y control de capacidades en todos los ámbitos.

1.2 *Guerra Híbrida / zona gris*

El concepto de zona gris se ha incluido como parte de los estudios estratégicos para describir conflictos que parten de amenazas híbridas. La definición formal es «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»[3]. Por su

[1] Estado Mayor de la Defensa (EMAD): entorno operativo 2035. Centro Conjunto de Desarrollo de Conceptos. Madrid, 2019. Disponible en: https://publicaciones.defensa.gob.es/entorno-operativo-2035-libros-papel.html

[2] Centro Conjunto de Desarrollo de Conceptos CESEDEN, abril de 2020. Nota Conceptual «OPERACIONES MULTI-DOMINIO».

[3] Centro Conjunto de Desarrollo de Conceptos CESEDEN, abril de 2020. Nota Conceptual «OPERACIONES MULTI-DOMINIO».

naturaleza este tipo de amenazas híbridas, son muy difíciles de identificar y caracterizar. Se trata de acciones que se centran en el uso de medios no convencionales como ciberataques, desinformación y propaganda para desestabilizar a un adversario, que puede tener conciencia de ser amenazado o no.

Esta falta de conciencia sobre las amenazas hace que, sin herramientas específicas, sea realmente difícil prepararse ante amenazas híbridas. En este marco, las herramientas de analítica más innovadoras ofrecen la posibilidad de predecir y prepararse ante estos ataques, en base a la obtención de conocimiento mediante la detección de patrones y generación de escenarios de crisis mediante el modelado.

El documento «El papel de las FAS en la zona gris», publicado por el Estado Mayor de la Defensa, a través del Centro Conjunto de Desarrollo de Conceptos (CCDC) del EMACON, examina las características fundamentales de esta zona gris, que incluye, entre otras acciones a largo plazo, uso de estrategias multidimensionales y la participación tanto de actores estatales como no estatales. En este documento también se destaca el papel esencial de las Fuerzas Armadas en la detección, prevención y respuesta a las agresiones en la zona gris, con especial énfasis en la coordinación entre los distintos instrumentos de poder.

En este punto, se puede afirmar, de forma rotunda, que la guerra híbrida es muy difícil de definir o no existe una definición con autoridad suficiente. Teniendo en cuenta esto, no se puede obviar que, posiblemente, la guerra híbrida no es algo nuevo en la historia de la guerra, si no que ha estado latente en todos los conflictos. Dado que la identificación de conflictos o amenazas híbridas incluye la búsqueda de eventos inesperados, quizá resulte más sencillo enfocar el problema desde otro punto de vista, el objetivo de la guerra híbrida.

Quizá la forma más sencilla de definir el objetivo de este tipo de acciones sea la explotación de las debilidades del oponente en todos los sectores de la sociedad y la capacidad de dañar a un oponente a menudo sin usar poder letal, por ejemplo, mediante el uso de propaganda, engaño o una campaña de información. En este artículo se trata de investigar la inteligencia relacionada con la guerra híbrida, y, para ello, se parte de la definición del MCDC[4], que describió este tipo de conflictos como «el uso sincronizado de múltiples instrumentos de poder adaptados a vulnerabilidades específicas en todo el espectro de funciones sociales para lograr efectos sinérgicos».

[4] *Multinational Capability Development Campaign* (MCDC, por sus siglas en inglés) es una iniciativa liderada por los Estados Unidos diseñada para desarrollar y evaluar de manera colaborativa conceptos y capacidades para abordar los desafíos asociados con la realización de operaciones conjuntas, multinacionales y de coalición.

En esta descripción de la guerra híbrida se amplía aún más la complejidad de este escenario, ya que incluye una nueva amenaza de la guerra híbrida que radica en la capacidad de un actor para sincronizar múltiples instrumentos de poder simultáneamente y explotar intencionalmente la creatividad, la ambigüedad, la no linealidad y los elementos cognitivos de la guerra, todo esto típicamente adaptado para permanecer por debajo de los umbrales obvios de detección y respuesta, es decir tratando de permanecer inadvertido.

Esta descripción proporcionada por el MCDC encaja bien en la problemática expuesta y proporciona un lenguaje común para los conflictos híbridos. Por ese motivo, de ahora en adelante, se propone usarla como referencia para explicar las características principales de estos conflictos.

1.2.1 Concepto de guerra híbrida según el MCDC

El estudio del MCDC explora el concepto de guerra híbrida, desarrollando un modelo conceptual para comprenderla. Este modelo es neutral en cuanto al tipo de agresor, pero se centra en los actores estatales como objetivo principal. Se basa en varias características clave:

— Uso combinado de múltiples instrumentos de poder para lograr asimetría, mediante el ataque a una amplia gama de vulnerabilidades.
— Un paquete de ataque sincronizado que explota tanto ejes horizontales como verticales de escalada.
— Énfasis en la creatividad y ambigüedad para lograr efectos sinérgicos, incluyendo en el dominio cognitivo.

El modelo describe cómo un actor que emplea la guerra híbrida puede utilizar una amplia gama de instrumentos de poder militar, político,

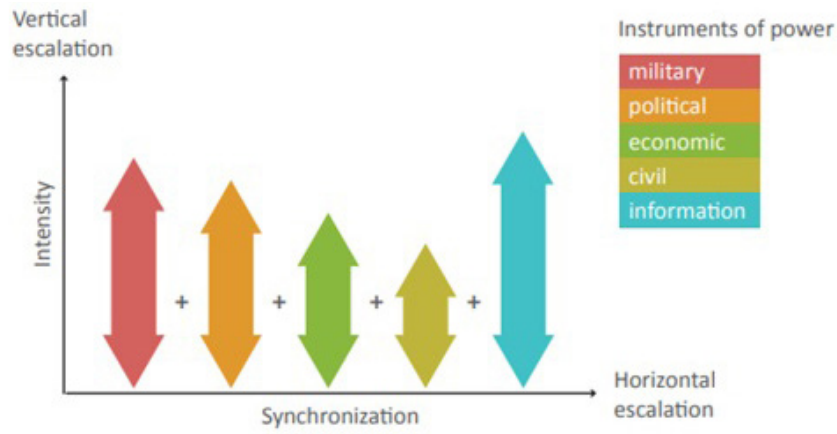

Figura 1. Escala de Guerra Híbrida.Fuente. MCDC Countering Hybrid Warfare Project: MCDC January 2017 Understanding Hybrid Warfare

económico, civil e informativo, dirigidos a las vulnerabilidades políticas, militares, económicas, sociales, informativas e infraestructurales de un sistema objetivo, para escalar tanto vertical como horizontalmente y lograr los objetivos deseados evitando o complicando acciones defensivas.

Se desarrolló un marco analítico para demostrar y visualizar un ataque híbrido, centrándose en las vulnerabilidades PMESII[5] del objetivo, la capacidad del agresor para sincronizar una variedad de instrumentos de poder MPECI[6] y los efectos creados por estas acciones. Este marco incorpora tres elementos interdependientes: funciones críticas y vulnerabilidades, sincronización de medios (escalada horizontal) y efectos y no linealidad.

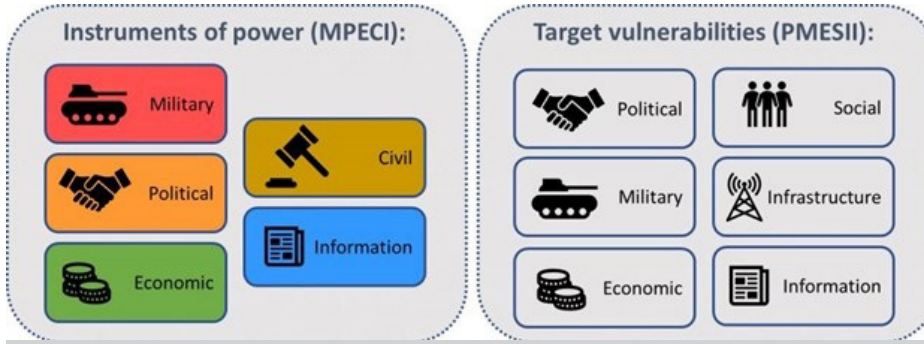

Figura 2. Instrumentos de poder (MPECI) y Vulnerabilidades (PMESII).Fuente. MCDC Countering Hybrid Warfare Project: MCDC January 2017 Understanding Hybrid Warfare

En resumen, se podría describir, en base a todo esto, la guerra híbrida como el uso sincronizado de múltiples instrumentos de poder adaptados a vulnerabilidades específicas.

1.2.2 Contramedidas para las amenazas híbridas

Otra forma de ver los conflictos híbridos es como la capacidad de los agresores para generar efectos y resultados similares a los de la guerra convencional sin necesidad de usar fuerza armada directa. Este tipo de guerra se desarrolla en un continuo de competencia y conflicto entre actores en el escenario internacional.

[5] PMESII (Político, Militar, Económico, Social, Informativo y de Infraestructuras). El modelo PMESII-PT permite, a su vez, estudiar una serie de variables genéricas e interrelacionadas entre sí que permite un conocimiento de la situación estratégica que proporciona la base necesaria para iniciar el proceso de planeamiento operativo a nivel estratégico.

[6] MPECI hace referencia al empleo de todos los instrumentos de poder, del estado y de la sociedad (militar, político, económico, civil e información).

Para contrarrestar la guerra híbrida, es crucial identificar la amenaza y establecer objetivos estratégicos, que de forma resumida consisten en:

— Mantener la capacidad de acción, maximizando las herramientas de poder adecuadas.
— Disuadir a los adversarios de la agresión híbrida, mediante acciones o contramedidas.
— Prevenir la continuación de dicha agresión, mediante el uso de técnicas de prospectiva.

La selección de objetivos estratégicos dependerá del contexto, la intensidad de la amenaza y la capacidad política y operativa para contrarrestarla, pero también en gran medida de las herramientas disponibles para la detección temprana de amenazas.

Para una correcta planificación de contramedidas, cabe destacar la necesidad de establecer umbrales para guiar a los responsables de la toma de decisiones sobre cuándo y cómo responder a la guerra híbrida. En este contexto las herramientas de análisis de datos más avanzadas contribuirán a establecer dichos umbrales.

En el marco del MCDC, se propone un marco integral para contrarrestar la guerra híbrida, que incluye la detección de amenazas híbridas, la disuasión de los agresores híbridos y la respuesta a los ataques híbridos. Este enfoque requiere una comprensión detallada de las tácticas y técnicas utilizadas por los agresores híbridos, así como una coordinación efectiva entre los actores nacionales e internacionales, y para todo ello de nuevo se requiere del análisis de numerosas fuentes de datos y el uso de herramientas de correlación.

1.2.3 Detección de amenazas híbridas

Un análisis de amenazas híbridas centrado en el enemigo, dada la incertidumbre sobre la atribución de las mismas, es inadecuado, por lo que se requiere de métodos alternativos para establecer una conciencia situacional sobre la guerra híbrida.

Uno de los mayores desafíos que presenta la guerra híbrida son los sistemas de alerta temprana. Estos sistemas basan la detección en indicadores militares tradicionales, seguido por una tipología básica de métodos para detectar la guerra híbrida. Este tipo de inteligencia tradicionalmente se basa en métodos basados en indicadores, donde se identifican y monitorizan indicadores clave a lo largo del tiempo para establecer una línea base de las actividades y operaciones «normales» de un adversario. La inteligencia de alerta basada en indicadores se centra en detectar cambios relevantes en el estado operacional que puedan proporcionar a los

analistas de inteligencia una alerta, o advertencia temprana, de actividades no deseadas.

Los nuevos sistemas de alerta requieren de procesos y métodos de inteligencia diseñados para proteger vulnerabilidades críticas en la sociedad, y para detectar ataques híbridos sincronizados y multisectoriales, diseñados intencionalmente para quedar fuera y por debajo de los umbrales de detección tradicionales. Para la detección de estos últimos la identificación de anomalías en series temporales y el empleo de IA para la identificación de patrones, jugará un papel fundamental. Por ejemplo, el empleo de técnicas como *machine learning* da la posibilidad de obtener información mediante el etiquetado automático de información o aplicando técnicas más complejas como el aprendizaje no supervisado.

A continuación, se muestran dos técnicas que son de gran importancia para la analítica actual para entender mejor su aprovechamiento en procesos de inteligencia:

— Detección de anomalías: la detección de anomalías consiste en detectar aquellos elementos de un conjunto cuyas características son significativamente diferentes del resto de elementos. Se utiliza mediante diferentes técnicas por las que se asocia a cada elemento un valor de rareza o especificidad que se utilizará para calificarlo como anomalía con técnicas más o menos convencionales como algoritmos de *clustering*.
— Aprendizaje no supervisado: antes de nada, es importante saber que el aprendizaje no supervisado se refiere a una rama del aprendizaje automático en la que el modelo se entrena sin la necesidad de etiquetas o guías explícitas. Es decir, el modelo puede descubrir patrones de manera autónoma en los datos. El aprendizaje no supervisado se usa para explorar y comprender información compleja y no estructurada de grandes conjuntos de datos, aunque no existan experiencias previas. Esto significa que el aprendizaje no supervisado elimina la necesidad de etiquetar datos, lo que hace que los enfoques estándar de aprendizaje automático sean más flexibles y automáticos. Se trata de técnicas relativamente complejas dentro de la inteligencia artificial. Este artículo no pretende profundizar en temas técnicos, no obstante, los lectores interesados pueden encontrar más información en publicaciones académicas (Naeem et *al*., 2023).

1.2.4 El papel de la inteligencia de datos en conflictos híbridos

La inteligencia de datos en Defensa juega un papel fundamental en la detección, análisis y respuesta a las amenazas híbridas. Especialmente en áreas como:

— Detección de amenazas híbridas: ayuda a monitorizar y analizar grandes cantidades de información para identificar patrones y anomalías que podrían indicar la presencia de amenazas híbridas. Los sistemas de inteligencia de datos pueden procesar datos de múltiples fuentes, incluidas señales de inteligencia, datos de redes sociales, transacciones financieras y más, para detectar posibles amenazas.
— Análisis y evaluación de datos: proporciona herramientas y técnicas para analizar y evaluar grandes volúmenes de datos de manera eficiente. Esto es crucial para comprender la intención y capacidad de los agresores híbridos, así como para evaluar la efectividad de las medidas de contramedidas.
— Coordinación y compartición de información: los sistemas de inteligencia de datos facilitan la coordinación y compartición de información entre diferentes agencias gubernamentales y países, lo que es fundamental para contrarrestar las amenazas híbridas. Al permitir el intercambio seguro y rápido de datos, la inteligencia de datos ayuda a crear una imagen completa de la situación y facilita una respuesta coordinada.
— Detección de patrones y conexiones: utiliza técnicas avanzadas de análisis, como el aprendizaje automático y la minería de datos, para detectar patrones y conexiones que podrían no ser evidentes a simple vista. Esto es crucial para identificar y anticipar posibles amenazas híbridas que no se han experimentado o imaginado antes.
— Desarrollo de contramedidas: proporciona información y análisis que informa el desarrollo de contramedidas efectivas. Al comprender las vulnerabilidades y los vectores de ataque potenciales, los tomadores de decisiones pueden diseñar estrategias de contramedidas más efectivas y basadas en datos.

En este entorno, resulta especialmente complejo identificar amenazas y hacer correlaciones entre eventos disjuntos que permitan identificar eventos sospechosos. Además, cobra especial importancia la capacidad de procesar grandes cantidades de datos en tiempo real que permitan no solo la detección temprana sino también la predicción de escenarios futuros para anticiparse.

Con este enfoque como referencia, se requieren nuevos procesos de inteligencia para la obtención de datos en cualquier ámbito y en tiempo real, permitiendo la detección mediante un análisis prospectivo basado en la identificación de patrones. Este estudio de patrones de comportamiento tiene como ventaja fundamental que permiten desarrollar respuestas automáticas mediante el uso de técnicas de inteligencia artificial.

Por último, cabe destacar la gran importancia y complejidad que conlleva la correcta definición de los indicadores a monitorizar. La calidad de

los cuadros de mando definidos tendrá un gran impacto en el éxito de la inteligencia obtenida apoyando la toma de decisiones para garantizar la Seguridad Nacional.

1.3 Evolución de la arquitectura

Una vez establecidos los principales retos a superar en el ámbito de la Seguridad Nacional, se propone a continuación una serie de consideraciones relativas a la arquitectura un sistema de información que permita aplicar y explotar la inteligencia de datos.

Promovido por el gran volumen de datos al que hay que hacer frente, y su rápido incremento, es necesario un enfoque altamente distribuido, que garantice la escalabilidad horizontal y el funcionamiento continuo del sistema.

La virtualización juega un papel fundamental en sistemas distribuidos altamente escalables horizontalmente, ya que facilita la distribución de carga de trabajo entre nodos. Esta capacidad de virtualización permite por ejemplo la agregación y administración de recursos virtuales bajo demanda, adaptándose a las necesidades en cada momento.

La evolución de arquitecturas de defensa para la explotación de inteligencia de carácter híbrido y multidominio ha sido muy significativa para dar respuesta a los desafíos que presenta. Estas arquitecturas deben adaptarse a ambientes cambiantes y evolucionar para integrar capacidades de inteligencia en múltiples dominios (humanos, señales, imágenes, etc.). Estos tipos de inteligencia se abordan en el presente artículo más adelante. El objetivo es lograr combinar estos datos para detectar actividades o amenazas híbridas y adquirir una compresión más completa de la situación.

La adaptación tecnológica también juega un papel fundamental. La industria en el mundo civil ha evolucionado a gran velocidad y en este sentido los sistemas de defensa se están adaptando a un entorno muy distribuido donde el gobierno del dato juega un papel fundamental. Dada la importancia del ciberespacio los sistemas deben priorizar la protección de redes y activos contra ataques cibernéticos. Este último punto obliga a adoptar un enfoque en la resiliencia tanto a nivel de infraestructuras como de capacidad del sistema para recuperarse ante ataques híbridos.

Todo esto se ejemplifica a la perfección mediante sistemas distribuidos en la nube. En este tipo de arquitectura se da un paso más en la virtualización incluyendo la infraestructura. Todo esto es fundamental para dar soporte en un contexto altamente demandante en el que los requisitos de almacenamiento y procesamiento dependen en gran medida de la cantidad y tipo de datos que se desean explotar, y en el que se deben conectar

sistemas de distintos ámbitos, pudiendo estar en localizaciones distantes o incluso ocupando espacios de información aparentemente no relacionados entre sí.

En resumen, las arquitecturas de defensa para explotación de datos han evolucionado hacia un enfoque integrado, colaborativo, con gran capacidad tanto de almacenamiento como de procesamiento.

1.4 Evolución de la analítica de datos

La analítica de datos es el proceso de examinar, limpiar, transformar y modelar datos con el objetivo de descubrir información útil para llegar a conclusiones y apoyar la toma de decisiones.

La analítica tradicional se basa en datos estructurados y relacionales almacenados por las organizaciones durante años. Este tipo de información, por lo general, es más sencilla de gestionar, administrar y procesar usando métodos convencionales. Sin embargo, proporcionan información menos sofisticada y su uso queda limitado a consultas simples.

La minería de datos y la obtención de nuevos recursos mediante el análisis predictivo, está desplazando el uso de analítica tradicional. En este sentido, el *big data* (o macrodatos) hace referencia a un conjunto de datos masivo y complejo, que incluye información estructurada y desestructurada. En cuanto al volumen de datos por su naturaleza será más demandante y en este sentido se destacan soluciones de almacenamiento de datos en la nube, seguro y de alta capacidad. Por otra parte, el almacenamiento permanece sin procesar ni estructurar por lo que no se pueden usar bases de datos tradicionales con un esquema fijo como hasta ahora. El *big data* requiere de un enfoque no relacional (ejemplos de bases de datos no relacionales son NoSQL Casandra, MongoDB...). Estos medios de almacenamiento, generalmente basados en ficheros, son ideales para el almacenamiento no estructurado.

El enfoque de *big data* es un paso más en la innovación, permitiendo descubrir patrones ocultos y predecir eventos futuros en base al proceso analítico. En resumen, se hace posible un proceso de prospectiva que abre la puerta a nuevos tipos de análisis para la identificación de tendencias a través del análisis masivo de datos para la identificación de cambios o anomalías y detección temprana de eventos o amenazas futuras.

En esto último, para la detección de futuras amenazas es fundamental el análisis predictivo, que permite la identificación de escenarios futuros mediante la elaboración de modelos. Los modelos predictivos permiten la evaluación de escenarios, anticipándose y permitiendo una toma de decisiones más informada.

En general, todo esto mejora la toma de decisiones estratégicas en base a información objetiva extraída de diversas fuentes de datos, que a simple vista quedaría inmersa en ingentes cantidades de información difícil de analizar mediante sistemas analíticos tradicionales.

1.5 *Evolución de la IA aplicada a defensa y seguridad*

Atendiendo a este contexto de multidominio y altamente conectado, la aplicación de técnicas de IA se ha convertido en una de las tecnologías más prometedoras en el campo de inteligencia de datos, permitiendo una clara mejora en los procesos de analítica y aumentando la eficacia de las operaciones. Como se ha mencionado numerosas veces, la IA puede ayudar en gran medida en distintos ámbitos, mejorando la identificación temprana de amenazas, permitiendo la automatización intensiva de procesos, identificando patrones de comportamiento, vigilando actividades sospechosas y finalmente dando soporte a la evaluación de riesgos.

Si bien la aplicación de técnica de inteligencia artificial mejora la eficiencia de las operaciones y permite una mejor gestión de un gran volumen de datos donde un analista convencional no tendría capacidad de asumir esa enorme cantidad de información, la IA también presenta retos difíciles de enfrentar por el momento en cuanto a desafíos éticos y legales que deben ser explorados y cuidadosamente analizados para garantizar la protección de datos y derechos de los ciudadanos.

A lo largo de este artículo se presentan beneficios del uso de IA en el ámbito de seguridad y defensa, así como las principales técnicas para abordar escenarios complejos de analítica.

2 Conceptos fundamentales de la inteligencia de datos

La inteligencia de datos puede definirse como la recopilación, procesamiento y utilización de una gran cantidad de información para descubrir patrones y tendencias que se esconden en ella. El análisis de estos datos en el contexto militar podría ser el proceso de recopilación y análisis de información a través de múltiples fuentes: satélites, sistemas de vigilancia, inteligencia humana (HUMINT), inteligencia de señales (SIGINT), inteligencia de comunicaciones (COMINT)... para descubrir información útil y apoyar la toma de decisiones estratégicas, operacionales e incluso tácticas. La inteligencia de datos desempeña, por lo tanto, un papel importante en los planes de las Fuerzas Armadas. Una forma de utilizar esta tecnología podría ser, entre otros propósitos, obtener una evaluación de posibles amenazas, la planificación de las operaciones, el apoyo a la toma de decisiones estratégicas, la identificación de patrones de actividades enemigas, la identificación de las vulnerabilidades, o incluso una evaluación del éxito de las operaciones en base a datos históricos almacenados.

2.1 Fuentes de datos utilizadas en la Seguridad Nacional

Las fuentes de datos utilizadas en la Seguridad Nacional dependen de muchos factores. Tal y como se expone en la introducción de este artículo, el multidominio y los conflictos híbridos obligan a considerar numerosas fuentes. En términos generales se puede establecer una clasificación clásica que incluiría al menos las siguientes fuentes de datos:

— Inteligencia de fuentes Humanas (HUMINT): en esta clasificación se encuentra la inteligencia que proviene de información facilitada por fuentes humanas, el proceso de obtención puede ser muy variado. Esta información permite validar otros datos de diversas fuentes que se pueden combinar y que se verá más adelante como OSINT, ciberinteligencia o IMINT. Es importante saber que la inteligencia de fuentes humanas no se refiere necesariamente a personas implicadas directamente en las actividades analizadas, sino a cualquier información que es obtenida a través de una fuente humana. En resumen, toda interacción humana para obtener información que ayude a la mejor comprensión de un hecho o a tomar una decisión es HUMINT.

— Inteligencia de Señales (SIGINT): esta modalidad de inteligencia recopila y analiza la información mediante la intercepción de comunicaciones entre personas y entre máquinas o dispositivos. Se trata de la intercepción y análisis de señales de comunicaciones militares y civiles. Esta actividad de nuevo es multidominio, las actividades de SIGINT se llevan a cabo desde estaciones terrestres, barcos, satélites y aeronaves, cuya tecnología va variando a medida que avanza la criptografía y los métodos y canales de comunicación. La inteligencia de señales cada vez es más central para la inteligencia militar debido a la transformación tecnológica e el ámbito de defensa, el desarrollo de las tácticas modernas de las guerras híbridas y los ciberataques.

— Inteligencia de Imágenes (IMINT): obtención y análisis de información a través de imágenes y fotografías, generalmente provenientes de satélites, aviones de reconocimiento, drones o cualquier fuente de imágenes. La explotación de este tipo de información viene impulsada por la necesidad de conocer el entorno o las actividades que se desarrollan en un área concreta. Los analistas de inteligencia puedan obtener gran cantidad de información útil y esta se ha ido incrementando gracias a los avances tecnológicos en el área de sensores, plataformas y comunicaciones. Otro tipo de inteligencia muchas veces relacionada con esta y que pueden resultar relevante es la Inteligencia de Geolocalización (GEOINT) que engloba conjunto de ciencias donde se integran los medios para la captura,

tratamiento, análisis, interpretación, difusión y almacenamiento de información geográfica. En este caso la combinación de ambas permite generar productos de inteligencia de gran valor analítico.

— Inteligencia de Comunicaciones (COMINT): obtención de información recopilada de las comunicaciones de personas, incluidas conversaciones telefónicas, mensajes de texto y diversos tipos de interacciones en línea. La obtención de datos se basa en información recabada sobre transmisiones de voz, texto y señales. La inteligencia, en este contexto, es información que brinda a una organización o individuo apoyo para tomar decisiones destinadas a brindarle una ventaja estratégica. Otras aplicaciones son la capacidad de reconocimiento y vigilancia de señales. Los datos obtenidos pueden alimentar cualquier sistema de fusión de información que permiten por ejemplo determinar la posición del emisor (geolocalización).
— Inteligencia de Fuentes Abiertas (OSINT): recopilación y análisis de información disponible públicamente, como noticias, redes sociales, informes académicos y otras fuentes accesibles al público. Su análisis permite acelerar y mejorar la obtención de datos e información en fuentes abiertas (principalmente internet) sobre personas, empresas e instituciones clave, contribuyendo así a una mejor toma de decisiones a nivel operativo, táctico y estratégico. El análisis de la información procesada se puede realizar de forma híbrida mediante herramientas automatizadas, así como manualmente, encontrando patrones que hagan que la información tenga un orden y sentido. A partir de los datos obtenidos se pueden obtener más datos adicionales en función de los patrones localizados.

A esta clasificación tradicional se pueden añadir otras de gran impacto para los procesos de inteligencia actuales como son:

— Ciberinteligencia: es una actividad de obtención y análisis de información cuyo objetivo es identificar, rastrear y predecir capacidades, intenciones y actividades de actores hostiles en el ciberespacio. Pudiendo ser información relacionada con amenazas cibernéticas, ataques informáticos y vulnerabilidades de seguridad en sistemas de información y redes. El análisis de este tipo de fuente permite disponer de un sistema predictivo de alertas tempranas relativas a ciberataques o ciberterrorismo, permitiendo conocer sus características para mitigar su impacto y mejorar así la toma de decisiones en el ámbito de la Ciberseguridad.
— Datos financieros: seguimiento de transacciones financieras y flujos de dinero para identificar actividades ilícitas, como el financiamiento de organizaciones terroristas u otras actividades que supongan una amenaza. Como ya se ha mencionado, la guerra híbrida se refiere a un enfoque estratégico que combina una variedad de métodos,

incluyendo guerra económica. El análisis de datos financieros en el contexto de la guerra híbrida implica el seguimiento y la evaluación de actividades financieras que pueden respaldar o facilitar acciones no convencionales.

Lo que se ha detallado son solo algunos ejemplos, pero permiten mostrar el nivel de complejidad al que tiene que hacer frente el analista de inteligencia en la actualidad. Para poder identificar amenazas será necesaria la combinación de datos obtenidos de todas estas fuentes y esa tarea requiere de una capacidad de procesamiento solo alcanzable mediante las técnicas más innovadoras para la explotación de datos. De nuevo la aplicación de técnicas de IA es muy relevante, ya que permite delegar gran parte de la carga de trabajo del analista y ofrecer procesos de automatización en tareas altamente demandantes.

2.2 *Tecnologías y herramientas clave para la inteligencia*

Hoy en día existen multitud de herramientas y soluciones tanto comerciales como *open source* para la extracción, análisis y visualización de datos. El empleo de unas u otras viene dado por diversos factores, entre los que hay que considerar:

- Volumen de datos: las herramientas deben ser capaces de procesar grandes volúmenes de datos en un tiempo razonable, por lo que es aconsejable que las herramientas tengan capacidad de paralelización, optimización, procesamiento distribuido, etc.
- Virtualización y capacidad de escalabilidad: en este ámbito las herramientas deben ser capaces de gestionar el aumento de carga de trabajo y para ello es necesario que sean capaces de escalar, virtualizar y gestionar clusters distribuidos. De esta forma se podrán adaptar a distintos niveles de exigencia, ya que las fuentes de datos abiertas por ejemplo tienen como una de sus principales características, el aumento constante de volumen de datos.
- Capacidad de integración de gran cantidad de fuentes de datos: las herramientas deben tener la capacidad de integrar datos de múltiples fuentes, que pueden incluir informes de inteligencia, datos de sensores, bases de datos gubernamentales, redes sociales, etc.
- Capacidad de análisis de datos en tiempo real: las herramientas deben tener capacidad de análisis en tiempo real de datos, como datos de redes, transacciones financieras sospechosas, comunicaciones interceptadas, procesamiento de imágenes y streaming de vídeo, etc.
- Capacidad de análisis avanzado: las herramientas deben tener la capacidad de para realizar análisis avanzados, como análisis de redes, análisis predictivo, detección de anomalías, reconocimiento de patrones, etc.

— Seguridad y privacidad: las herramientas deben ser capaces de manejar información con distintos niveles de clasificación (información de difusión limitada, clasificada, pública...), por lo que se requiere que en muchos casos las herramientas estén certificadas.
— Tolerancia a fallos y resiliencia: las herramientas deben garantizar su funcionamiento constante. Muchos datos son procesados en tiempo real y los sistemas, como se ha mencionado anteriormente, son susceptibles a ciberataques o fallos inesperados. Por este motivo las herramientas distribuidas capaces de replicar su funcionamiento en varios nodos resultan altamente recomendables.

Atendiendo a estas características y las necesidades específicas de la Inteligencia de Datos, a continuación se presentan algunas herramientas que pueden resultar muy útiles al analista. No se trata de hacer una selección de herramientas comerciales si no de exponer las tecnologías fundamentales para la recopilación de información y analítica de datos.

3 Recopilación, procesamiento y almacenamiento de datos

La integración de datos es un componente fundamental en la aplicación de la inteligencia de datos para la Seguridad Nacional. A través de los procesos de Extracción, Transformación y Carga (ETL) o Extracción, Carga y Transformación (ELT), se facilita la recopilación, limpieza y preparación de grandes volúmenes de información de diversas fuentes, convirtiéndola en un recurso valioso para el análisis y la toma de decisiones estratégicas. Estos enfoques permiten a las agencias de Seguridad Nacional no solo recopilar datos de manera eficiente, sino también transformarlos en conocimientos accionables, utilizando algoritmos y técnicas avanzadas para identificar patrones, tendencias y amenazas emergentes.

A continuación se explican en más profundidad cada uno de estos procesos desde una perspectiva técnica:

— Métodos de recopilación de datos (extracción)

La fase de extracción en el proceso de inteligencia es fundamental para obtener información relevante de diversas fuentes. Estas pueden clasificarse en dos categorías principales: fuentes abiertas y fuentes cerradas.

- Las fuentes abiertas comprenden una amplia gama de recursos accesibles públicamente, como redes sociales, noticias en línea, blogs y sitios web gubernamentales, que proporcionan información valiosa para el análisis.
- Las fuentes cerradas incluyen datos confidenciales del gobierno, registros financieros, bases de datos de inteligencia y otros recursos restringidos.

Para acceder y recopilar datos de manera eficiente, las agencias de Seguridad Nacional pueden emplear una variedad de técnicas, como el uso de APIs (Interfaces de Programación de Aplicaciones) para obtener datos estructurados de manera programática, técnicas de web *scraping* para extraer información de sitios web públicos, o incluso la recopilación manual de datos cuando sea necesario. Es importante destacar que los datos recopilados pueden ser altamente heterogéneos en términos de formato, calidad y estructura. La capacidad de manejar e integrar eficazmente estos datos heterogéneos es crucial para garantizar la coherencia y la integridad de la información utilizada en el análisis de inteligencia de datos, lo que a su vez fortalece la capacidad para identificar y abordar amenazas potenciales.

— Transformación de datos. Algoritmos y técnicas de análisis utilizadas

En la fase de transformación de datos para la Seguridad Nacional, tanto la limpieza de datos como la generación de metadatos, por ejemplo, mediante técnicas de Procesamiento del Lenguaje Natural (NLP) desempeñan roles fundamentales.

La limpieza de datos implica una serie de procesos para identificar y corregir errores, eliminar duplicados, y asegurar la coherencia y calidad de la información. Esto incluye la detección y manejo de valores nulos o faltantes, la corrección de errores tipográficos, la normalización de datos y la validación de la integridad de los mismos. Este proceso es crucial para garantizar la fiabilidad de los resultados del análisis y evitar sesgos que podrían surgir debido a datos incorrectos o inconsistentes.

Por otro lado, la generación de metadatos mediante técnicas de NLP permite enriquecer la información con etiquetas adicionales que describen el contenido de los datos. Estos metadatos pueden incluir entidades clave extraídas del texto, como nombres de personas, organizaciones, ubicaciones, fechas, así como categorías de temas relevantes. Además, técnicas como la clasificación de texto pueden utilizarse para categorizar automáticamente documentos según su contenido. Esto facilita la organización y estructuración de grandes volúmenes de información, lo que a su vez agiliza la posterior exploración y análisis de los datos.

— Almacenamiento

En el contexto del almacenamiento, la combinación de distintas formas de almacenamiento juega un papel crucial en la gestión eficiente y efectiva de grandes volúmenes de información heterogénea. Esta combinación de tecnologías de almacenamiento, que incluye bases de datos SQL, NoSQL, *data lakes* y *data lakehouse*, ofrece flexibilidad y escalabilidad para satisfacer las necesidades cambiantes de recopilación, almacenamiento y análisis de datos en entornos de Seguridad Nacional.

Las bases de datos SQL, tradicionalmente utilizadas en aplicaciones empresariales, son adecuadas para datos estructurados que requieren transacciones consistentes y consultas complejas. Estas bases de datos ofrecen integridad de datos y soporte para consultas SQL, lo que las hace ideales para la gestión de datos críticos y confidenciales en el ámbito de la Seguridad Nacional.

Por otro lado, las bases de datos NoSQL proporcionan una alternativa escalable y flexible para el almacenamiento de datos no estructurados o semiestructurados, como documentos, grafos o datos de series temporales. Estas bases de datos son especialmente útiles para la gestión de grandes volúmenes de datos distribuidos en entornos de alta disponibilidad y rendimiento, lo que las convierte en una opción atractiva para aplicaciones de inteligencia de datos en tiempo real.

Además, los *data lakes* emergen como una opción, cada vez más popular, para el almacenamiento de datos en bruto y no estructurados. Estos repositorios altamente escalables permiten almacenar una amplia variedad de datos en su formato original, sin necesidad de estructurarlos previamente. Ofrecen flexibilidad para almacenar datos de diferentes fuentes y tipos, lo que resulta especialmente relevante en el contexto de la Seguridad Nacional, donde la información puede provenir de diversas fuentes y tener formatos heterogéneos.

Recientemente, ha surgido el concepto de *data lakehouse*, que combina las capacidades de los *data lakes* con la funcionalidad de estructuración, procesamiento y analítica de las bases de datos tradicionales. Esta combinación proporciona una arquitectura unificada para la ingesta, almacenamiento y análisis de datos, lo que permite a las organizaciones integrar datos en bruto con datos procesados y generar conocimiento de manera más eficiente.

4 Analítica de datos

La necesidad de análisis de datos en el contexto de la Seguridad Nacional es fundamental para convertir la información recopilada y procesada en conocimiento accionable. Permite identificar patrones, tendencias y relaciones ocultas dentro de los conjuntos de datos, proporcionando una comprensión más profunda de las amenazas emergente. Además, puede ayudar a predecir y anticipar eventos futuros, permitiendo a las organizaciones adoptar enfoques proactivos para abordar las amenazas en tiempo real.

Dentro de esta sección, se puede distinguir entre una analítica convencional y otra más avanzada, basada en el reciente auge de los modelos de inteligencia artificial:

4.1 Analítica convencional

La analítica convencional, respaldada por herramientas de Business Intelligence (BI), es esencial para extraer información valiosa a partir de conjuntos de datos complejos y generar ideas significativas para la toma de decisiones. Utilizando herramientas BI, el enfoque se centra en la recopilación y análisis de datos para generar gráficos, informes y tablas mediante la agregación de datos y estadísticas simples. Estas herramientas permiten la generación de gráficos interactivos, informes detallados, tablas dinámicas y estadísticas simples que facilitan la comprensión de patrones y tendencias.

Los gráficos visuales simplifican la interpretación de datos, mientras que las tablas dinámicas permiten realizar desgloses detallados y análisis en profundidad. Además, la generación de informes automatizados facilita la distribución regular de actualizaciones críticas a los interesados.

La analítica convencional con herramientas BI no solo se limita a la presentación visual de datos, sino que también abarca funciones estadísticas más avanzadas. Estas herramientas permiten realizar análisis de regresión, correlación y tendencias temporales, proporcionando una comprensión más profunda de los datos y apoyando la toma de decisiones basada en evidencias.

4.2 Analítica avanzada

En esta sección, se presenta un conjunto de técnicas de analítica avanzada con algunos ejemplos que podrían ser de utilidad para la Seguridad Nacional.

4.2.1 Análisis de series temporales

El análisis de series temporales implica examinar datos recopilados a lo largo del tiempo para identificar patrones, tendencias y comportamientos cíclicos. Esto será de gran importancia para evaluar la estabilidad a lo largo del tiempo y prever posibles eventos significativos.

La implementación del análisis de series temporales implica el uso de herramientas y técnicas estadísticas avanzadas, como modelos ARIMA, SARIMA, o métodos más modernos basados en aprendizaje automático, dependiendo de la complejidad de los datos y la naturaleza de los eventos a prever. Integrar estas capacidades permitirá una evaluación continua de la estabilidad y una respuesta proactiva ante posibles desafíos. A continuación, se presentan algunos casos interesantes para la Seguridad Nacional:

— Seguimiento de indicadores clave: analizar series temporales de datos económicos, sociales y políticos para identificar indicadores clave que puedan afectar la estabilidad nacional, como tasas de desempleo, inflación, índices de criminalidad y otros factores relevantes.

— Detección de anomalías: utilizar técnicas de análisis de series temporales para identificar patrones inusuales o anomalías que podrían indicar la proximidad de eventos críticos, como disturbios civiles, conflictos étnicos...
— Modelado predictivo: aplicar modelos predictivos basados en series temporales para anticipar posibles crisis o eventos futuros. Esto podría incluir la predicción de movimientos en los mercados financieros, cambios en la opinión pública o incluso la ocurrencia de desastres naturales.

4.2.2 Análisis de agrupaciones de datos

El análisis de agrupaciones de datos o *clústering* es una técnica que agrupa conjuntos de datos similares en grupos, basándose en similitudes entre ellos. Algunos casos de interés se muestran a continuación:

— Segmentación demográfica: utilizar análisis de *clústeres* en datos demográficos para identificar grupos específicos de la población que comparten características similares. Podría ser útil para comprender la distribución demográfica de la opinión pública y adaptar estrategias de comunicación.
— Análisis de amenazas potenciales: aplicar técnicas de *clústering* en datos relacionados con la seguridad, como incidentes criminales, protestas o eventos disruptivos. Esto puede ayudar a identificar patrones geográficos y temporales que sugieran áreas de riesgo o tensiones potenciales.
— Evaluación de redes sociales: analizar las interacciones en redes sociales para identificar comunidades, grupos de interés o posibles influencias. Esto puede proporcionar información sobre la propagación de ideas, opiniones y la formación de grupos que podrían tener implicaciones para la Seguridad Nacional.

4.2.3 Análisis de sentimiento

Se trata de una técnica de procesamiento de lenguaje natural que evalúa y determina la polaridad emocional asociada con un fragmento de texto. Por lo general, se clasifica el texto como positivo, negativo o neutro, permitiendo entender la actitud o la opinión expresada en dicho texto. Para la Seguridad Nacional, podría ser de gran utilidad en diversos casos, como los que se presentan a continuación:

— Monitoreo de medios de comunicación: analizar noticias, redes sociales y otros medios de comunicación para evaluar la percepción pública y la opinión general hacia la situación del país.
— Detección de amenazas potenciales: identificar posibles amenazas o señales de descontento social mediante el análisis de sentimiento

en foros en línea, blogs y otras plataformas donde se discuten temas relacionados con la Seguridad Nacional.
— Reacciones a eventos relevantes: evaluar la reacción del público ante eventos críticos, como elecciones, crisis económicas o desastres naturales, para anticipar posibles tensiones sociales.
— Identificación de tendencias a largo plazo: seguir la evolución del sentimiento a lo largo del tiempo para identificar tendencias y patrones que puedan indicar cambios significativos en la estabilidad del país.

4.2.4 Modelos de lenguaje de gran tamaño (LLM)

Un *Large Language Model* es un tipo de modelo de inteligencia artificial diseñado para comprender y generar texto de manera avanzada. Estos modelos son capaces de procesar grandes cantidades de datos textuales y aprender patrones lingüísticos complejos, lo que les permite realizar una amplia variedad de tareas relacionadas con el lenguaje natural, como traducción automática, generación de texto, resumen de documentos, respuesta a preguntas... El uso de LLM para Seguridad Nacional ofrece una serie de aplicaciones y ventajas significativas. Estos modelos avanzados de procesamiento del lenguaje natural pueden transformar la forma en la que se analizan, comprenden y gestionan los datos en este contexto tan crítico.

— Análisis de grandes volúmenes de datos: una de las principales aplicaciones de los LLM es su capacidad para analizar grandes volúmenes de datos no estructurados, como informes de inteligencia, transcripciones de llamadas, correos electrónicos y documentos clasificados. Estos modelos pueden extraer información relevante, identificar patrones y relaciones, y generar resúmenes automatizados de contenido, lo que permite a los analistas centrarse en áreas críticas y tomar decisiones más informadas y rápidas.
— Detección de anomalías: los LLM pueden ser utilizados para mejorar la detección de anomalías y comportamientos sospechosos en los datos, lo que ayuda a identificar posibles amenazas de seguridad de manera más eficiente. Al analizar los datos en tiempo real, estos modelos pueden alertar sobre actividades inusuales o potencialmente peligrosas, lo que permite una respuesta más rápida y efectiva por parte de las agencias de seguridad.
— Multi-idioma: otra ventaja clave de los LLM es su capacidad para traducir y analizar información en múltiples idiomas, lo que es crucial en el contexto de la Seguridad Nacional, donde la información puede provenir de diversas fuentes internacionales. Esto facilita la colaboración y el intercambio de información entre agencias de seguridad de diferentes países, mejorando la capacidad de detectar y prevenir amenazas transnacionales.

— Automatizar tareas rutinarias: los LLM pueden utilizarse para automatizar tareas rutinarias de análisis de datos, como la clasificación y categorización de información, la generación de informes y la respuesta a consultas de manera rápida y precisa. Esto libera tiempo y recursos para que los analistas se centren en tareas más estratégicas y de alto valor añadido.

5 Aplicaciones de la inteligencia de datos en la Seguridad Nacional

5.1 *Detección y prevención de amenazas terroristas*

El uso de analítica de datos en la detección y prevención de amenazas terroristas es un enfoque, cada vez más importante, en materia de Seguridad Nacional e internacional. Consiste en recopilar, analizar e interpretar grandes volúmenes de datos de múltiples fuentes, que incluyen las redes sociales, comunicaciones electrónicas, transacciones financieras, registros de viaje, entre otros; con el objetivo de identificar posibles patrones, tendencias o comportamientos sospechosos que representen la existencia de actividades terroristas y/o su planteamiento.

Para ello es capaz de identificar conexiones entre individuos, grupos o entidades, detectar actividades inusuales o anómalas, y anticipar posibles escenarios de ataque.

Además, la analítica de datos en la detección y prevención de amenazas terroristas también puede incluir la vigilancia en tiempo real de eventos y situaciones relevantes, el monitoreo de tendencias en línea y la evaluación de riesgos potenciales en diferentes áreas geográficas o sectores específicos. Al incorporar la analítica de datos en los esfuerzos de seguridad y aplicación de la ley, organizaciones gubernamentales e inteligencia pueden mejorar su capacidad para anticipar y responder de manera efectiva a amenazas terroristas, identificando y neutralizando riesgos potenciales antes de que puedan llevarse a cabo actos violentos. Sin embargo, es importante tener en cuenta que la analítica de datos en este contexto plantea desafíos éticos y de privacidad, por lo que es crucial garantizar que la información recopilada sea utilizada de manera legal y responsable.

5.2 *Vigilancia fronteriza y marítima*

Es fundamental para garantizar la Seguridad Nacional, y la inteligencia de datos desempeña un papel crucial en esta área. Además de los métodos tradicionales de vigilancia, como cámaras de seguridad y patrullas, se pueden utilizar técnicas avanzadas de análisis de datos e inteligencia artificial para mejorar la eficiencia y efectividad de la vigilancia.

— Análisis de imágenes satelitales y de drones: permite monitorizar grandes áreas geográficas de manera continua y detectar actividades sospechosas, como movimientos de personas o vehículos en zonas remotas. La IA también puede ser utilizada para analizar estas imágenes a través de modelos de visión artificial (detección de objetos, *tracking*...) e identificar automáticamente patrones y anomalías, lo que facilita la detección de posibles amenazas.
— Análisis de datos de otros sensores, como radares y sistemas de detección acústica: puede ayudar a identificar la presencia de embarcaciones o aeronaves no autorizadas en áreas fronterizas o marítimas. La IA puede ser empleada para procesar estos datos de manera rápida y eficiente, identificando patrones de comportamiento y alertando a las autoridades sobre posibles intrusiones o actividades ilegales.
— Análisis de datos de tráfico marítimo: posibilita el rastreo del movimiento de embarcaciones y la identificación de patrones de tráfico sospechosos, como el cambio repentino de ruta o la navegación en áreas prohibidas. Utilizando algoritmos de aprendizaje automático, se pueden identificar automáticamente embarcaciones sospechosas y generar alertas en tiempo real para su intercepción por parte de las autoridades.

5.3 *Identificación de vulnerabilidades en infraestructuras críticas*

Las infraestructuras críticas en Seguridad Nacional son aquellos sistemas y activos que son esenciales para el funcionamiento y la seguridad de un país. Estas infraestructuras son vitales para el bienestar económico, social y político de una nación, y su protección es de suma importancia para garantizar la estabilidad y la Seguridad Nacional. Las principales infraestructuras críticas son: energía, agua, transporte, comunicaciones, finanzas, salud y seguridad.

Se trata de un aspecto clave para asegurar la resiliencia y la Seguridad Nacional. La inteligencia de datos desempeña un papel crucial en este ámbito, aprovechando una variedad de tecnologías emergentes para fortalecer la detección y mitigación de riesgos. A continuación, se explican algunos ámbitos de aplicación.

— El uso de internet de las cosas (IoT) permite una monitorización continua y en tiempo real de equipos e infraestructuras críticas. Sensores conectados pueden recopilar datos (por ejemplo, rendimiento, temperatura, presión...), lo que facilita el mantenimiento predictivo y la detección temprana de posibles fallos o anomalías. Al analizar estos datos con técnicas avanzadas de análisis, se pueden identificar patrones de comportamiento anormal y predecir fallos potenciales,

permitiendo una intervención predictiva para evitar interrupciones no planificadas.

— El análisis de ciberseguridad también desempeña un papel crucial en la identificación de vulnerabilidades en infraestructuras críticas. Mediante el monitoreo y análisis continuo de datos de seguridad cibernética, como registros de eventos, tráfico de red y comportamiento de usuarios, se pueden identificar posibles amenazas y ataques cibernéticos. Al utilizar algoritmos de detección de anomalías y análisis de comportamiento, se pueden identificar patrones sospechosos que podrían indicar intrusiones o actividades maliciosas, permitiendo una respuesta rápida y efectiva por parte de los equipos de seguridad.

— La inteligencia de datos también puede ser utilizada para la detección temprana de la propagación de enfermedades, especialmente en el contexto de la Seguridad Nacional. Al analizar datos de salud pública, como registros de enfermedades, datos de movilidad y patrones de comportamiento, además de informes médicos internacionales, se pueden identificar brotes de enfermedades y prevenir su propagación. Mediante el uso de técnicas de análisis de datos en tiempo real, como el procesamiento de texto y el análisis de redes sociales, se pueden identificar patrones y tendencias emergentes que podrían indicar la aparición de nuevas enfermedades o la propagación de virus existentes, permitiendo una respuesta rápida y coordinada por parte de las autoridades de salud.

— Una de las principales áreas de enfoque para protección frente a guerra híbrida, es el análisis de la desinformación y la propaganda en línea. Mediante el monitoreo de redes sociales, foros en línea y sitios web de noticias falsas, se pueden identificar campañas de desinformación diseñadas para influir en la opinión pública y sembrar la discordia. Al utilizar técnicas de análisis de texto y detección de sentimientos, se pueden identificar patrones y tendencias que indican la presencia de propaganda maliciosa, permitiendo a las autoridades contrarrestarla con información verificada y precisa.

5.4 Apoyo a la toma de decisiones militares

En un entorno táctico militar, los dispositivos *IoT* (*internet of things*, por sus siglas en inglés) integrados en vehículos militares, equipamiento, unidades y bases pueden recopilar datos sobre el estado operativo, ubicación, condiciones ambientales..., proporcionando una imagen en tiempo real de los activos y recursos disponibles. Además, las cámaras de vigilancia y drones permiten la observación y vigilancia de áreas remotas y de difícil acceso, proporcionando inteligencia sobre la presencia y movimientos de fuerzas enemigas, así como de posibles amenazas.

El análisis de estos datos en tiempo real permite a los comandantes y líderes militares tomar decisiones informadas y adaptar estrategias en función de la situación actual. Mediante el análisis de datos históricos y simulaciones de escenarios, se pueden evaluar diferentes cursos de acción y prever posibles resultados, lo que permite tomar decisiones estratégicas con mayor confianza y precisión.

5.5 *Apoyo a la toma de decisiones políticas*

La inteligencia de datos desempeña un papel crucial en el ámbito político al permitir la generación de indicadores que facilitan el análisis actual de diversas variables sociales, económicas y demográficas. Estos indicadores proporcionan una visión detallada y actualizada del estado de la sociedad, incluyendo aspectos como el crecimiento económico, el empleo, la educación, la salud pública y la seguridad ciudadana. Con esta información, los líderes políticos pueden evaluar el impacto de las políticas existentes, identificar áreas de mejora y desarrollar estrategias efectivas para abordar los desafíos y necesidades de la población.

6 Ejemplos de aplicación prácticos

La aplicación práctica de las técnicas anteriormente analizadas es muy amplia y de sobra conocida. En el ámbito de defensa, por ejemplo, se ha empezado a utilizar la inteligencia artificial para la selección de objetivos de ataques aéreos o para mejorar los sistemas de logística.

La IA encuentra aplicaciones generalizadas en la industria, y una de ellas es la automatización, donde las tecnologías de inteligencia artificial agilizan las tareas repetitivas, mejorando la eficiencia y la productividad. Además, los algoritmos de IA permiten el análisis de datos a gran escala, identificando patrones y brindando información valiosa crucial para la toma de decisiones informada donde el operador tradicional tardaría mucho más tiempo.

A continuación, se recogen algunos casos prácticos sin entrar en detalle, para ejemplificar algunos casos de uso:

6.1 *Sistemas de recomendación de objetivos*

Es de sobra conocido que Israel está utilizando la IA de forma significativa para la toma de decisiones en conflictos bélicos. Aunque las actividades realizadas dentro de la dirección de inteligencia de las *IDF* (siglas en ingles de las Fuerzas de Defensa de Israel) están clasificadas, ellos mismos, a través de un comunicado publicado en su página web en noviembre de 2023, declaraban estar usando inteligencia artificial para proporcionar

recomendaciones a los analistas. Si bien no se puede determinar, de forma concreta, cuales son las fuentes de datos explotadas por estos algoritmos, todo apunta a una combinación de imágenes tomadas por drones, comunicaciones interceptadas y análisis de comportamiento de grupos de individuos.

Otro ejemplo del que apenas se tiene información, pero resulta relevante, es el sistema de cámaras para el control de fronteras empleado por Israel que ha sido entrenado con miles de horas de grabaciones para automatizar la identificación de personas y objetos en imágenes.

6.2 *Procesamiento de imágenes y detección de patrones*

Una de las primeras herramientas con mayor visibilidad del *DoD* de Estados Unidos fue el proyecto Maven. Se trata de una herramienta de inteligencia artificial diseñada para procesar imágenes y vídeos desde drones que permite la detección automática de objetivos potenciales. Fue un proyecto pionero en el procesado de inteligencia mediante el aprendizaje automático, que surge de la necesidad de acelerar el proceso de análisis de imágenes. Los drones son ante todo plataformas de inteligencia, vigilancia y reconocimiento, y esta herramienta permitió a los analistas humanos procesar dos o tres veces más información por medio de algoritmos entrenados para la clasificación y detección de objetos.

7 Reflexiones finales sobre el papel de la inteligencia de datos en la Seguridad Nacional

El presente artículo trata de poner en valor la importancia de la inteligencia de datos para la Seguridad Nacional, destacando los retos que enfrenta el analista debido al contexto de la guerra híbrida y el multidominio. En este contexto es necesario adaptar las estrategias de defensa a la alta demanda de un entorno complejo, altamente interconectado, donde las amenazas pueden coexistir en distintos dominios incluidos el ciberespacio y el dominio cognitivo. La guerra híbrida se caracteriza por la dificultad de identificar amenazas que requerirá por parte de los sistemas de inteligencia capacidades de analítica avanzada que permita su detección y la explotación de vulnerabilidades mediante el modelado predictivo.

La detección temprana juega un papel crucial en estos sistemas de inteligencia que deben proporcionar al analista información efectiva para el desarrollo de contramedidas efectivas, dar soporte a la toma de decisiones y mejorar la conciencia situacional. Para dar soporte a todo esto las arquitecturas de los sistemas de inteligencia deben evolucionar hacia sistemas distribuidos, basados en la virtualización tanto de recursos como operaciones, generalmente en la nube, y que sean lo suficientemente flexibles para

poder adaptarse y escalarse en función de los datos que procesen. En este sentido se destaca el papel crucial del *big data* y las técnicas de analítica avanzada basada en inteligencia artificial para la detección de patrones y conexiones ocultas.

La analítica de datos implica examinar, limpiar, transformar y modelar para obtener información útil mediante procesos de automatización. Tradicionalmente se han usado datos estructurados y relacionales, pero los avances en minería de datos y analítica han desplazado este contexto y en la actualidad se explota información de cualquier tipo de fuente incluso las fuentes desestructuradas. Este enfoque es esencial para la obtención de datos en el escenario híbrido que requiere la explotación de fuentes de datos alternativas como redes sociales y otros elementos conectados al dominio global en el que operan. Asimismo, se requiere un esfuerzo importante para la definición y selección de los indicadores más relevantes a analizar en cada dominio, puesto que junto con el conocimiento y experiencia de los analistas son parte clave del proceso para garantizar la Seguridad Nacional.

Por otro lado, no se deben olvidar los factores éticos derivados del empleo de IA, especialmente respecto a la protección de datos y los derechos de los ciudadanos.

En cualquier caso, se puede afirmar que la aplicación de técnicas de inteligencia artificial y *big data* es un desarrollo prometedor para la automatización de procesos, identificación temprana de amenazas y el aumento de la eficacia en operaciones de seguridad y defensa.

Bibliografía

Allen, E, Gilbert, P. y Gilbert, D. (2010). NATO Cooperative Cyber Defence Centre of Excellence Conference. *Journal of information Warfare*, Vol. 9.

Naeem, S. et al. (2023). *An Unsupervised Machine Learning Algorithms Comprehensive Review*. *International Journal of Computing and Digital Systems*. [Consulta: 2024]. Disponible en: https://journal.uob.edu.bh/bitstream/handle/123456789/4777/IJCDS130172.pdf

Necesidad de disponer de sistemas tácticos de aeronaves no tripuladas (TUAS) en las fuerzas terrestres

Juan Ignacio Fernández González

«There have been many technologies introduced during this eight-and-a-half years of war. However, I don't think any has made a greater impact than UAS»[1]

General Peter Chiarelli,
jefe de gabinete adjunto, US Army.

Resumen

Es evidente la creciente proliferación y el uso, cada vez más habitual, de sistemas de aeronaves no tripuladas en los conflictos armados actuales. El Ejército de Tierra no ha sido ajeno a este auge en el empleo de UAS, dotando a sus unidades en los últimos años con sistemas para satisfacer las necesidades de información en beneficio de las diferentes funciones tácticas. En el futuro inmediato, el combate terrestre seguirá constituyendo el centro de gravedad de las operaciones, así como el elemento primordial para la consecución de su éxito. Por este motivo, los TUAS constituyen el medio más versátil y eficiente para efectuar el reconocimiento de amplias zonas de interés. La interoperabilidad de estos sistemas permitirá avanzar en el desarrollo de conceptos emergentes que aseguren la integración de plataformas aéreas tripuladas y no tripuladas. En la Operación Romeo/Alfa, el TUAS PASI se reveló como un sistema fundamental dentro de la estructura de Inteligencia, ejecutando un gran número de misiones de vuelo en beneficio de las tropas del contingente multinacional. Hoy se prepara para recibir a su relevo, un sistema que igualará sus capacidades, superándolo en muchos aspectos.

Palabras clave

RPAS, Interoperabilidad, Multidominio, Integración, Burbuja de interés.

[1] *U.S. Army Unmanned Aircraft Systems: Changing Modern Warfare. Institute of Land Warfare Association of the United States Army.*

Need to have tactical unmanned aircraft systems (TUAS) in the Land Forces

Abstract

The growing proliferation and increasingly common use of unmanned aircraft systems in current armed conflicts is evident. The Army has not been immune to this boom in the use of UAS, providing its units in recent years with systems to satisfy information needs for the benefit of different tactical functions. In the immediate future, ground combat will continue to constitute the center of gravity of operations, as well as the primary element for achieving their success. For this reason, TUAS can be the most versatile and efficient means to carry out the recognition of large areas of interest. The interoperability of these systems will allow progress in the development of emerging concepts that ensure the integration of manned and unmanned aerial platforms. In the operation Romeo/Alfa, the TUAS PASI was revealed as a fundamental system within the Intelligence structure, executing a large number of flight missions for the benefit of the troops of the multinational contingent. Today it is preparing to receive his replacement, a system that will equal its capabilities, surpassing it in some aspects.

Keywords

RPAS, Interoperability, Multidomain, Integration, Interest bubble.

1 Introducción

En las dos últimas décadas, las operaciones de combate generalizado han puesto de manifiesto la creciente proliferación y el uso, cada vez más habitual, de sistemas de aeronaves no tripuladas. Los conflictos bélicos de Ucrania, Siria, Gaza, Azerbaiyán, Armenia, Yemen, la crisis del golfo Pérsico y la respuesta de occidente contra el estado islámico, entre otros, evidencian un incremento de la presencia de este tipo de medios de obtención de información por parte de la mayoría de fuerzas involucradas en los mismos.

El Ejército de Tierra no ha sido ajeno a este auge en el empleo de UAS, dotando a sus unidades con varios exponentes de esta capacidad, para satisfacer las necesidades de información en beneficio de las diferentes funciones tácticas. Desde que en 2005 se iniciaran las primeras colaboraciones entre el Ejército de Tierra (ET) y el INTA[2] para la operación y el mantenimiento del sistema UAV[3] SIVA[4], pasando por la adquisición de los UAS PASI y RAVEN para apoyar al contingente desplegado en la Operación Romeo/Alfa en Afganistán, hasta llegar al proyecto actual de desarrollo del Sistema Remotamente Tripulado de Altas Prestaciones (SIRTAP), las unidades de la Fuerza se han ido familiarizando con la participación de estas aeronaves en sus ejercicios de instrucción y adiestramiento. De forma prácticamente simultánea, la doctrina y los procedimientos han tenido que acompasar su desarrollo al ritmo que están imponiendo las lecciones identificadas sobre el uso de los UAS en los conflictos bélicos anteriormente descritos.

Desde el punto de vista del empleo, y teniendo en cuenta la clasificación en función del peso máximo al despegue (MTOW)[5] que establece el Reglamento de la Circulación Aérea Operativa (RCAO), las distintas categorías de UAS pueden diferenciarse en tres grandes grupos. En el primero de ellos figurarían los sistemas de Clase I, con un MTOW inferior a 150 kg, encuadrados en las brigadas en función de su desempeño, cometido o adscripción a una determinada función táctica. Por encima de esta categoría se encuentran los TUAS[6], como escalón intermedio entre los UAS de Clase I y los representantes de la Clase III. Estos últimos con un peso máximo al despegue que excede de los 600 kg y destinados a un uso fundamentalmente estratégico y operacional o de teatro.

---

[2] INTA: Instituto Nacional de Técnica Aeroespacial.
[3] UAV, del inglés *Unmanned Aerial Vehicle*.
[4] SIVA: Sistema Integral de Vigilancia Aérea. Demostrador tecnólogico de UAS de clase II (300 kg de peso máximo al despegue), desarrollado por el INTA.
[5] MTOW, del inglés *Maximun Take of Weight*.
[6] TUAS, del inglés *Tactical Unmanned Aerial System*.

Es precisamente en ese escalón intermedio, el que representa a los TUAS de Clase II, donde el ET necesita centrar sus esfuerzos para garantizar la aportación de información a los procesos ISTAR[7] y TARGETING[8] para facilitar el conocimiento y la comprensión del entorno operativo (IPOE[9]), proporcionar el apoyo a determinadas operaciones en curso y, en definitiva, para el apoyo a la toma de decisiones.

2 TUAS en las fuerzas terrestres

En el proceso de transformación del ET dentro del proyecto Ejército 35[10], se tiene en cuenta que en el horizonte próximo (diez a veinte años), el combate terrestre seguirá constituyendo el centro de gravedad de las operaciones, así como el elemento primordial para la consecución de su éxito.

La rápida evolución de los actuales entornos de actuación, en los que seguirá jugando un papel importante la amenaza híbrida, obligará a dotar a todas las funciones tácticas de medios tecnológicamente avanzados, con capacidad para cubrir grandes superficies y adaptarse a las necesidades que demandan las operaciones multidominio[11], e incrementando el conocimiento de la situación (*situational awareness*) para aumentar la eficacia de los órganos decisores.

El Cuerpo de Ejército (CE) y la División (DIV), como exponentes de las unidades operativas más completas de las fuerzas terrestres, deberán disponer de sistemas de obtención de información que permitan cubrir sus burbujas de interés de una manera integral.

Sobre ese terreno, los TUAS pueden constituir el medio más versátil y eficiente para efectuar el reconocimiento de amplias zonas de interés, mediante la transmisión de imágenes y vídeo en tiempo real, o cercano al real, así como para proporcionar información sobre el desarrollo de las operaciones, el apoyo a movimientos tácticos y despliegues de unidades, e incluso participar en acciones de Guerra Electrónica (EW).

---

[7] ISTAR, del inglés Intelligence, *SurveillanceTarget Acquisition and Reconnaissance*.

[8] Targeting: es el proceso de seleccionar y priorizar objetivos y asignarles una acción adecuada (letal o no letal), teniendo en cuenta las capacidades y requisitos operacionales (ATP-3.9.2).

[9] IPOE, del inglés *Intelligence Preparation of the Operating Environment*.

[10] EME, Estado Mayor del Ejército. Centro de Fuerza Futura 35 (Revisión OCT23). Conceptos de transformación FUERZA 35.

[11] *Multidomain operation* (MDO): operación desarrollada en un entorno operativo donde confluyen distintos dominios físicos (terrestre, marítimo y aeroespacial), virtuales (espectro electromagnético) y psicológicos (cognitivo), creando ambientes degradados en ciertas áreas para impedir el acceso a la misma o para anular la capacidad operativa de las unidades allí desplegadas.

De este modo, un TUAS encuadrado en el Núcleo de Tropas de Cuerpo de Ejército (NTCE), debería disponer de sensores diurnos, nocturnos, infrarrojos y radar de apertura sintética para ejecutar misiones de vuelo ISR[12], adquisición de objetivos y valoración táctica de daños.

Su autonomía de vuelo debería ser de al menos veinticuatro horas, con un alcance mínimo de 300 km en VLOS[13], y enlace satelital BVLOS[14], un techo de vuelo de 20 000 pies (6000 m aproximadamente), y la capacidad de garantizar la ejecución de tres misiones de vuelo simultáneas de manera continuada.

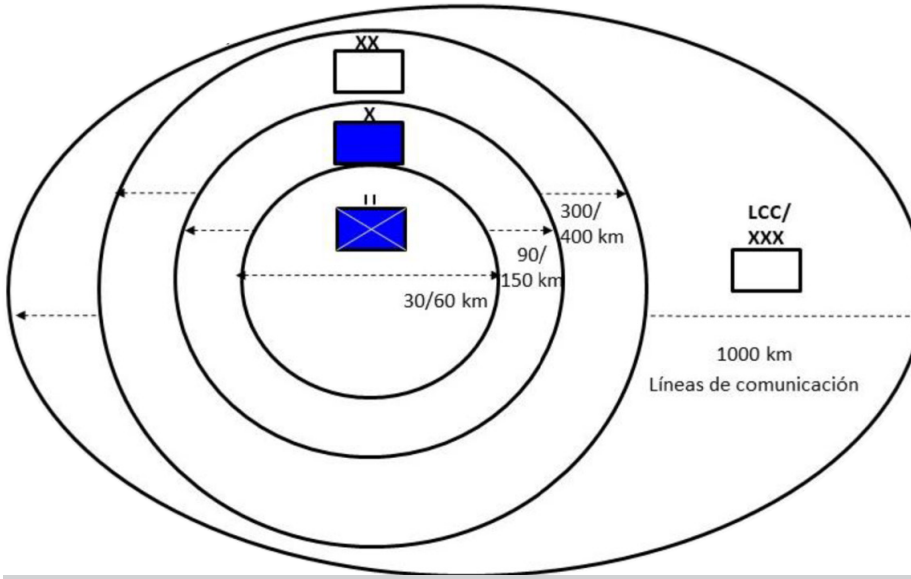

Figura 1. Burbujas de interés concepto FUERZA 35. Fuente: EME

3 Conceptos emergentes

La ejecución de operaciones terrestres rápidas y decisivas necesita la completa interoperabilidad de los sistemas de mando y control (C2) de CE y DIV con los sistemas de gestión ISR y C2 de los fuegos, junto con una gestión ágil y eficaz del espacio aéreo.

[12] ISR, del inglés *Intelligence, Surveillance and Reconnaissance*.

[13] VLOS, del inglés *Visual Line of Sight*. Debido a la curvatura de la tierra, el horizonte máximo visible de terreno desde una altura de vuelo de 20 000 pies no supera los 270 km. En este tipo de enlace, es imprescindible que la estación de control en tierra (GCS) desde la que se controla el UAV, disponga de un enlace de visión directa entre las antenas directivas de la estación y las antenas embarcadas en la aeronave.

[14] BVLOS, del inglés *Beyond Visual Line of Sight*.

Esta interoperabilidad permitirá el auge de conceptos emergentes como el denominado MUM-T[15], que se puede definir como el desarrollo de sistemas de trabajo en equipo para la operación coordinada de UAS desde aeronaves tripuladas.

Las unidades de Aviación del ET podrían actuar integradas con los TUAS mediante el intercambio de información en tiempo real, siendo posteriormente empleada en la designación de objetivos y el guiado de municiones aire-tierra, así como para el reconocimiento, la evaluación de daños, o la transmisión de información de toda índole (en modo relé de comunicaciones). Se logra así reducir la exposición de las tripulaciones de helicópteros al fuego enemigo, principalmente en misiones de reconocimiento y ataque.

Esta integración permitiría fusionar la información obtenida y gestionarla de forma autónoma en red mediante inteligencia artificial, convirtiendo cada plataforma en un sensor, y cada sensor en un arma, capaz de potenciar exponencialmente las capacidades de las fuerzas terrestres en el medio aéreo.

Un segundo concepto emergente, el *sensor to shooter*, contempla que los medios de obtención de información o adquisición de objetivos (*sensor*), están permanentemente interconectados, de manera que la toma de decisiones y la transmisión de las órdenes de ejecución se trasmiten con enlaces de datos rápidos, empleando procedimientos íntegros y seguros. De este modo, si el TUAS detecta un objetivo, la información se traslada de forma simultánea al órgano decisor y al medio productor de efectos (fuegos, EW, etc), manteniendo la visual sobre el objetivo mientras se ejecuta la acción, para efectuar su seguimiento posterior, reiterar la acción o proporcionar la correspondiente evaluación táctica de daños.

4 UAS PASI. El precursor de la capacidad

Tras los acuerdos surgidos de la conferencia general de generación de fuerzas que tuvo lugar en el SHAPE[16],Bélgica, en el año 2007, las Fuerzas Armadas españolas alcanzaron, en 2008, el compromiso de desplegar una unidad UAS en el marco de la Operación Romeo/Alfa[17], bajo mando táctico del Mando Regional Oeste (RC-W) de ISAF[18].

---

[15] MUM-T, en inglés *Manned-Unmanned Teaming*. Dentro de este concepto existen diferentes iniciativas, como los Aviones de Combate Colaborativos (*Collaborative Combat Aircraft-CCA*) de la *US Air Force* (USAF), o el proyecto Loyal Wingmen de la Real Fuerza Aérea Australiana (RAAF).

[16] SHAP, del inglés: *Supreme Headquarters Allied Powers Europe*.

[17] Acuerdo de Consejo de Ministros, de 25 de marzo de 2008, por el que se decide el despliegue y participación, dentro de la misión ISAF-AFGANISTÁN de expertos en el manejo de vehículos aéreos no tripulados (UAV) para reforzar la seguridad de las tropas españolas allí desplegadas.

[18] ISAF, del inglés *International Security Assistance Force*.

Mientras estuvo desplegado en la Operación Romeo/Alfa, el TUAS PASI se reveló como un sistema fundamental dentro de la estructura de Inteligencia del RC-W de ISAF, ejecutando misiones de vuelo en beneficio de las tropas del contingente multinacional que operaba en su área de responsabilidad, fueran estas españolas o no. Para transmitir la información de aquellas misiones que fueran de interés nacional, se instaló SICONDEF[19] para remisión de las imágenes vía satélite al MOPS[20]. Seis años más tarde, el PASI había totalizado 5300 horas de vuelo y 940 misiones ISR, antes de su repatriación.

Una vez completado el repliegue de los sistemas a Territorio Nacional, el 1 de octubre de 2015 se constituyó el Grupo de Obtención por Sistemas Aéreos IV/1 (GROSA IV/1), integrado en el Regimiento de Inteligencia N.º 1, quien tiene en dotación en exclusiva estos sistemas y el encargado de su operación en el ámbito del ET.

Las misiones de vuelo que lleva a cabo en la actualidad el TUAS PASI no difieren sustancialmente de las ejecutadas en zona de operaciones. Las necesidades de información que deben satisfacer hoy en día los analistas IMINT[21] de la Unidad de Vuelo del GROSA IV/1 son muy similares a las que recibían del *J3 UAV Planning and Tasking*[22] en el RC-W. La diferencia estriba en que ahora esa interrelación se realiza con el CCMO[23] de la unidad ISTAR de CE o DIV.

5 SIRTAP. El futuro TUAS de las fuerzas terrestres

En noviembre de 2023 la empresa Airbus firmó un contrato con el Ministerio de Defensa de España para el desarrollo y adquisición del SIRTAP[24], como respuesta al programa conjunto TUAS-LA (Vehículo Aéreo no Tripulado de Largo Alcance). Este TUAS se convertirá en el relevo del PASI, con el que convivirá un tiempo hasta la retirada del servicio de este último, prevista en 2018.

---

[19] SICONDEF: Sistema de Inteligencia Conjunto de la Defensa.

[20] MOPS: Mando de Operaciones. Órgano responsable a su nivel del planeamiento operativo, la conducción y el seguimiento de las operaciones militares, tanto de carácter nacional como de aquellas operaciones multinacionales con participación española, cuando España asume su liderazgo.

[21] IMINT: Inteligencia de Imágenes.

[22] J3 UAV *planning and tasking:* oficial español destacado en el RC-W, encargado del planeamiento y la asignación de misiones ISR a las unidades UAV.

[23] CCMO: Centro de Control de los Medios de Obtención.

[24] *BOE* n.º 290, de 5 de diciembre de 2023. Anuncio de formalización de contratos de: Subdirección General de Adquisiciones de Armamento y Material DGAM. Objeto: Adquisición de nueve sistemas SIRTAP.

Cada uno de los cuatro sistemas SIRTAP que se suministrarán al GROSA IV/1 estará compuesto por tres UAV y una GCS[25]. En este sentido, la experiencia en la operación del PASI ha demostrado que la GCS es el elemento más crítico de un TUAS, al ser el elemento imprescindible para realizar el control de la aeronave y el aumento de sus capacidades de actuación mediante transferencia de control[26].

A pesar de que, por diseño, cada aeronave tendrá un MTOW de 750 kg, las versiones ISR, que no necesitan portar cargas externas, se espera que no sobrepasen los 600 kg (el PASI en la actualidad tiene un MTOW de 430 kg). Este aumento de peso se traduce directamente en una mayor capacidad de carga útil (hasta 150 kg para un MTOW de 750 kg), y mayor autonomía, al incrementar la cantidad de combustible embarcado, pudiendo superar las veinte horas, frente a los 80 kg y doce horas del PASI. Dispone también de capacidad de volar dos aeronaves de manera simultánea, permitiendo alcanzar técnicamente una operación «24/7» real.

La versión inicial con la que se dotará al GROSA IV/1 será la denominada ISR, con sistemas electroópticos y radar de apertura sintética (SAR). Este último incrementa las capacidades respecto del PASI.

Si bien el techo operativo será similar al PASI, mejorará la estanqueidad de la aeronave y, por ende, aumentará su capacidad de vuelo en condiciones de lluvia, dispondrá de ciertas capacidades como relé de comunicaciones de unidades terrestres, IFF modo 5 y data link, etc. que le conferirán además una mayor interoperabilidad y una mayor resiliencia en entornos hostiles.

El SIRTAP podrá tener capacidad BVLOS, que le permitirá apoyar operaciones de nivel CE dentro de las distancias de su burbuja de interés (1000 km), mediante un sistema de Clase II, más acorde a los nuevos escenarios no lineales de las operaciones actuales y futuras.

6 Conclusión

La incorporación de tecnologías cada vez más disruptivas puestas a disposición de los órganos de mando con capacidad de decisión, permitirán alcanzar de forma más inmediata una ventaja táctica y operacional en los entornos de actuación actuales. La rapidez y agilidad con la que los nuevos sistemas permitan el flujo e intercambio de información en todos los escalones de mando, facilitarán la consecución del éxito en las operaciones terrestres.

[25] GCS, del inglés *Ground Control Station*.

[26] Trasferencia de Control: ee utilizan dos GCS para aumentar la distancia de operación al trasferir el control del UAV en vuelo de una estación a la siguiente.

Los TUAS, actuando como verdaderas plataformas aéreas multipropósito, disponen de un amplio abanico de dispositivos electroópticos y de obtención de información en configuración ISR. Pueden, además, incorporar armamento para transformarse en UCAV[27] y operar de manera conjunta y colaborativa con la Aviación de Ejército, permitiendo a las fuerzas terrestres disponer de una herramienta versátil y eficiente para la consecución de sus objetivos.

La organización operativa de nivel CE deberá contar con medios UAS provistos de las capacidades adecuadas para apoyar el proceso de planeamiento y decisión del comandante, por lo que serán no solo necesarios sino imprescindibles los TUAS Clase II en cualquier operación.

[27] UCAV, del inglés *Unmanned Combat Aerial Vehicle*.

Cómo la inteligencia en emergencias se enfrenta a las nuevas amenazas

Jaime Mata Laencina

Resumen

Los riesgos y amenazas en emergencias no han cambiado con el paso del tiempo, pero sí se observa que la amenaza ha aumentado tanto en frecuencia como en intensidad, debido, principalmente, a factores como: el cambio climático, la globalización, el abandono rural y la ocupación por parte de la población de zonas de riesgo. Con este artículo se pretende dar una visión sobre las técnicas de análisis empleadas para la detección de eventos que puedan desencadenar una situación de emergencia y ofrecer un nuevo punto de vista de cómo la inteligencia en emergencias debe evolucionar para integrar las nuevas tecnologías en apoyo a las técnicas de análisis.

Palabras clave

UME, SIGUME, Indicadores, Alertas, Riesgos naturales, Riesgos tecnológicos.

How intelligence in emergencies faces new threats

Abstract

The risks and threats associated with emergencies have not changed over time, but it has been observed that the threat has increased both in frequency and intensity, mainly due to factors such as: climate change, globalization, rural abandonment and population occupying areas at-risk. This article aims to provide an overview of the analysis techniques used to detect events that may trigger an emergency and offer a new perspective on how intelligence in emergencies must evolve to integrate new technologies to support analysis techniques.

Keywords

UME, SIGUME, Indicators, Alerts, Natural risks, Technological risks.

1 Introducción

La Ley 17/2015 del Sistema Nacional de Protección Civil (SNPC), define el riesgo como «la posibilidad de que una amenaza llegue a afectar a colectivos de personas o a bienes». De igual modo, describe amenaza como «la situación en la que las personas y bienes preservados por la protección civil están expuestos en mayor o menor medida a un peligro inminente o latente».

Desde el punto de vista de protección civil, la amenaza en España es relativamente baja por sus propias características geográficas y climatológicas. No obstante, se está viendo paulatinamente potenciada por factores como la despoblación rural y la sobrepoblación de ciudades, la degradación del ecosistema agravada por los efectos del cambio climático o el incremento en la magnitud y frecuencia de algunos fenómenos meteorológicos adversos (ESN 21)[1].

A la hora de definir futuras amenazas en el ámbito de las emergencias, en realidad lo que se pretende es identificar situaciones nuevas que tengan el potencial de causar daños a personas y/o bienes que sean susceptibles de ser afectados en mayor o menor medida por tales circunstancias.

El tercer capítulo de la Estrategia de Seguridad Nacional 2021 (ESN 21), describe los riesgos y amenazas para la Seguridad Nacional y pone de manifiesto que estos riesgos y amenazas están interconectados, presentando un panorama actual de seguridad de gran incertidumbre. En este capítulo se enumeran cuatro riesgos y amenazas relacionadas con las emergencias: epidemias y pandemias, emergencias y catástrofes, flujos migratorios y efectos del cambio climático y de la degradación del medio natural.

En los últimos cinco años, España se ha enfrentado a nuevas emergencias y a otras que ya eran conocidas que han comprometido o saturado los dispositivos de emergencia, como: en 2019, la emergencia sanitaria originada por el COVID-19; en 2021, la erupción volcánica en La Palma y las nevadas provocadas por la borrasca Filomena que paralizaron la actividad de varias ciudades españolas y en 2022, la campaña de incendios forestales que fue especialmente intensa y que supuso que la UME llegara a desplegar el máximo de sus efectivos.

2 Análisis prospectivo de amenaza

Tradicionalmente las amenazas en emergencias se clasifican en dos grandes grupos:

[1] Estrategia Seguridad Nacional 2021.

— Amenazas naturales: procesos o fenómenos naturales potencialmente peligrosos como inundaciones, incendios forestales, fenómenos meteorológicos adversos, terremotos, maremotos y volcanes.
— Amenazas antrópicas: derivados de la acción del ser humano, entre ellos encontramos los riesgos tecnológicos[2] y los medioambientales.

Como se puede ver, en el ámbito de las emergencias no hay un solo adversario (amenaza) al que enfrentarse, sino varios. También, se debe tener en cuenta que dichas amenazas pueden producirse con mayor probabilidad en una o varias épocas determinadas a lo largo del año o que puedan tener lugar con igual probabilidad en cualquier momento.

2.1 *Amenazas naturales*

Las amenazas naturales, a su vez, pueden ser encuadradas en otros dos grupos, dependiendo de la causa desencadenante: amenazas de origen meteo-climático y de origen geológico.

Las amenazas derivadas de la meteorología o del propio clima no han cambiado a lo largo del tiempo, pero sí lo han hecho algunos aspectos que hacen que el riesgo pueda ser mayor. Prácticamente, la mayoría de la comunidad científica coincide en que la causa del aumento de esta amenaza es el cambio climático.

Los cambios en el clima tienen un carácter cíclico y han ocurrido a lo largo de la historia. Sin embargo, el cambio climático actual parece ir más deprisa de lo normal. La causa más probable es la actividad humana, que acelera o potencia estas variaciones en el clima y está produciendo que los fenómenos extremos que antes había, ahora se presenten con mayor ocurrencia e igual o mayor intensidad. Además, ya no se encuadran solo en su estación del año, sino que aparecen fuera de su temporada natural.

Según la World Meteorological Organization, en su publicación sobre Cambio Climático y Clima Extremo, se ha detectado un aumento de los episodios extremos de calor, derivados de un calentamiento continuado de la temperatura global. Este efecto se ve acompañado de una tendencia generalizada de temperaturas medias más cálidas. En consecuencia, existe una mayor evaporización del agua, dando lugar a dos consecuencias claras: sequías generalizadas (por desaparición de recursos hídricos) y

[2] Un riesgo tecnológico viene definido por los daños o pérdidas que pueden presentarse debido a eventos asociados con el almacenamiento, producción, transformación manipulación o transporte de sustancias y/o residuos químicos peligrosos, nucleares, radiactivos, biológicos, líquidos inflamables, materiales combustibles, electricidad y/o hidrocarburos, así como con las actividades que operen a altas presiones, altas temperaturas o con posibilidades de impacto mecánico (UME, PDE-0013).

episodios de lluvias extremas (por mayor disponibilidad de vapor de agua en la atmósfera). Según informe del Panel Intergubernamental del Cambio Climático (IPCC), es probable que los eventos extremos de precipitación se intensifiquen en aproximadamente un 7 % por cada 1 °C de calentamiento global (IPCC Report, 2021: 16).

De hecho, la Agencia Estatal de Meteorología (AEMET) ha detectado un aumento de las precipitaciones máximas en el área peninsular mediterránea en los últimos años. Estas precipitaciones máximas, muchas veces incluso superiores a las medias anuales, provocan lluvias torrenciales y procesos de erosión e inundaciones más intensos que los registrados históricamente.

Por lo tanto, el calentamiento global del planeta, derivado del cambio climático, no solo tiene efectos sobre la temperatura, sino también sobre: las precipitaciones, la intensidad del viento y la dinámica atmosférica. Como consecuencia, repercute en la frecuencia de los fenómenos meteorológicos extremos.

Según el IPCC, también es probable que las olas de calor, los episodios de precipitaciones intensas, las sequías y los ciclones tropicales aumenten en el futuro.

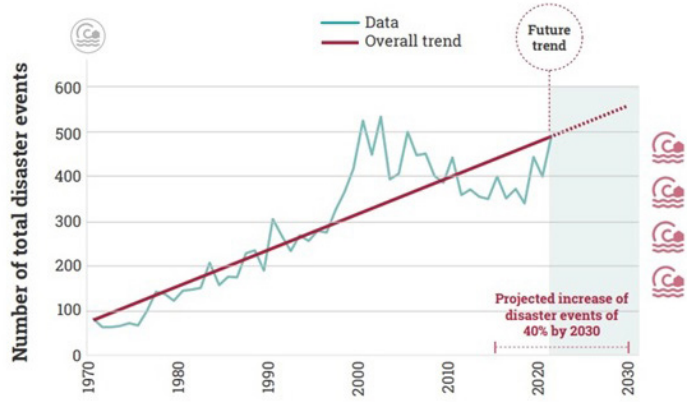

Figura 1. Tendencia desastres próximos años Fuente: UNDRR analysis based on EM-DAT (CRED, 2021)

Sin embargo, estas variaciones climáticas, unidas a otras de origen antrópico, son responsables del aumento de la amenaza frente a los fenómenos meteorológicos extremos. Entre estas causas de origen antrópico se pueden destacar:

— La concentración de grandes poblaciones en zonas de peligro como son los asentamientos en zonas inundables.

— Una población más vulnerable ante dichos fenómenos, porque no está acostumbrada a reaccionar, independientemente de que sí lo esté su sistema de protección civil.
— El éxodo rural que, desde mediados del siglo pasado, ha pasado a ser un potenciador de la amenaza. El monte en España crece, pero la explotación forestal como medio económico es muy pequeña. Por ello, el combustible vegetal invade los montes, transformándolos en auténticos polvorines, no solo en épocas estivales, sino también fuera de ellas.

Este nuevo escenario de «crisis climática» se está materializando en las siguientes amenazas a las que la UME ya se está enfrentando:

— Incendios forestales: incendios catalogados de 6.ª generación. La intensidad de estos hace que la respuesta del operativo se destine a minimizar los daños y a proteger a la población. Dichos megaincendios, en ocasiones, sobrepasan las capacidades de extinción del operativo, debido principalmente a su virulencia y su velocidad de propagación, ocasionando grandes pérdidas en vidas humanas y materiales. En España, el último incendio de gravedad tuvo lugar en la sierra de la Culebra (Zamora) en el verano de 2022, cobrándose la vida de cuatro personas y calcinando alrededor de 66 000 ha. A nivel internacional se muestran ejemplos de devastación de este tipo de megainciendios, como los ocurridos en Hawái en agosto del 2023 o en Valparaíso (Chile) en febrero del 2024, cobrándose este último la vida de 1331 personas y se calcinaron unas 7 000 viviendas.
— Olas de calor: Los organismos científicos coinciden en que las olas de calor son cada vez más frecuentes, comienzan antes y terminan más tarde. Eso influye directamente en la deshidratación de los combustibles y en la generación de incendios de mayor intensidad, antes del verano y después.
— Aumento de las inundaciones relámpago o Flash Flood[3].
— Tormentas invernales severas[4]: menor ocurrencia que en el pasado, pero de igual o mayor magnitud. Cada vez es más frecuente que a un episodio de nevadas le suceda otro de subida de temperaturas, acompañado de precipitaciones. Esta situación provocará crecidas extraordinarias de los ríos[5] producto del deshielo y las precipitaciones.

[3] *Flash Flood*: inundación relámpago o crecida súbita del caudal del río, torrente de montaña o rambla, como consecuencia de una lluvia muy intensa de corta duración.
[4] Tormentas invernales severas (TIS): emergencias derivadas por gran acumulación de nieve, a consecuencia de grandes nevadas, que originan atrapamientos de gran número de personas, vehículos, restringen el movimiento habitual o dejan poblaciones incomunicadas.
[5] Crecida extraordinaria: que desborda el cauce y supera el caudal de la máxima crecida ordinaria.

— El aumento global de la temperatura como consecuencia del cambio climático tendrá un gran impacto en la desertificación de territorios, con la consiguiente reducción de la disponibilidad de alimentos que impulsará a más población a emigrar a zonas más templadas. Estos movimientos de población se verán acrecentados debido al aumento de la población mundial, que según las previsiones de Naciones Unidas, África duplicará su población actual en el horizonte 2050, con lo que contribuirá al aumento de los flujos migratorios (United Nations, Cambios demográficos).

Una vez estudiadas las amenazas meteorológicas, se analizarán las de carácter geológico, que se dividen en tres grupos bien diferenciados: terremotos, volcanes y tsunamis.

España está situada en una zona considerada moderada, desde el punto de vista de la sismicidad, pero no se debe olvidar que en épocas pasadas se han sufrido terremotos de grandes intensidades. Si estos terremotos se volvieran a repetir, las consecuencias en vidas humanas, económicas, deterioro de los servicios esenciales y daños en las infraestructuras serían catastróficas.

Los terremotos más destructivos ocurrieron antes del siglo XX, como por ejemplo, el terremoto de Arenas del Rey (Granada), en 1884, con una estimación de magnitud de 6,5 Mw e intensidad entre IX-X y que tuvo las siguientes consecuencias: 839 muertos, 4400 edificios destruidos y 13 000 dañados[6]. Aunque las técnicas constructivas han mejorado considerablemente, un terremoto de esta magnitud tendría consecuencias desastrosas para la población.

La actividad volcánica en España se localiza principalmente en las islas Canarias pero existen en la península Ibérica otras áreas con actividad volcánica: Olot (Gerona), Campos de Calatrava (Ciudad Real) y la franja entre el cabo de Gata y el mar Menor.

Por último, los tsunamis asociados a terremotos producidos en el mar son la mayor amenaza actual para la población y un reto para el sistema de respuesta. La repetición de un tsunami como el producido por el terremoto de Lisboa en 1755, al suroeste del cabo de San Vicente, y que produjo daños gravísimos (15 000 muertos), sería actualmente el fenómeno natural más catastrófico debido a la exposición de la gran concentración de población en zonas de costa.

Como se describe anteriormente, la amenaza no ha variado con el paso del tiempo, pero si la exposición de la población.

[6] Véase: https://www.ign.es/web/ign/portal/terremotos-importantes

2.2 *Amenazas tecnológicas y medioambientales*

Las amenazas tecnológicas, al contrario que los naturales, tienen un origen derivado de la acción humana y pueden ser de naturaleza accidental o bien de tipo intencionado. Su carácter súbito e imprevisible, en la gran mayoría de los casos, sumado a que no atiende a ningún tipo de estacionalidad, como sí sucede con los riesgos naturales, hacen que sea una amenaza latente que puede sorprender a los dispositivos de emergencias en cualquier momento.

Los riesgos tecnológicos derivan del desarrollo tecnológico y de la aplicación y uso significativo de las tecnologías. La principal amenaza se focaliza en los riesgos químicos, biológicos, radiológicos y nucleares, sin obviar las derivadas medioambientales de las mismas. Las infraestructuras críticas, el tejido industrial y el medio ambiente son objetivos de alto valor estratégico para los que pretenden desestabilizar la convivencia y el estado de bienestar.

Los principales factores que potencian las amenazas tecnológicas son los siguientes:

— El incremento de población urbana en zonas de peligro ambiental o antrópico, modificando la relación del ser humano con su entorno en varios ámbitos: poblacionales (tamaño y fragilidad), uso y ocupación del suelo, movilidad y desplazamientos de población, conflictos y transporte de mercancías.
— La vulnerabilidad de la infraestructura económica y tecnológica ante riesgos naturales hace que un riesgo natural se transforme en un riesgo tecnológico, conocido como NATECH[7].

La reciente experiencia acontecida por la emergencia sanitaria del COVID-19 y las dificultades sufridas durante los años de pandemia, junto con las dramáticas consecuencias vividas, ponen de manifiesto que el fenómeno de las epidemias y pandemias supone un riesgo significativo de primer orden para la Seguridad Nacional, además de para todo el entorno global.

3 Cómo la inteligencia puede contribuir en la toma de decisiones para responder ante estas amenazas

Como se ha podido comprobar en los apartados anteriores, los riesgos a los que se enfrenta la UME no han cambiado, pero sí se observan nuevas

[7] NATECH (*Technological accidents triggered by a natural hazard*): accidentes tecnológicos desencadenados por un desastre o peligro natural que tiene como resultado consecuencias relacionadas con sustancias peligrosas (por ejemplo, incendio, explosión, liberación tóxica) (UME,PDE3-013).

amenazas, que, debido al cambio climático y a la globalización, han incrementado su frecuencia, intensidad y vulnerabilidad de las personas y sus bienes.

Desde la Sección de Inteligencia del Estado Mayor de la UME debe existir adaptabilidad a estos cambios, al igual que evolución, con una mayor rapidez a lo que lo hacen estas nuevas amenazas, para estar en disposición de presentar al general jefe de la UME valoraciones en las que pueda sustentar sus decisiones.

Las técnicas de análisis aplicadas a la inteligencia en emergencias no difieren en las empleadas por otras unidades militares, con las siguientes especificidades:

— El adversario es la catástrofe, la calamidad o cualquier amenaza que suponga un riesgo para la seguridad de las personas y sus bienes, principalmente.
— Una vez que se produce una catástrofe, el tiempo juega en contra de los intervinientes y de las personas afectadas. Por lo que la respuesta debe ser lo más rápida posible e incluso, si las circunstancias lo permiten, debe estar planificada y preparada antes de la ocurrencia de la propia catástrofe.

Una de las particularidades de las catástrofes es que, en la mayoría de las ocasiones, no es posible anticiparse a ellas. Por lo que la forma más adecuada de poder actuar, rápida y oportunamente, va a ser mediante la realización de un análisis previo de las amenazas que puedan afectar a un determinado territorio, que delimite las zonas de mayor riesgo para cada una de esas amenazas y es aquí, en ese análisis, donde la inteligencia en emergencias juega un papel fundamental.

Una vez identificadas las zonas de riesgo, en función del tipo de amenaza, se debe establecer una serie de indicadores y alertas que prealerten del desencadenamiento de una posible emergencia. La inteligencia en emergencias debe centrar su esfuerzo en llevar a cabo una monitorización permanente de la situación que permita prever una emergencia y anticipar la intervención de la Unidad con la mayor antelación posible.

Por último, y no menos importante, se debe realizar una revisión de los indicadores y alertas para detectar que el proceso por el cual se han generado dichos indicadores y alertas y los umbrales de los mismos es correcto conforme a los eventos y las activaciones de la UME.

3.1 Identificación de las zonas de riesgo

El primer cometido que asumirá la función de inteligencia en emergencias es analizar y determinar las zonas de mayor riesgo donde se pueda

producir una catástrofe en un territorio determinado, pudiendo ser este todo el Territorio Nacional, una comunidad autónoma, una provincia, una comarca, etc., apoyando así el planeamiento de las diferentes campañas que se activan durante el año (incendios forestales, LCIF; Rescate e Inundaciones y Tormentas Invernales Severas, TIS) y los planes de contingencia (COP) que se elaboren.

En esos procedimientos, la inteligencia básica y de objetivos va a ser un elemento fundamental e imprescindible en la obtención de la información inicial necesaria para empezar a dar las primeras respuestas a las necesidades de información que se planteen. Se entiende por inteligencia básica aquella que, con cierto carácter de permanencia, está disponible sobre un tema determinado y se conserva en bases de datos para su consulta, debiéndose actualizar continua y constantemente para mejorarla, lo cual proporciona ese ahorro de tiempo del que se carece.

Por otro lado, la inteligencia de objetivos describe una instalación sensible o crítica como puede ser una presa, una industria SEVESO[8] o una central nuclear. Sitúa las diferentes áreas y elementos que la componen, estudia sus planes de emergencia e identifica sus vulnerabilidades y riesgos. Un estudio profundo de estas infraestructuras permite disponer de un conocimiento previo de cómo podría evolucionar una emergencia en caso de producirse en una de ellas.

Complementando lo anterior, una vez producida la catástrofe se deberá elaborar la inteligencia actual, contemplando: su intensidad y magnitud; sus efectos y consecuencias personales y materiales; los acontecimientos derivados que se hayan podido o se puedan producir como consecuencia de la misma que tengan alguna implicación para las fuerzas intervinientes, los planes activados o la resolución de la emergencia en curso, incluyendo la evaluación del resultado y eficacia de las actuaciones que se estén llevando a cabo durante la misma.

En este punto es importante resaltar el papel fundamental que tiene la meteorología, puesto que no solo afecta a la conducción de las operaciones, sino que suele tener una relación directa, o ser ella misma la causa que ha provocado la emergencia.

Actualmente, todos los organismos nacionales o internacionales con competencias en el estudio de un determinado riesgo publican y comparten en sus páginas web oficiales sus análisis del riesgo en cuestión. La UME dispone de un visor de información geográfica (Sistema de Información

[8] Instalación con riesgo de accidente químico. SEVESO debe su nombre al accidente más grave con sustancias químicas registrado en Europa hasta la fecha. El suceso tuvo lugar el 10 de julio de 1976 en la localidad de Seveso, en el norte de Italia, cerca de Milán (UME, PDE3-013).

Geográfica de la UME, SIGUME) donde, en una única plataforma, se pueden visualizar todos los mapas de riesgo organizado por capas. Este visor almacena en forma de diferentes capas toda la inteligencia básica, de objetivos y actual recopilada por los analistas.

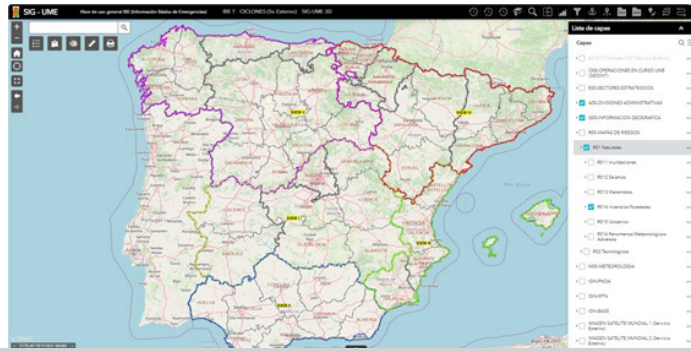

Figura 2. Visor SIGUME Fuente: UME

3.2 Generación de indicadores y alertas

Se trata de un proceso detallado y único para cada uno de los diferentes riesgos naturales y tecnológicos descritos anteriormente. Para poder desarrollar este proceso es necesario que los analistas dispongan de un gran conocimiento sobre cada tipo de riesgo y de cuáles son las variables que pueden desencadenar y potenciar los efectos de una catástrofe.

En la UME, este proceso está dividido en dos fases: la primera consiste en establecer una serie de indicadores y alertas para tratar de establecer si un determinado riesgo se va a producir y en una segunda fase se identifican los indicadores y alertas que adviertan si el riesgo en cuestión será de entidad suficiente para que la comunidad autónoma afectada solicite la activación de la UME.

Para el estudio durante la fase uno, se han identificado una serie de entidades nacionales o autonómicas que ya han desarrollado sus propios indicadores y avisos para cada tipo de riesgo, como pueden ser:

— AEMET que a través de su plan Meteoalerta, pretende facilitar toda la información posible sobre los fenómenos meteorológicos adversos que puedan afectar a España por un plazo máximo de sesenta horas y mantener la información sobre el evento una vez iniciado[9]. La AEMET también proporciona el riesgo de incendios forestales para España con un horizonte temporal de siete días.

[9] Véase: https://www.aemet.es/es/lineas_de_interes/meteoalerta

— Los Sistemas Automáticos de Información Hidrológica (SAIH) de las diferentes confederaciones hidrográficas que proporcionan información, en tiempo real, de los niveles y caudales de los principales ríos y afluentes, así como, el nivel y volumen de los embalses[10].
— El Instituto Geográfico Nacional (IGN) proporciona datos en tiempo real sobre los terremotos producidos, vigilancia volcánica y maremotos[11].

Pero también existen entidades europeas o internacionales que proporcionan indicadores y avisos sobre diferentes riesgos a nivel mundial como pueden ser:

— Programa Copernicus de la Unión Europea, que dispone de tres sistemas de alerta temprana. El European Flood Awareness System (EFAS)[12] que ofrece previsiones de inundación hasta diez días de antelación a nivel Europeo. El European Forest Fire Information System (EFFIS)[13] que proporciona información histórica y en tiempo cuasireal sobre incendios forestales en Europa. El European Drought Observatory (EDO)[14] que proporciona información y alerta temprana de sequía en Europa.
— La Nasa dispone de un Sistema de Información de Incendios (FIRMS)[15] que muestra los incendios activos en tiempo cuasireal a escala global.
— La Organización de las Naciones Unidas (ONU) cuenta con una red mundial de alerta y respuesta GOARN (Global Outbreak Alert and Response Network)[16]. Es un mecanismo de colaboración técnica entre instituciones y redes ya existentes que aúnan recursos humanos y técnicos para identificar, confirmar y responder rápidamente a brotes epidémicos de importancia internacional.

Como se puede observar, se disponen de herramientas suficientes que proporcionan, con un alto grado de fiabilidad, información que un tipo de riesgo pueda ocurrir en un horizonte temporal de hasta siete días. Pero existen riesgos que no son tan fáciles de predecir cómo pueden ser los terremotos o los riesgos tecnológicos que, al contrario de los naturales, tienen un origen derivado de la acción humana y que pueden ser de naturaleza accidental o bien de tipo intencionado. Su carácter súbito e imprevisible y

[10] Disponible en: https://www.miteco.gob.es/es/agua/temas/evaluacion-de-los-recursos-hidricos/saih.html
[11] Véase: https://visualizadores.ign.es/tproximos/
[12] Disponible en: https://www.copernicus.eu/en/european-flood-awareness-system
[13] Véase: https://www.copernicus.eu/en/european-forest-fire-information-system
[14] Disponible en: https://www.copernicus.eu/en/european-drought-observatory
[15] Véase: https://firms.modaps.eosdis.nasa.gov/
[16] Disponible en: https://goarn.who.int/

que en la gran mayoría de los casos no atiende a ningún tipo de estacionalidad, como sí sucede con los riesgos naturales (incendios forestales, inundaciones o tormentas invernales) hacen que la inteligencia de objetivos sea la única manera de poder reducir los tiempos de respuesta y asesoramiento sobre las técnicas, tácticas y procedimientos de emergencias a emplear.

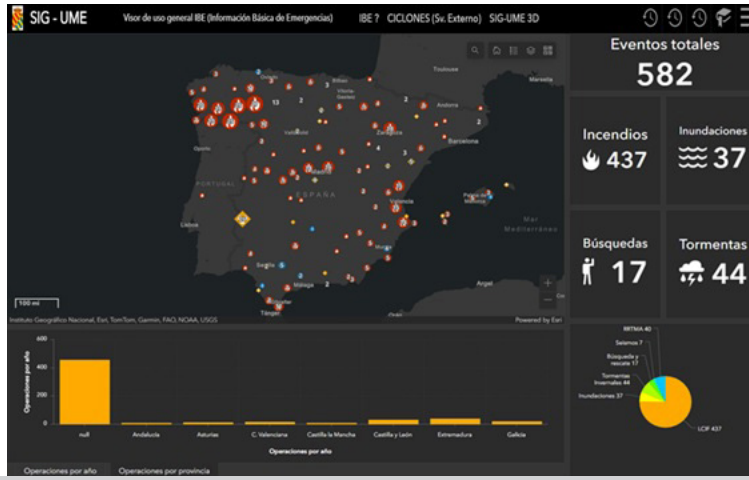

Figura 3. Visor de eventos a nivel nacional de SIGUME. Fuente: UME

Durante la segunda fase, y una vez observado que un riesgo tiene una alta probabilidad de manifestarse o ya está ocurriendo, se deben estudiar otros indicadores que permitan identificar si puede ser requerida la activación de la UME por las autoridades competentes.

En esta fase se incluyen los estudios de las zonas de riesgos, vulnerabilidad de la población, afectación de servicios esenciales, capacidades de los servicios de emergencias de cada comunidad autónoma, planes de protección civil activados, datos históricos de eventos anteriores y operaciones donde la UME ha sido activa.

Debido a que las competencias en materias de protección civil en España están delegadas en las comunidades autónomas y a los diferentes climas existentes en el territorio nacional hay que particularizar el análisis a cada comunidad autónoma y región climática.

Además, la UME dispone de diferentes simuladores que permiten conocer hacia donde puede evolucionar un incidente. En cuanto a riesgos naturales, se dispone de simuladores de incendios forestales y terremotos. En cuanto a riesgos tecnológicos, el Grupo de Intervención en Emergencias Tecnológicas y Medioambientales (GIETMA) de la UME dispone de simuladores de tipo nuclear (RADPROCALCULATOR o el JEM), químico (ALOHA o el CBRN Análisis) y biológico (JEM) para la ayuda a la toma de decisiones.

Gracias a estos simuladores se puede predecir el impacto que podría tener el evento sobre la población y sus bienes.

Una vez realizado este proceso desde la sección de inteligencia de la UME se presenta una serie de alertas para cada tipo de riesgo y provincia en forma de semáforo con cuatro colores:

- Verde: baja probabilidad de ocurrencia de un riesgo.
- Amarillo: alta probabilidad de ocurrencia de un riesgo pero baja probabilidad de activación de la UME.
- Naranja: alta probabilidad de ocurrencia de un riesgo y probabilidad moderada de activación de la UME.
- Rojo: alta probabilidad de ocurrencia de un riesgo y probabilidad alta de activación de la UME.

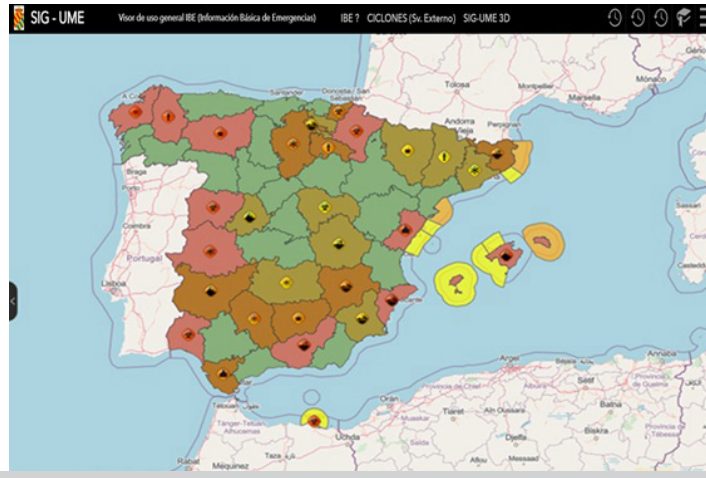

Figura 4. Visor de indicadores de alerta a nivel nacional del SIGUME.
Fuente: UME

3.3 *Revisión de indicadores y alertas*

Este proceso debe ser constante y continuo, donde el analista debe descomponerlo en dos fases. Primero identificar si la valoración inicial sobre la ocurrencia del riesgo se ha presentado conforme a lo analizado y, segundo, si ese evento producido ha desencadenado una activación de la UME.

Las redes sociales y prensa digital tienen una gran importancia en este proceso, ya que, permiten tener una idea clara de las dimensiones del evento producido. Para ello la UME utiliza varias herramientas OSINT[17] que facilitan tanto el seguimiento y monitorización de los eventos como detectar

[17] *Open Sources intelligence.* Inteligencia de fuentes abiertas.

los daños causados. Las imágenes obtenidas por los satélites, también, son una gran herramienta para comprobar la magnitud del evento.

Cotejar los datos iniciales de la previsión del evento y la evaluación inicial de los daños con los datos reales y daños causados es una gran herramienta para actualizar los umbrales de los indicadores y alerta. Además, este proceso permite establecer patrones de repetición de eventos que al compararlos con las predicciones futuras mejorarán los indicadores de alerta de activación de la UME.

4 Futuro de la inteligencia en emergencias

Como se ha podido observar, los analistas de la UME deben de analizar una gran cantidad de datos e indicadores y establecer una línea de análisis por cada riesgo definido, comunidad autónoma y región climática. Actualmente el proceso de análisis se reduce a monitorizar y seguir un número limitado de variables y simplificar el proceso de análisis de forma que el analista pueda controlarlo en todo momento.

Pero, hoy en día, existe un entorno donde las nuevas tecnologías están evolucionando de manera exponencial y permiten que las entidades con responsabilidades en la gestión del riesgo elaboren nuevos productos. Y, sobre todo, han conseguido reducir los periodos de actualización de sus productos de riesgo de un horizonte temporal de décadas a actualizarlos casi anualmente.

Gracias a todo lo anterior, el SIGUME cada vez compila más información que podrá ser incorporada al proceso de análisis de la UME. Pero esta información tiene que ser lo más actual posible y las entidades oficiales tienen periodos de actualización de las diferentes capas que van desde el tiempo real hasta pocos años, lo que conlleva un esfuerzo enorme de actualización permanente. Pero el principal problema al que se está enfrentando el analista es la sobreinformación y que no es capaz de gestionar la cantidad de información disponible.

Además, como ya se ha mencionado en las fases iniciales de este documento, la amenaza está variando en intensidad y estacionalidad, afectando a una mayor población debido principalmente al cambio climático, globalización, crecimiento de la población y abandono rural. Por lo tanto, los periodos de tiempo para estudio de patrones se encuentran actualmente desfasados, por lo que se debe reducir el tiempo de estos estudios a los últimos años para ajustar y contemplar estos nuevos cambios.

Por ello, la UME se encuentra en un proceso de evolución donde se considera que las herramientas de inteligencia con las que actualmente se trabaja deben de ser potenciadas e integrar nuevas tecnologías como inteligencia artificial (IA), *deep learning* y *big data*.

Por este motivo están estudiando nuevas líneas de trabajo para mejorar el análisis de inteligencia en emergencias:

- Disponer de una base de datos georrefenciada que contenga la Información Básica de Emergencia (IBE) con toda la inteligencia básica, de objetivo y actual de manera organizada. Y, sobre todo, que sea capaz de integrar de forma ágil y rápida los nuevos productos publicados por las diferentes entidades con responsabilidad en la gestión del riesgo tanto a nivel nacional como internacional.
- Elaborar un registro de eventos capaz de almacenar y registrar de manera automática todos los datos de predicción y observación, así como, los efectos o daños producidos e incorporar las diferentes bases de datos históricos que las entidades nacionales con responsabilidad en la gestión del riesgo generan.
- Integración de herramientas de IA, deep learning y big data en el SIGUME, capaces de procesar la ingente cantidad de datos que el analista tiene a su disposición. El analista intervendrá en la definición de variables, cómo se relacionan entre ellas y su ponderación y establecerá los indicadores y alertas. Mientras que estas tecnologías se encargarán de automatizar todos los procesos, de gestionar y procesar los datos, integrar las distintas capas en el análisis definido por el analista, identificar patrones y corregir y evaluar los indicadores y alerta.
- Integrar en el SIGUME un gemelo digital del terreno de alta resolución a escala nacional. La Comisión Europa ha puesto en marcha una iniciativa denominada Destination Earth (DestinE) con el objetivo de desarrollar un gemelo digital del terreno a escala mundial que supervisará, simulará y predecirá la interacción entre los fenómenos naturales y las actividades humanas[18]. Esta iniciativa se centrará en los efectos del cambio climático y los fenómenos meteorológicos adversos extremos, su impacto socioeconómico y las posibles estrategias de adaptación y mitigación.
- Integrar simuladores en el SIGUME de forma que se puedan reproducir los eventos en el gemelo digital del terreno para ser capaz de identificar las zonas con mayor probabilidad de daños, población afectada, etc..., permitiendo que se puedan tomar las decisiones oportunas en tiempos próximos al real. Se está estudiando integrar los siguientes simuladores:
  - Meteorológicos: con capacidad de simular las previsiones meteorológicas de forma reducida (disminuyendo la generación y procesado de los datos). El analista, además, podrá actuar sobre las principales variables meteorológicas (temperatura, humedad,

[18] Disponible en: https://digital-strategy.ec.europa.eu/es/policies/destination-earth#tab_2

precipitación, viento, etc), para poder simular los escenarios más probables y más peligrosos.
  - Incendios forestales: mejora de los actuales y con capacidad de lanzar simulaciones automáticas en base a los puntos calientes proporcionados por los satélites, alertando de los incendios que tienen gran probabilidad de desarrollo o que interfieran con la vida normal de las personas.
  - Inundaciones: este simulador deberá integrar los datos en tiempo real de caudales, previsiones meteorológicas (precipitación, deshielo, escorrentía) y zonas de riesgo, de forma que se puedan identificar las zonas inundables más probables.
  - Sísmico: a partir de los datos en tiempo real reportados por la Red Sísmica Nacional lanzar simulaciones que indiquen las estimaciones de las zonas más afectadas, incluyendo edificios colapsados, dañados e intactos así como la estimación de víctimas.
- Integrar herramientas OSINT en el SIGUME para poder analizar toda la información relacionada con RRSS. Actualmente las RRSS sociales tienen un papel fundamental a la hora de identificar las nuevas amenazas y permite realizar un seguimiento de las mismas a través de la información que publican las fuentes oficiales y el personal próximo a la emergencia.

5 Conclusión

Son muchas las fuentes que apuntan que las amenazas a las que se van a enfrentar los servicios de emergencias no han variado con respecto a años anteriores. Pero sí se está observando que debido al cambio climático y otros factores de carácter antrópico, como pueden ser la globalización, abandono del medio rural y ocupación por parte de la población de las zonas de riesgo, la amenaza a la que se enfrenen dichos servicios será mayor y más acentuada según pasen los años.

La inteligencia en emergencia tiene un papel clave a la hora de alertar sobre los posibles riegos que puedan afectar a la población. El proceso de análisis basado en indicadores y alertas se puede considerar el más idóneo para prever una posible emergencia, pero debido a la gran cantidad de datos que se obtienen de las diferentes fuentes de información, este proceso está sobrepasando la capacidad de análisis del analista y se hace imprescindible recurrir a la simplificación del problema desechando en algunos casos variables que pueden tener importancia en el estudio del riesgo.

Por ello, la UME propone un cambio de paradigma en el uso de tecnologías que ayuden al analista a resolver el problema complejo al que se enfrenta en su quehacer diario. La AI, *deep learning* y *big data* han llegado

para quedarse y es importante hacer un profuso uso de ellas. Sobre todo, para mejorar la calidad y eficiencia del análisis, reduciendo la carga de trabajo rutinaria de forma que ese tiempo pueda ser empleado en el estudio de las nuevas amenazas y en mejorar su asesoramiento a la hora de alertar de una posible emergencia con la mayor antelación posible.

Bibliografía

Agencia Estatal de Meteorología. (2022). *Plan Nacional de Predicción y Vigilancia de Fenómenos Meteorológicos adversos. Meteoalerta*. [Consulta: 2024]. Disponible en: https://www.aemet.es/documentos/es/eltiempo/prediccion/avisos/plan_meteoalerta/plan_meteoalerta.pdf

España. (2015). Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil. Referencia: BOE-A-2015-//30. [Consulta: 2024]. Disponible en: https://www.boe.es/eli/es/l/2015/07/09/17/con

—. (2021). Real Decreto 1150/201, de 28 de diciembre, pro el que se aprueba la Estrategia de Seguridad Nacional 2021. Referencia: BOE-A-20121-21884. Disponible en: https://www.boe.es/eli/es/rd/2021/12/28/1150

Instituto Geográfico Nacional. (s. f.). *Terremotos más importantes*. [Consulta: 2024]. Disponible en: https://www.ign.es/web/ign/portal/terremotos-importantes

Intercovernmental Panel on Climate Change. (2021). *Intergovernmental Panel on Climate Change, Climate Change 2021*. [Consulta: 2024]. Disponible en: https://www.ipcc.ch/report/ar6/wg1/downloads/report/IPCC_AR6_WGI_SPM_final.pdf

Naciones Unidas. (2022). *Global Assement Reporto n Disaster Risk Redution*. [Consulta: 2024]. Disponible en: https://www.undrr.org/media/79595/download?startDownload=true org)

—. (2024). Cambios demográficos. [Consulta: 2024]. Disponible en: https://www.un.org/es/un75/shifting-demographics

Oria Iriarte, P. (2021). *¿Está aumentando la frecuencia o intensidad de las precipitaciones extremas en el Mediterráneo?* [Consulta: 2024]. Disponible en: https://aemetblog.es/2021/05/02/esta-aumentando-la-frecuencia-o-la-intensidad-de-las-precipitaciones-extremas-en-el-mediterraneo/

Unidad Militar de Emergencias. (2021). *PDE3-013 Riesgo tecnológicos y medio ambientales (RRTTyMA)*.

Unidad Militar de Emergencias. (2020a). *PDE3-002 Inteligencia y Seguridad de la Unidad Militar de Emergencias*.

Unidad Militar de Emergencias. (2020b). *Pr2-207 Indicadores para seguimiento y monitorización de emergencias por los centros de operaciones y seguimiento de la UME*.

Artículo decimocuarto

Contrainteligencia en el ámbito aeroespacial: amenazas a la libertad de acción del EA en el actual entorno de seguridad

Alberto Díaz Martín

«Es más fácil y eficaz destruir el poder aéreo del enemigo destruyendo sus nidos y huevos en el suelo que cazando sus pájaros volando en el aire».

General Giulio Douhet

«Every airman should have his place in the defence scheme. It must be understood by all ranks that they are expected to fight and die in the defence of their airfields [...]. Every airfield should be a stronghold of fighting air-groundmen, and not the abode of uniformed civilians in the prime of life protected by detachments of soldiers».

Sir Winston S. Churchill

Resumen

El entorno de seguridad global actual se caracteriza por una enorme complejidad debida a una diversidad de factores como la aparición de tecnologías disruptivas o el surgimiento de actores no estatales de influencia global. Todo esto ha propiciado un cambio en la tipología de los conflictos, caracterizada por una zona gris donde las acciones hostiles llevadas a cabo por potencias antagonistas tratan de pasar desapercibidas o confundirse con otras legítimas, generando efectos, principalmente en el ámbito cognitivo, con el objetivo de limitar la capacidad de respuesta del adversario.

Este tipo de acciones encubiertas, diferentes de las actividades convencionales típicamente militares, pero que pretenden los mismos objetivos que estas, son muy difíciles de identificar y, más aun, de neutralizar. Su importancia se acrecienta día a día, especialmente ante la posibilidad,

hasta hace poco considerada poco probable, de una guerra en la que participara España junto con sus aliados.

El Ejército del Aire y del Espacio, por sus particulares características, es especialmente vulnerable a este tipo de amenazas y, al mismo tiempo, objetivo prioritario de ellas, por lo que su comprensión y el diseño de medidas para su neutralización resultan de la máxima importancia. De estas tareas se encarga la contrainteligencia militar.

Palabras clave

Amenazas no convencionales, TESSCO, Servicios de inteligencia, Zona gris, Guerra híbrida.

Counterintelligence in the aerospace domain: threats to the Air and Space Force's freedom of action in the current security environment

Abstract

The current global security environment is characterized by enormous complexity due to a variety of factors such as the appearance of disruptive technologies or the emergence of non-state actors with global influence. All this has led to a change in the typology of conflicts characterized by a gray zone where hostile actions, carried out by antagonistic powers, try to go unnoticed or be confused with other legitimate ones, generating effects, mainly in the cognitive field, with the aim of limiting the adversary's ability to respond.

This type of covert actions, different from typically military conventional activities, but seeking the same objectives, are very difficult to identify and to neutralize. Its importance increases day by day, especially given the possibility, until recently considered unlikely, of a war in which Spain would participate along with its allies.

The Spanish Air and Space Force, due to its particular characteristics, is especially vulnerable to this type of threats and, at the same time, a priority target for them, so its understanding and the design of measures to neutralize them is of the utmost importance. Military counterintelligence is responsible for these tasks.

Keywords

Unconventional threats, TESSOC, Intelligence services, Gray zone, Hybrid warfare.

1 Introducción. El entorno de seguridad global actual: zona gris y conflictos complejos

España y los países del entorno se encuentran inmersos en una situación de conflictividad permanente, a todos los niveles, y con presencia de múltiples actores. Esta situación ha provocado que, en los últimos años, la polemología haya incorporado nuevos conceptos para caracterizar los conflictos actuales como son zona gris, guerra híbrida, conflicto asimétrico o el término conflicto complejo.

El término zona gris se refiere al estadio de conflictividad entre estados o bloques que va desde una situación de paz (ausencia de conflicto) a la guerra abierta o declarada. En este extenso intervalo se producen acciones hostiles diferentes a las tradicionales acciones llevadas a cabo por fuerzas militares. La característica principal de este tipo de actividades, denominadas generalmente acciones no convencionales, es que son llevadas a cabo por actores diferentes a las fuerzas regulares. La opacidad, ubicuidad, decepción y clandestinidad son características propias de este tipo de acciones y su fin suele ser generar efectos sin provocar una respuesta bélica por parte del adversario. Estas acciones pueden ser de cualquier naturaleza, incluyendo la violencia extrema, y no se ven limitadas por norma legal, nacional o internacional, o tratado alguno.

La guerra híbrida se refiere a un tipo de conflicto en el que, simultáneamente, se producen acciones típicas de la guerra convencional, llevadas a cabo por fuerzas militares, y acciones no convencionales propias de la zona gris.

Conflicto asimétrico es un término que se refiere a un tipo de conflicto en el que los contendientes presentan una muy marcada disparidad entre fuerzas o, sobre todo, una notable diferencia en su sometimiento a límites legales o morales. Este tipo de conflictos se desarrollan en los ámbitos físicos tradicionales (tierra, mar y aeroespacial), pero también en el muy tecnológico ámbito del ciberespacio. Sus acciones tienden a producir efectos, sobre todo, en el ámbito cognitivo. En el contexto de seguridad actual, este tipo de operaciones suelen tener como objetivo mantener a la sociedad de uno de los estados contendientes confundida sobre la naturaleza real del conflicto, sus actores o sus motivaciones y así conseguir que esta nación no movilice todas sus capacidades de defensa.

Ejemplos de operaciones no convencionales fueron las llevadas a cabo por fuerzas paramilitares (personal pertrechado y actuando como militar pero sin divisas o banderas que pudieran identificarlos como fuerzas regulares) durante la invasión de la península de Crimea por Rusia en el 2014. Aunque se pudo establecer que sus integrantes eran militares rusos en activo, el Gobierno de Putin los bautizó como «batallones de autodefensa»

ucranianos, negándose así a reconocer la implicación de las Fuerzas Armadas de Rusia, siguiendo una clara estrategia de limitar la capacidad de respuesta internacional y una contestación interna (Haines, 2016).

Otro ejemplo de este tipo de operaciones es el uso de compañías privadas militares (PMC), en el caso de Rusia y otros países como EE. UU., o compañías privadas de seguridad (PSC), en el caso de China, para realizar actividades propias de fuerzas militares sin tener que reconocer esta actividad, tratando así de conseguir objetivos militares por medios no militares. El ejemplo más conocido es el de la PMC Wagner dirigida hasta su muerte, en agosto del 2023, por Yevgeny Prigozhin.

Pero quizá el ejemplo más común, actualmente, sea el empleo continuo e indiscriminado de organizaciones criminales, muy especialmente de ciberdelincuentes, para causar daños a las infraestructuras del adversario, tanto civiles como militares.

De este modo, se puede afirmar que el entorno de seguridad global actual se caracteriza por la presencia de conflictos complejos en los que las nuevas tecnologías y los cambios sociales han producido una nueva forma de hacer la guerra mediante acciones híbridas que mezclan todo tipo de amenazas, protagonizadas por una diversidad de actores, en muchos caso diferentes de las fuerzas militares.

La doctrina militar se está adaptando a este entorno evolucionando, por ejemplo, hacia las operaciones multidominio. Esta adaptación debe tener muy en cuenta las amenazas no convencionales, las cuales tienen un enorme protagonismo en los conflictos actuales y, se prevé, lo vayan a tener aún más en el futuro.

Para proporcionar a los decisores un adecuado conocimiento de la situación y contrarrestar estas amenazas, la contrainteligencia (CI) se presenta como una disciplina imprescindible. Lamentablemente, en no pocos momentos, esta especialidad de la inteligencia ha sido tratada como el «patito feo» frente al área que trata las amenazas convencionales. Quizá esto se deba al hecho de que la CI nunca se ha entendido correctamente por lo difícil que esto resulta debido a la naturaleza esquiva de las amenazas de las que trata.

2 Las amenazas a la seguridad del EA: negar o limitar su libertad de acción

En el marco de las operaciones militares llevadas a cabo por el Ejército del Aire y del Espacio (EA) y el resto de las Fuerzas Armadas, los actores hostiles a los que deban enfrentarse intentarán siempre negar o limitar su capacidad de acción. Esto lo pueden tratar de alcanzar por medio de acciones convencionales o por otras no convencionales.

El primer caso tendrá lugar, muy probablemente, en situaciones de conflicto armado, mientras que las acciones no convencionales se podrán producir en todo el espectro del conflicto con el objetivo de degradar las capacidades de un adversario mientras se niega a este sus opciones de respuesta.

En tiempo de paz o crisis esto se consigue mediante acciones hostiles graduadas, de acuerdo con las limitaciones legales y los factores sociales de la nación o grupo social objetivo, sin que estas sean percibidas como suficientes para escalar la crisis a un conflicto armado. Para alcanzar este fin, la clandestinidad y la no atribución son factores clave.

En la doctrina rusa, por ejemplo, esto se conoce con el término «Medidas Activas» y de su planeamiento y ejecución se encargan principalmente sus servicios de inteligencia (Galeotti, 2019). Entre estas medidas se encuentran las acciones de influencia o subversión, el espionaje o el sabotaje. Medidas similares las implementan también otros estados potencialmente hostiles.

Se ha constatado un creciente interés, por parte de estos actores en las actividades que sean capaces de degradar la operatividad de un posible adversario, como podrían ser el EA, para posicionarse en una situación de ventaja en caso de conflicto armado. Este tipo de actividades preparatorias previas a un conflicto no son una novedad, siendo la más común de ellas la obtención de inteligencia.

Sin embargo, en los últimos tiempos, debido a los avances tecnológicos, las transformaciones sociales y los cambios geopolíticos, este tipo de acciones no convencionales han tomado una nueva dimensión, generando un espacio de permanente conflictividad (zona gris) en el que se llevan a cabo todo tipo de acciones encubiertas, algunas asimilables a acciones militares.

Estas acciones son más frecuentes y más agresivas cuanto mayor es la proximidad, dentro del espectro de los conflictos, a una situación de guerra. Lo mismo ocurre cuanto más se acortan las distancias geográficas con el adversario, como ocurre en los destacamentos del EA en Europa del Este, Irak o el norte de África.

Muchas de estas acciones hostiles se llevan a cabo en el ámbito cognitivo, como es el caso de las acciones relacionadas con la subversión, tratando de producir efectos, no solo en los gobiernos o la población civil, sino también en las fuerzas militares. Otras son más directas, generando la capacidad de llevar a cabo acciones especiales en el futuro, cuando el agresor lo considere adecuado, mediante el establecimiento de redes de colaboradores, la implantación de elementos tecnológicos que puedan producir efectos (usualmente *malware*) o la obtención de inteligencia sobre

personas o capacidades de alto valor, como ocurre con los pilotos y aviones de combate o los radares de identificación y alerta temprana del EA.

Las naciones potencialmente hostiles suelen recurrir a sus servicios de inteligencia para la realización de este tipo de acciones. Algunas de ellas, como es el caso de Rusia o China, poseen enormes capacidades, tanto técnicas como humanas, además de una dilatada experiencia y sus formas de actuación tienen un amplio reflejo en su doctrina militar.

De todo lo anterior, no cabe duda de que, en caso de participación en un conflicto bélico, las bases aéreas suponen un objetivo de alto valor para las fuerzas enemigas por lo que estas emplearán todos los medios a su alcance para neutralizar o degradar su operatividad. Por lo tanto, su defensa resulta una prioridad absoluta, estableciéndose así una competencia entre medios ofensivos del enemigo y defensivos propios.

Existe el grave riesgo de confiar esta defensa solamente a capacidades tecnológicas típicas del poder aéreo como aviones, radares y misiles, y pasar por alto o subestimar las capacidades no convencionales del enemigo. Estas capacidades no convencionales son, frecuentemente, mucho más accesibles y fáciles de implementar, como han demostrado los potenciales adversarios en numerosas ocasiones.

3 TESSCO: terrorismo, espionaje, sabotaje, subversión y crimen organizado

Las amenazas de naturaleza no convencional a las que se enfrenta actualmente el EA se pueden resumir en el acrónimo TESSCO (terrorismo, espionaje, sabotaje, subversión y crimen organizado), parte nuclear de las responsabilidades de la CI. Las principales características de estas amenazas se deducen de su naturaleza ubicua y encubierta, lo que hace que sean muy difíciles de detectar y contrarrestar.

Todas ellas afectan directamente a las operaciones del EA y se encuentran activas en este mismo momento, en algún lugar y en alguna de sus fases de planeamiento, aprovisionamiento, preparación o ejecución.

En muchos casos, detrás de estas amenazas se encuentran servicios de inteligencia hostiles (SIH). En otros, sus promotores son organizaciones no estatales o individuos aislados, afiliados a alguna de estas organizaciones por causas diversas, desde ideológicas a económicas.

La reserva y ocultación propias de las actividades de la inteligencia cobran una mayor transcendencia en el caso de la CI, ya que esta se encarga de obtener inteligencia de otras organizaciones de inteligencia.

La CI existe como una especialidad de la inteligencia precisamente por esta exclusiva característica de las amenazas que trata. Por lo tanto, la

amenaza que suponen estos SIH resulta especialmente difícil de detectar por lo que el hecho de que estas amenazas no resulten evidentes no debe llevar a suponer que no estén presentes.

Existen numerosos ejemplos en la historia de los servicios de inteligencia aliados de casos de espionaje descubiertos muchos años después de que cesara su actividad y cuando el daño infringido era ya difícil de reparar. Esta capacidad para no generar una respuesta en la organización objetivo, por pasar estas amenazas desapercibidas, supone la mayor ventaja de los SIH y el mayor reto para la CI del EA y las FF. AA.

Otra característica de las amenazas TESSCO es que no suelen presentarse aisladas sino mezcladas entre sí o con otras amenazas convencionales u ocultas bajo la apariencia de actividades legítimas o amparadas por estas.

Como consecuencia de todo lo anterior, detectar y contrarrestar este tipo de actividades requiere contar con avanzadas capacidades y con profesionales dedicados con un elevado grado de adiestramiento, además de mucho tiempo y la implicación de todo el personal de la organización. Esto es especialmente importante en el caso de acciones hostiles llevadas a cabo o que cuenten con la colaboración de agentes internos al EA (*insiders*), como ocurre frecuentemente.

Un ejemplo que demuestra claramente lo aquí expuesto es la intensa actividad de los servicios de inteligencia de la Federación Rusa en Ucrania en los ocho años que van desde la llamada «Revolución del Euromaidán» hasta la invasión del país en febrero de 2022, actividades dirigidas precisamente a la preparación de esta invasión (Watling et *al*., 2023).

A continuación, se tratan someramente las características de las diferentes amenazas TESSCO en relación al entorno de seguridad global actual y las operaciones del EA.

3.1 Subversión: operaciones hostiles en el ámbito cognitivo

La subversión, en el ámbito de las operaciones militares, se puede definir como el conjunto de acciones que tratan de degradar la lealtad y la confianza de una fuerza en sus mandos, su voluntad de combate o dañar el apoyo de la sociedad a la que sirven.

Se materializa en operaciones sicológicas de diferente naturaleza que se llevan a cabo durante largos periodos de tiempo y son muy difíciles de detectar y contrarrestar por camuflarse como conflictividad social y afectar a derechos fundamentales como la libertad de expresión. Sus efectos pueden no ser evidentes en tiempo de paz, pero ponerse de manifiesto de forma abrupta al inicio o durante una crisis o conflicto.

Aunque han estado históricamente siempre presentes, siendo por ejemplo el eje de la «Medidas Activas» empleadas por la inteligencia de la URSS y Rusia desde mediados del siglo XX, las herramientas que pone al alcance la nueva sociedad de la información permiten que sea una amenaza de aún mayor transcendencia.

Existen, por lo tanto, razones para considerar la subversión como la amenaza TESSCO más importante y una de las más significativas a las que se enfrentan las sociedades occidentales y sus fuerzas armadas, incluido el EA.

Las acciones de subversión pretenden alcanzar efectos en el ámbito cognitivo cambiando la percepción de la realidad de la audiencia objetivo. Cuando se realizan con éxito pueden incluso conseguir que una amenaza no sea reconocida como tal, imposibilitando así cualquier acción defensiva, de ahí su valor.

Cuando estas acciones tienen como objetivo dañar el EA, se pueden realizar de dos formas:

— De forma indirecta, dirigiéndose a la ciudadanía española para desacreditar al ejército, privándole del necesario apoyo que requiere para su operación en cuanto a soporte legal y de recursos.
— De forma directa, dirigiéndose a los propios militares para conseguir diferentes efectos como el descrédito de los jefes y la creación de redes de mando paralelas, afectando al mando y control de las operaciones; la creación de un clima de confrontación social interno; la degradación de la confianza o la moral de la fuerza, y la percepción engañosa de la realidad en relación con la justificación de sus operaciones militares o el resultado o los efectos de estas.

Este tipo de actividades suelen estar planeadas para ser ejecutadas durante muy largos periodos de tiempo antes de conseguir sus efectos y se basan en la explotación de las vulnerabilidades sicosociales de las audiencias objetivo.

Por último, estas acciones se camuflan entre actividades legítimas como las actividades culturales, la acción política o sindical, la libertad de prensa, de opinión, credo y expresión, o la lícita competitividad entre estados.

Todo lo anterior convierte a este tipo de amenazas en desafíos muy peligrosos por la gravedad de sus efectos, por lo difícil de su identificación y neutralización y por lo económicas que resultan para el actor agresor, especialmente con las herramientas que ofrece actualmente el ciberespacio y la sociedad de la información. Pueden conseguir la derrota de un adversario sin llegar a combatir[1].

[1] La frase «la mejor victoria es vencer sin combatir» se atribuye al filósofo y estratega militar chino Sun Tzu (c. siglo V a. C.) y resume un concepto todavía presente en la doctrina militar de este país.

Además, suponen un precursor de las acciones de terrorismo o espionaje, debido que la subversión de un grupo o individuo, en forma de adoctrinamiento, radicalización o cambio de lealtades, es el paso previo a la comisión de este tipo de acciones hostiles.

3.2 *Espionaje: las operaciones de inteligencia del adversario*

Los países que pueden tener interés en conocer información crítica sobre las capacidades o las operaciones encomendadas al EA son aquellos a los que España o sus aliados podrían llegar a enfrentarse en un conflicto armado. Estos países disponen de significativas capacidades para realizar exitosas operaciones de inteligencia. Y el criterio principal para que estas operaciones resulten fructíferas para el agresor es, precisamente, que no sean detectadas por la víctima.

Los ejemplos conocidos de este tipo de acciones son las que finalmente terminaron fallando. De las que resultaron fructíferas durante todo el periodo que estuvieron activas solo se ha sabido algo mucho tiempo después, cuando esta información ya no era relevante, o no se tiene ningún conocimiento de ellas aún hoy en día.

Incluso países con limitado potencial militar, como es el caso de Cuba, son capaces de infligir un daño considerable a potencias como los EE. UU. El caso de Ana Montes, ciudadana americana analista del área de Cuba en la *Defence Intelligence Agency* (DIA), equivalente al CIFAS, es muy significativo, ya que estuvo pasando información a la Dirección de Inteligencia (DI) cubana durante dieciseis años, hasta su arresto en 2001 (Federal Bureau of Investigation, s. f).

Cuba es un país conocido por actuar como *proxy* de Rusia en muchas áreas, especialmente en la de inteligencia. Pero la lista de naciones que podrían ejecutar acciones de espionaje contra España es larga e incluye, incluso, naciones consideradas aliadas, interesadas en conocer las intenciones del país respecto a potenciales conflictos o la tecnología aeroespacial de la que se dispone, para favorecer a su propia industria de defensa.

Para la detección de las actividades de espionaje resulta fundamental la concienciación y colaboración de todo el personal del EA[2] que permita detectar comportamientos anómalos y una sólida capacidad de investigación de CI.

A todo lo anterior hay que añadir las operaciones ISR del adversario, las cuales son ahora más frecuentes por la utilización generalizada de UAS[3] y

[2] Un ejemplo de este tipo de colaboración es el programa Eagle Eyes de la *US Air Force*. Disponible en: https://www.jbsa.mil/News/News/Article/2035476/eagle-eyes-program-urges-people-to-say-something-if-they-see-something/

[3] *Unmanned Aerial System*.

el acceso al espacio de un mayor número de países, materia merecedora de un estudio aparte.

3.3 Sabotaje: acciones cinéticas bajo el umbral del conflicto

Las operaciones de sabotaje se pueden calificar como «un clásico» de las operaciones militares encubiertas y, por lo tanto, una de las amenazas no convencionales más importantes. Sin embargo, en los países occidentales no se les suele dar la importancia que merecen y que sí reciben en países que pueden llegar a ser adversarios de España en un conflicto armado, como es el caso de Rusia.

La característica principal de estas acciones es que se realizan por el enemigo en el propio territorio o zona controlada. Para su realización requieren de una intensa preparación y, en muchos de los casos, de la colaboración de personal propio o afín, actuando como agentes del enemigo.

Su ejecución puede ocurrir en el marco de un conflicto armado o en ausencia de este (zona gris), pero su planeamiento y preparación necesita llevarse a cabo en momentos previos al conflicto, incluso mucho tiempo antes, mediante acciones de inteligencia para la selección y análisis de objetivos y mediante el reclutamiento de agentes, el establecimiento de redes de apoyo o, incluso, acciones directas.

El valor de estos ataques, cuando se producen por debajo del umbral del conflicto, no reside tanto en las pérdidas causadas, sino en su capacidad de influir en la sociedad, ciertos actores de esta, como sus Fuerzas Armadas, o las autoridades del país objetivo, sobre todo cuando se combinan con otras acciones cinéticas como los asesinatos (Bellingcat Investigation Team, 2021).

La identificación de estas acciones previas en tiempo de paz resulta clave para contrarrestar esta amenaza y constituye una de las tareas claves de la CI. El actual conflicto de Ucrania está ofreciendo valiosas lecciones a este respecto.

Otra de las lecciones identificadas en el conflicto en Europa del este es el recurso a estas acciones para dañar el poder aéreo del adversario dónde y cuándo este es más vulnerable, esto es, en tierra. Además de los daños materiales, los efectos en la moral de una fuerza aérea o la opinión pública pueden llegar a ser muy importantes.

Capítulo aparte merecen las acciones en el ciberespacio o cibersabotajes. Actualmente, sus efectos se notan de forma continua y, en caso de conflicto, pueden llegar a ser decisivos. Es importante tener en cuenta que, aunque sea el ciberespacio el medio o el objetivo, detrás de esas acciones siempre se encuentran personas u organizaciones, generalmente SIH o actores *proxy*, trabajando para ellos o en coalición con ellos.

3.4 Terrorismo: acciones cinéticas en los conflictos híbridos

El terrorismo es la amenaza no convencional más importante de los llamados conflictos híbridos. En muchos casos se considera como el «arma de los pobres» porque se necesita muy poco para causar un daño importante, tanto en los ámbitos físicos como en el cognitivo.

Durante una operación fuera de área, los medios y las instalaciones del EA, por ejemplo una DOB[4], suponen un objetivo prioritario por su elevado valor y por su vulnerabilidad en cuanto a su defensa terrestre.

Conocer las capacidades de las redes terroristas, sus TTP[5] y sus intenciones, objetivo principal del análisis de contrainteligencia, resulta vital para contrarrestar esta amenaza.

Pero incluso en tiempo de paz, el terrorismo supone una grave amenaza, especialmente cuando intervienen agentes internos o cercanos a la organización.

El acto terrorista es muy difícil de detener cuando se ha iniciado su ejecución y sus consecuencias suelen ser irreparables. Dado que supone la culminación del proceso de subversión, en forma de radicalización o adoctrinamiento, la forma más eficaz de evitarlo es el establecimiento de un plan para la detección de indicadores de amenaza en el personal propio, proceso que consume muchos recursos. Además, se debe tener en cuenta que, en los últimos años, se ha constatado una aceleración en estos procesos de radicalización que en casos recientes han llegado a durar solo algunas semanas (Vera et *al.*, 2023).

Un ejemplo de lo anteriormente expuesto es el atentado perpetrado el 6 de diciembre de 2019 por un teniente de la Fuerza Aérea de Arabia Saudí, en la base naval de Pensacola (EE. UU), donde se encontraba realizando un curso de vuelo y en el que murieron tres militares americanos. La investigación posterior determinó que el asesino tenía ideas islamistas radicales y un claro sentimiento antiamericano, según mostraban sus redes sociales. Cuando, posteriormente al ataque, se investigó a sus veintiún compañeros saudíes de curso, se observó que diecisiete de ellos mostraban el mismo nivel de radicalismo. Incluso, se detectaron otros indicadores de alerta como que quince de ellos habían estado en contacto recientemente con pornografía infantil (Federal Bureau of Investigation, 2000).

Lamentablemente, estas investigaciones llegaron demasiado tarde. Y no existe ningún elemento de juicio que indique que este tipo de acciones no puedan repetirse en bases del EA donde, por ejemplo, también se han adiestrado pilotos de Arabia Saudí.

---

[4] *Deployable Operating Base*.
[5] Tácticas, técnicas y procedimientos.

Además de lo anterior, la capacidad de CI del EA debe estar preparada para analizar la estructura, capacidades, intenciones y TTP de las redes terroristas presentes en las zonas de operaciones (ZO) donde pueda llegar a desplegarse un DAT[6] o una DOB, ya que estas instalaciones son objetivo prioritario de estas organizaciones por su importancia operativa y por el enorme impacto mediático que generan. Contrarrestar este tipo de ataques resulta muy difícil, como lo demuestra el ataque sufrido por una base aérea en el centro de Pakistán en noviembre de 2023, en el que murieron nueve miembros de la Fuerza Aérea y tres aviones y un depósito de combustible fueron dañados (Gul, 2023). La CI resulta, por lo tanto, fundamental para contrarrestar la amenaza terrorista.

3.5 *Crimen organizado: la externalización de los SIH*

El fenómeno criminal es connatural a las sociedades humanas. Pero, en los últimos tiempos, las redes criminales se han internacionalizado y aumentado sus capacidades y ámbito de actuación, debido a la globalización y las nuevas tecnologías. Este hecho está siendo aprovechado por ciertas potencias para externalizar las actividades de sus servicios secretos con el objetivo de realizar actividades de manera encubierta, difíciles de atribuir y sin emplear recursos propios.

Esta externalización de las amenazas no convencionales es una característica fundamental de los conflictos modernos que se mueven en una zona gris donde la respuesta militar tiene difícil encaje. Esto supone un reto importante para la contrainteligencia militar cuya capacidad de actuación fuera del ámbito castrense está muy limitada.

Los SIH se valen de redes criminales para llevar a cabo acciones relacionadas con todo el ámbito de las amenazas TESS, desde los secuestros y asesinatos hasta las acciones de sabotaje y la agitación social, pasando por el espionaje.

Este último caso es especialmente trascendente debido a las capacidades de los grupos delictivos, bien asentados en un entorno concreto, de llegar a amplios sectores de la población y, por lo tanto, también del EA, a través de la red oscura o profunda, pero también la visible, o las redes sociales y sistemas de mensajería. Es conocido, por ejemplo, el incremento del tráfico de drogas por esta vía (Naciones Unidas, s. f.).

Las organizaciones de crimen organizado obtienen beneficios adicionales poniendo a disposición de los SIH estos sistemas para el reclutamiento de personas, generalmente con alguna necesidad económica o escasa moralidad, para la realización de encargos concretos y puntuales como la

[6] Destacamento Aerotáctico.

obtención de información sensible. Un número indeterminado de personas con acceso a esta información en el EA pueden ser susceptibles de responder a estos anuncios de dinero fácil. Detectar estas acciones resulta, una vez más, extremadamente difícil y pasa por una robusta capacidad de CI que permita identificar vulnerabilidades en el personal del EA y aquel contratado que trabaje en las bases y cuarteles del país.

Mención aparte merece el uso de ciberdelincuentes para la realización de acciones de sabotaje, espionaje y subversión en el ciberespacio. Actualmente, existen numerosas organizaciones criminales, patrocinadas o dirigidas por ciertos estados, que dispones de enormes capacidades y atacan, de manera casi continua, infraestructuras en España. Cabe esperar que en una situación más cercana al conflicto armado, estas capacidades sean dirigidas con más frecuencia e intensidad contra el EA. No se debe olvidar que, aunque se trata de una amenaza que utiliza, principalmente, la tecnología como medio u objetivo, detrás se encuentran siempre personas o grupos de personas cuya identificación y análisis es responsabilidad de la CI.

Por último, la utilización de grupos paramilitares o de mercenarios como fuerzas civiles subrogadas para las actividades militares de ciertos gobiernos genera dudas en cuanto a la forma de enfrentarlas, lo que limita la capacidad de respuesta de las Fuerzas Armadas. En este contexto, conocer sus capacidades, métodos de acción e intenciones se convierte en algo muy importante y, a la vez, complejo de conseguir.

3.6 La amenaza interna: indicadores de compromiso

Como se ha comentado en los puntos anteriores, con mucha frecuencia, los SIH y las organizaciones involucradas en actividades TESSCO recurren al personal interno de la organización objetivo, los llamados *insiders* para la realización de sus ataques. Esta razón, añadida a la naturaleza clandestina de las acciones de los SIH, provoca que estas actividades resulten muy difíciles de detectar y merezcan un estudio exhaustivo y particularizado.

Estos *insiders*, que puede apoyar a actores hostiles sin ni siquiera saberlo, pueden llegar a causar un enorme daño debido a que tienen acceso legítimo a recursos críticos, conocen las vulnerabilidades y tienen una significativa capacidad de pasar desapercibidos. Por todo ello, su identificación resulta difícil y requiere de recursos desplegados en toda la organización.

Pero estos recursos, que siempre serán escasos, no pueden alcanzar a todo el personal ni todos los rincones de las bases aéreas. Por ello, la respuesta más eficaz pasa por una intensa labor de concienciación del personal del EA, civil y militar, que permita, primero, elevar su nivel de alerta para evitar ser víctimas de las «trampas» tendidas por actores hostiles y,

segundo, actuar como sensores sobre la presencia de indicadores de compromiso en el personal con el que puedan tener contacto.

Sin embargo, existen ciertos indicadores, visibles solo para el personal del entorno de la persona posiblemente involucrada en este tipo de actividades, que deben generar una alerta y provocar la acción del personal de CI. De esta manera, la seguridad del EA se convierte en una tarea de todos («todo aviador es un sensor»).

A modo de ejemplo y de manera esquemática, se presentan, a continuación, algunos de estos indicadores:

- Personas relacionadas con países de interés para la CI.
- Notable interés por la cultura de estos países.
- Viajes a alguno de estos países, incluidos los que no requieren comunicación o autorización.
- Posturas ideológicas o religiosas extremas o relación con personas u organizaciones que defiendan estos postulados.
- Interés por conocer información clasificada sin relación con sus puestos de trabajo, bien por calidad o por cantidad.
- Manejo de información clasificada fuera de los lugares o sistemas autorizados, especialmente en el domicilio particular.
- Trabajo con información clasificada fuera del horario habitual sin justificación.
- Uso indebido de los sistemas informáticos.
- Negligencias reiteradas en su labor profesional.
- Comisión de faltas o delitos.
- Situaciones personales que supongan un riesgo o una vulnerabilidad explotable por los SIH u otras amenazas TESSCO: problemas económicos importantes, consumo o abuso de sustancias u otras dependencias, problemas sicológicos graves, etc.

La vigilancia sobre estas situaciones se debe extremar en el caso de personal eventual o contratado por empresas externas. Para estos casos resulta muy importante la realización de procesos de *vetting* por parte del personal de seguridad o CI, especialmente cuando este personal va a tener acceso a información, personas, lugares o medios de interés para los SIH o las organizaciones involucradas en actividades TESSCO.

4 Particularización de las amenazas no convencionales al ámbito aeroespacial

La forma de operar del EA presenta diferencias con respecto a las de otros ámbitos. Estas características influyen, a su vez, en cómo le afectan las amenazas de los SIH y las organizaciones o individuos involucrados

en acciones TESSCO y, por lo tanto, en las capacidades de CI que deben implementarse para identificarlas y neutralizarlas.

Se exponen, a continuación, de forma breve, algunas de estas características particulares.

4.1 Dependencia de la tecnología

Todos los elementos de las sociedades modernas dependen extraordinariamente de la tecnología y su adaptación a los rápidos cambios que esta sufre de manera continua supone un reto constante. Las Fuerzas Armadas no son ajenas a esta situación. Pero, en el caso del EA, esta dependencia es mucho más marcada por así exigirlo el operar, casi exclusivamente, en un medio tan ajeno al ser humano como es el aire y el espacio y por sus características de velocidad, alcance y penetración en territorio enemigo. De esta circunstancia se derivan dos tipos de vulnerabilidades muy diferentes.

Por un lado, un ataque puntual y de duración limitada que niegue el acceso de una unidad del EA (un avión o paquete de aviones realizando una misión) a un tipo de tecnología, como puede ser la comunicación vía radio o la geolocalización, puede dar al traste con toda la operación e, incluso, tener consecuencias irreparables. Un avión en vuelo no puede parar y esperar a que se solucione el problema. En tierra, los sistemas aéreos necesitan de complejas y delicadas acciones de preparación y mantenimiento a realizar por personal muy cualificado. En esta situación, estos sistemas no disponen de medios de autoprotección incorporados, por lo que dependen de medidas externas de defensa activa y pasiva. Además, la operación de estos sistemas recae también en personal cuya cualificación lleva muchos años y, por lo tanto, es muy escaso y difícil de sustituir.

Por otro lado, esta visión de las operaciones tan centrada en la tecnología puede dificultar entender lo frágil que esta resulta y lo sencillo que puede llegar a ser negar su acceso con acciones mucho más mundanas. Contrarrestar la capacidad del poder aéreo de alcanzar sus objetivos con sofisticados y caros sistema A2/AD, por ejemplo, puede resultar muy complejo y solo está al alcance de unas pocas potencias, pero realizar acciones de tipo TESSCO que neutralicen o degraden, al menos temporalmente, las capacidades del EA durante una operación está a disposición de la totalidad de los actores potencialmente hostiles. Ejemplos de estos ataques pueden ser las acciones de sabotaje (cibernético o convencional) con participación o no de *insiders*, los ataques terroristas sobre personal clave (secuestros o asesinados) o acciones sobre la moral o lealtad de estos.

De lo anterior se deduce que, debido a su dependencia tecnológica, los medios del EA son especialmente vulnerables a las amenazas TESSCO, algo que, en ocasiones, resulta difícil de percibir y valorar.

4.2 Dependencia de bases

Otra característica fundamental del poder aeroespacial es su dependencia de bases para operar. Estas bases son lugares muy concretos en los que se acumulan todos los medios que requieren las aeronaves para su funcionamiento, algunos de ellos muy tecnológicos como se trató en el punto anterior, y otros muy vulnerables, como por ejemplo los aviones o los depósitos de combustible. Además, en las bases se encuentra un elemento esencial para la operación de las aeronaves, la pista de despegue y aterrizaje, cuya longitud obliga a que estas instalaciones sean de una extensión considerable.

Esta concentración de medios hace que el establecimiento de una base aérea sea algo muy complejo y costoso por lo que se tiende a disponer de un número limitado de ellas. Además, su defensa resulta difícil por las características ya mencionadas: su extensión, sus componentes sensibles y vulnerables y el hecho de que las aeronaves no disponen, en el suelo, de medios de autoprotección activa o pasiva.

Por lo tanto, queda claro que una manera de degradar o neutralizar el poder aéreo es atacar sus bases. Esto se puede llevar a cabo mediante operaciones convencionales, generalmente realizadas con sistemas de misiles de largo o muy largo alcance o mediante el poder aéreo del adversario (operaciones OCA[7]). Para contrarrestar estas amenazas se deben establecer sofisticados sistemas de defensa, que siempre resultan insuficientes dada la larga lista de elementos a proteger en la zona de operaciones. Esto genera una competencia en complejas capacidades ofensivas y defensivas entre los adversarios.

Existe otra manera de dañar las bases aéreas y es mediante acciones no convencionales. Estas serán más difíciles de llevar a cabo si la base se encuentra en territorio nacional pero mucho más sencillas si se encuentra desplegada en el marco de una operación fuera de área, en un país no aliado que pueda presentar carencias en cuanto a su estabilidad social o seguridad interna. Una concentración de civiles que rodee una base aérea e impida la entrada y salida de personal y suministros puede ser suficiente para dejar la instalación inoperativa (AFP, 2023). Lo mismo es válido para el caso de despliegues en la proximidad del frente en un conflicto entre potencias similares.

De nuevo, se concluye que, debido a su dependencia de bases, el poder aéreo es especialmente vulnerable a las acciones TESSCO.

4.3 Geometría del despliegue de los medios aéreos

Los medios aéreos se despliegan en bases o aeródromos. A la hora de determinar su ubicación y para asegurar la protección de estas instalaciones,

[7] *Offensive Counter-Air.*

en línea con lo establecido en los puntos anteriores, el primer factor que se contempla es la distancia a la línea de las fuerzas enemigas o al área donde deberán operar las aeronaves.

Como norma general, cuanto mayor es la distancia con las fuerzas hostiles, menor es el grado de amenaza, siendo la situación ideal el operar desde territorio nacional. Una mayor distancia supone el inconveniente de un menor alcance o tiempo en zona, además de la necesidad de medios adicionales de apoyo como los de reabastecimiento en vuelo. En ocasiones, por las características de los medios aéreos o por necesidades operativas, las bases de despliegue deberán localizarse relativamente cerca de la zona de conflicto.

Otro factor a tener en cuenta es que la construcción desde cero de una base o aeródromo eventual es extremadamente difícil por lo que, en la práctica totalidad de casos, se dependerá de bases ya existentes aunque estas puedan necesitar arreglos o actualizaciones.

En resumen, el lugar de despliegue de una unidad del EA se elegirá de entre aquellas instalaciones ya existentes que cuenten con los mínimos medios adecuados para el despliegue del tipo de aeronave necesario y teniendo en cuenta que se encuentre en una zona con un nivel de riesgo aceptable, dados ciertos condicionantes operativos.

Para la gestión de este riesgo se deberán asignar las medidas de protección proporcionales a las capacidades ofensivas del adversario.

Este es un punto crítico, ya que las capacidades de un actor hostil convencional para alcanzar una base aérea dependen, como ya se ha comentado, de complejos sistemas de largo alcance, elevada precisión y capacidad de supervivencia, y estos resultan difíciles de esconder. Por lo tanto, obtener inteligencia relativa a la existencia de este tipo de amenazas convencionales, al menos hasta cierto punto, no resulta del todo difícil. De esta cuestión se encarga la inteligencia aeroespacial convencional.

Cuestión muy diferente es identificar y valorar las amenazas no convencionales, que utilizan medios poco sofisticados, al alcance de una generalidad de individuos, grupos o fuerzas irregulares, mezclados en la mayoría de los casos con la población civil local, amparados muchas veces por servicios de inteligencia de terceros países y cuya naturaleza implica, como primera premisa, pasar desapercibidos. Existen numerosos ejemplos en la historia reciente de los conflictos, especialmente en operaciones de estabilización y contrainsurgencia (COIN), de ataques a bases aéreas en los que un adversario ha logrado infligir un daño significativo con recursos muy precarios (Vick, 1995).

A todo lo anterior hay que añadir otro factor que contribuye a que este tipo de amenazas no convencionales puedan pasar desapercibidas hasta

que se ponen de manifiesto. Se trata de que, al encontrarse las bases aéreas ubicadas en zonas relativamente alejadas de la linea de contacto, el personal percibe el nivel de riesgo como inferior al del resto de fuerzas. Esta sensación de falsa seguridad contribuye a una relajación del nivel de alerta y autoprotección del personal, situación que facilita la realización de actividades de tipo TESSCO.

Con toda probabilidad, esta situación se agravará en un futuro próximo debido al acceso generalizado a tecnologías que facilitan las acciones no convencionales, siendo el ejemplo más de actualidad el incremento en el uso de UAS adaptados de sistemas comerciales de bajo coste.

De todo lo anterior se concluye la importancia del conocimiento de la situación en lo relativo a las amenazas, tanto convencionales como no convencionales, que se ciernen sobre las instalaciones y el personal del EA en operaciones.

En cuanto a las amenazas no convencionales, este conocimiento solo se puede adquirir con una intensa interacción con el entorno humano de la zona de influencia donde se ubica la unidad o destacamento aéreo. Conocer las dinámicas sociales de la población local para identificar organizaciones hostiles, la estructura de sus redes, sus capacidades, medios de apoyo y TTP resulta vital para poder influir en ellas y tener una cierta capacidad de alerta temprana, así como poder planear una adecuada defensa.

Por lo tanto, se puede decir que pensar que la ubicación de una base o aeródromo «en retaguardia», por este solo hecho, le dota de una condición de seguridad suficiente, solo alterable cuando el adversario posea sistemas avanzados de largo alcance, puede ser un error que resulte fatal. Las amenazas TESSCO están presentes en cualquier escenario aunque en unos de forma más severa que en otros.

La defensa y protección de un base o aeródromo militar debe ser planeada y dotada en base a un riguroso juicio de inteligencia, para lo que se requieren de capacidades de contrainteligencia suficientes para llevar a cabo las acciones de obtención y análisis sobre este tipo de amenazas no convencionales.

4.4 Objetivos lucrativos

Como colofón a este punto sobre las particularidades del poder aeroespacia,l en relación con las amenazas no convencionales, merece la pena incidir en que las bases y aeródromos donde se despliega el personal y los medios del EA son un objetivo de máxima prioridad para las fuerzas hostiles, debido a su importancia estratégica y operacional. Se trata de capacidades muy concretas y escasas, pero con una enorme capacidad

de influencia en el desarrollo de un conflicto, a lo que hay que añadir el impacto mediático que tiene todo lo relacionado con ellas.

Por lo tanto, cabe esperar que un adversario hará todo lo posible por negar o degradar estas capacidades o limitar su libertad de acción por cualquier medio a su alcance. Si dispone de armas convencionales en calidad y cantidad suficiente y con capacidad de empleo superior, las utilizará. Si no, recurrirá a medios no convencionales que, en muchas ocasiones, presentan ventajas superiores a los anteriores. O, como se ha puesto de manifiesto en el conflicto de Ucrania, utilizará una mezcla de ambos.

En conclusión, el EA es objetivo prioritario de los SIH y de las organizaciones involucradas en actividades TESSCO y esta amenaza se hace más importante cuanto más se acerca la posibilidad de un conflicto armado.

5 Amenazas a la libertad de acción del poder aeroespacial en conflictos actuales: lecciones identificadas en la actual guerra de Ucrania

El 24 de febrero de 2022, el primer día de la invasión de Ucrania, las fuerzas militares de la Federación Rusa intentaron la toma del aeropuerto de la empresa Antonov, en la localidad de Hostomel, en las proximidades de Kiev. El objetivo era utilizar este aeródromo para el despliegue de fuerzas que permitieran la toma de la capital y propiciar la caída de su Gobierno, lo que supondría la culminación de la «operación militar especial» preparada por el ejecutivo de Putin y la consecución de sus objetivos en unos pocos días, todo ello sin tener que involucrarse en un largo y costoso conflicto armado. La acción resultó infructuosa, lo que originó a su vez, un cambio radical en el devenir del conflicto (Collins *et al.*, 2023).

A juicio de la mayoría de analistas, el factor determinante en el resultado de esta crucial operación fueron las operaciones de información de ambos contendientes.

Por el lado ruso, se dieron dos circunstancias que influyeron de manera determinante en el resultado de la operación. Primero, los elementos del FSB[8] desplegados en la zona, a pesar de su significativa entidad y de contar con el apoyo de una amplia red de colaboradores establecida con anterioridad, no consiguieron su objetivo de proporcionar información táctica relevante y oportuna sobre capacidades, despliegue y moral de las fuerzas ucranianas en la zona (Miller y Belton, 2022). Segundo, el planeamiento y preparación de la operación se vio limitado por el escaso conocimiento que las fuerzas participantes tenían de ella, motivado por la necesidad

[8] FSB son las siglas en inglés del Servicio Federal de Seguridad de la Federación de Rusia, encargado de inteligencia, contrainteligencia y seguridad interior. Forma, junto con el SVR (encargado de la inteligencia exterior) y el GRU (el servicio de inteligencia militar) el núcleo de los servicios de espionaje y contraespionaje de Rusia.

de mantener la información inaccesible a los servicios de inteligencia de Ucrania y de otras naciones aliadas de esta (Watling et *al*., 2023).

Del lado ucraniano, el principal factor que influyó en el resultado, fue la capacidad de sus servicios de contrainteligencia de identificar a ciertos elementos del FSB, limitando así su capacidad de movimiento y posibilitando la interrupción de sus operaciones.

Por otro lado, los esfuerzos de Rusia de mantener sus planes operativos en secreto resultaron infructuosos debido a que parte de estos fueron obtenidos por los servicios de inteligencia de Estados Unidos y Reino Unido y puestos a disposición de los ucranianos (Watling et *al*., 2023), lo que demuestra carencias en la capacidad de contrainteligencia militar de las Fuerzas Armadas rusas.

Todo lo anterior pone de manifiesto la relevancia de las operaciones de espionaje y contraespionaje para el devenir de los conflictos actuales, especialmente en lo relativo a las operaciones en el ámbito aeroespacial.

Pero no es este el único ejemplo acerca de la importancia del juego de inteligencia y contrainteligencia en este conflicto. Se ofrecen, a continuación, de manera muy breve, algunas notas a este respecto.

5.1 *La subversión como eje central de las operaciones*

Resulta patente que la primera opción del gobierno de Rusia no era el verse involucrado en un largo conflicto armado contra Ucrania y sus aliados internacionales. Al contrario, todo apunta a que su plan consistía en utilizar sus fuerzas armadas en una acción limitada como forma de presión que diera el golpe de definitivo que propiciara la instauración de una forma de gobierno en Ucrania propicia a sus intereses.

Pero, ¿cuál era entonces el eje central de la estrategia de Putin para conseguir este objetivo? La respuesta es la subversión, en forma de acciones sobre elementos clave de los diferentes poderes de la sociedad ucraniana que debían preparar el terreno antes del golpe de gracia.

Este tipo de actividades son planeadas, coordinadas y ejecutadas principalmente por los servicios de inteligencia de Rusia, los cuales tienen amplios recursos y experiencia. Resulta obvio, sin embargo, que el plan no dio suficientes resultados como para ser definitivo, probablemente porque la decisión de comenzar las operaciones convencionales se tomó antes de que este plan hubiera alcanzado sus objetivos.

En el ámbito específico militar se realizaron múltiples acciones de este tipo, siendo las más destacas la captación como agentes de personas en puestos de dirección dentro de las fuerzas armadas ucranianas o las acciones directas sobre la práctica totalidad de sus mandos con empleo de

coronel y general mediante llamadas telefónicas horas antes de la invasión, solicitándoles su rendición o un cambio de lealtades (Watling et *al*., 2023).

5.2 *El valor de la disciplina HUMINT para la obtención de inteligencia táctica*

En el conflicto de Ucrania se ha puesto de manifiesto la importancia de la obtención de inteligencia de fuentes humanas (HUMINT). En un contexto donde la tecnología tiene cada día un peso más determinante, las forma de obtención más tradicional, basada en el entorno humano, sigue teniendo una transcendencia capital.

Las fuerzas rusas han realizado un enorme esfuerzo para el establecimiento de una red de colaboradores dentro del territorio enemigo, algo iniciado mucho tiempo antes del comienzo de las operaciones estrictamente militares. Una vez iniciadas estas, unidades de operaciones especiales, encuadradas en sus servicios de inteligencia o dirigidas por estas, han aumentado sus capacidades de obtención de inteligencia.

Resulta muy destacable la prolija utilización de estos elementos para operaciones de *targeting*, incluido la fase de *battle damage assessment* (BDA), como demuestra la implantación de un centro de coordinación de *targeting* dirigido por el GRU (Watling et *al*., 2023).

Algo parecido ha sido llevado a cabo por las fuerzas ucranianas en los territorios ocupados por Rusia, mediante el establecimiento de redes de resistencia, lo que ha llevado a las fuerzas ocupantes al establecimiento de una nutrida capacidad de contrainteligencia para detectarlas y neutralizarlas, en muchas ocasiones mediante procedimientos brutales claramente contrarios al derecho internacional.

Por último, en relación con los procedimientos de los servicios de inteligencia de Rusia para el reclutamiento de fuentes y agentes dentro de las fuerzas armadas de Ucrania, se ha podido comprobar como estos servicios se esfuerzan, no en el reclutamiento de una amplia red de agentes, si no en unos pocos individuos seleccionados de entre los oficiales de elevada graduación, especialmente los relacionados con la inteligencia. Cada uno de estos agentes se encarga, a su vez, del reclutamiento de la red que trabajaría para él. De esta manera, estos agentes de segundo nivel y sucesivos desconocen que, aun siendo leales a su jefe, trabajan en realidad para una potencia extranjera (Watling et *al*., 2023).

Esto supone una dificultad más a la hora de identificar estas amenazas debido, por un lado, a que a los oficiales de alta graduación se les suele suponer unos mayores estándares de fiabilidad y, por otro, a que el personal en contacto con sus operadores (de los SIH) son muy pocos por lo que es más sencillo mantener la operación oculta.

5.3 El recurso al sabotaje

El enorme despliegue de elementos de los servicios de inteligencia de Rusia no solo ha tenido como finalidad la subversión de las fuerzas ucranianas o la obtención de información, también se ha encargado de la realización de numerosas acciones de sabotaje, especialmente contra infraestructuras críticas, algo que no sorprende si se tienen en cuenta otros conflictos recientes en los que ha participado Rusia y el hecho de que este tipo de acciones es totalmente coherente con su doctrina militar.

Resulta más destacable aún el recurso a este tipo de acciones por parte de los servicios de inteligencia de Ucrania. Ante la falta de capacidades para alcanzar objetivos de alto valor en profundidad del territorio ruso, elementos de estos servicios han llevado a cabo múltiples acciones decisivas, como la intrusión en la base aérea de Chkalovsky, a 25 km al noreste de Moscú, en el que se atacaron objetivos de alto valor como un avión de ISR Il-20M Coot-A, además de un avión de transporte An-148 y un helicóptero de ataque Mi-28N (Court, 2023). O la acción, supuestamente realizada por un único saboteador, que destruyó un bombardero Su-34 Fullback en la base de Chelyabinsk, situada al norte de Kazakhstan, a 900 km de la frontera ucraniana (Axe, 2024).

Sistemas aéreos como el Coot-A, considerado un HVAA[9], o el Su-34, son muy difíciles de alcanzar mientras realizan sus operaciones aéreas. Sin embargo, en estos ejemplos fueron inutilizados con poco más que una lata de gasolina, un mechero y una acción bien planeada y ejecutada.

5.4 Fuerzas irregulares: las PMC de Rusia

Uno de los aspectos de este conflicto que más páginas de periódicos y horas de televisión han llenado ha sido el recurso de Rusia a fuerzas irregulares o *Private Military Companies* (PMC) como Wagner.

A pesar de la reconocida rigidez y falta de capacidad de adaptación de las fuerzas regulares de la Federación Rusa en este conflicto, en el uso de capacidades no convencionales, Rusia ha demostrado una gran iniciativa. Aunque las fuerzas de Wagner saltaron a los medios principalmente por su rol en la batalla de Bajmut, su aportación a la consecución de los objetivos militares de Rusia va mucho más allá de proporcionar tropas de asalto.

Este grupo se originó en el conflicto del Donbás, en 2014, como un batallón de mercenarios contratados por el GRU. Su conexión con este servicio

[9] HVAA son las iniciales en inglés de aeronave de alto valor. Este término, en la doctrina OTAN, se otorga a los sistemas cuya pérdida supone una muy significativa ventaja para el enemigo por su impacto operativo o mediático.

ha sido muy estrecha desde entonces y muchos de sus dirigentes proceden de los servicios de inteligencia de Rusia (Watling et *al*., 2023).

Los grupos como Wagner, o su probable sucesor Redut, realizan todo tipo de actividades encubiertas al servicio del Ministerio de Defensa de Rusia, bajo la dirección de sus servicios de inteligencia y en múltiples escenarios, desde África a Oriente Próximo. En Ucrania, ya desde la guerra del Donbás, los mercenarios de Wagner han realizado acciones de obtención de inteligencia (HUMINT), de sabotaje o apoyo al *targeting*. En ocasiones, proporcionan capacidades muy especializadas como pilotos de drones, especialistas en sistemas antiaéreos o tiradores de élite (Kats et *al*., 2020).

Funcionan como auténticos grupos de crimen organizado, contratando especialistas de entre antiguos militares o personal civil sin experiencia operativa, de acuerdo con las necesidades puntuales o más amplias que no pueden ser cubiertas por las fuerzas regulares, en muchos casos por quedar fuera de cualquier principio de legalidad.

Este tipo de fuerzas irregulares tienen una significativa importancia en los conflictos híbridos actuales lo que debe tenerse en cuenta a la hora de definir las capacidades y, sobre todo, la doctrina militar para contrarrestar la amenaza que suponen, especialmente teniendo en cuenta su naturaleza no militar y su frecuente utilización en operaciones encubiertas de tipo TESSCO.

6 Conclusión

Se ofrecen, a continuación, unas breves conclusiones de lo expuesto en los puntos anteriores en relación con la importancia de la contrainteligencia para la identificación y neutralización de las amenazas a la libertad de acción del EA en el contexto de seguridad global actual.

- El entorno de seguridad global actual, así como los nuevos conflictos en los que es posible que participe el EA, se caracterizan por una mayor preponderancia de amenazas de tipo no convencional.
- Estas amenazas no convencionales comparten ciertas propiedades:
  - Utilizan medios no militares para alcanzar objetivos militares o emplean una mezcla de ambos en una estrategia de guerra híbrida.
  - Permanecen ocultas o camufladas como actividades legítimas.
  - Para alcanzar sus fines recurren, en muchos casos, a actores internos a las organizaciones objetivo.
  - Sus efectos, aunque muy dañinos, pueden no ser evidentes de forma inmediata o incluso pasar completamente desapercibidos por mucho tiempo o hasta que el agresor decida explotarlos de la manera que considere oportuna.
  - En muchos casos, persiguen la no atribución como forma de influir en la opinión pública y en las diferentes estructuras del Estado,

incluidas las Fuerzas Armadas, con el objetivo de mantener el conflicto en una zona gris que dificulte la implementación de acciones de respuesta.

- Todo lo anterior hace que estas amenazas sean muy difíciles de identificar y, por lo tanto, neutralizar.
- Los actores hostiles a los que el EA podría enfrentarse en el futuro poseen muy significativas y variadas capacidades en el ámbito de las amenazas no convencionales. El actual conflicto de Ucrania ofrece múltiples ejemplos de su utilización y aunque en algunos casos los posibles actores hostiles hayan cometido errores es probable que, en próximas ocasiones, estos no vuelvan a suceder.
- Enfrentarse a este tipo de amenazas en tiempo de paz o prepararse para hacerlo durante un conflicto, obliga al desarrollo de iguales o superiores capacidades que los adversarios, especialmente en contextos de amenaza no compartida.
- La contrainteligencia es la especialidad de la inteligencia encargada de la identificación, análisis y neutralización de las amenazas de tipo no convencional, especialmente las que proceden de SIH.
- El EA debe desarrollar una eficaz capacidad de contrainteligencia militar específica de acuerdo con sus misiones e idiosincrasia propia y proporcional a su nivel de ambición, al igual, si no mejor, que los hacen otras fuerzas aéreas de países del entorno y siempre de acuerdo con la doctrina nacional y aliada, de modo que se asegure la acción conjunta-combinada.

Bibliografía

AFP. (2023). Thousands of coup supporters gather near French military base in Niger. *Alarabiya News*. [Consulta: 2024]. Disponible en: https://english.alarabiya.net/News/north-africa/2023/08/11/Thousands-of-coup-supporters-gathered-near-French-base-in-Niger

Axe, D. (2024). A Ukrainian saboteur traveled 900 miles to a snowy Russian airfield and, in the dead of night, lit a Russian Sukhoi fighter-bomber on fire. *Forbes*. [Consulta: 2024]. Disponible en: https://www.forbes.com/sites/davidaxe/2024/01/04/a-ukrainian-saboteur-traveled-600-miles-to-a-snowy-russian-airfield-and-in-the-dead-of-night-lit-a-russian-sukhoi-fighter-bomber-on-fire/

Bellingcat Investigation Team. (2021). How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine. *Bellingcat*. [Consulta: 2024]. Disponible en: https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/

Collins, L. et al. (2023). The Battle of Hostomel Airport: A Key Moment in Russia's Defeat in Kyiv. *War on the Rocks. Texas National Security Review*. [Consulta: 2024]. Disponible en: https://warontherocks.com/2023/08/the-battle-of-hostomel-airport-a-key-moment-in-russias-defeat-in-kyiv/

Court, E. (2023). Military intelligence: Russian airbase hit by sabotage attack. *The Kyiv Independent*. [Consulta: 2024]. Disponible en: https://kyivindependent.com/military-intelligence-russian-airbase-hit-by-sabotage-attack/

Federal Bureau of Investigation. (s. f). *Ana Montes: Cuban Spy*. [Consulta: 2024]. Disponible en: https://www.fbi.gov/history/famous-cases/ana-montes-cuba-spy

—. (2020). Shooting at Naval Air Station Pensacola Called "Act of Terrorism". [Consulta: 2024]. Disponible en: https://www.fbi.gov/news/stories/naval-air-station-pensacola-shooting-called-act-of-terrorism-011320

Galeotti, M. (2019). *Active Measures: Russia's Covert Geopolitical Operations*. The George C. Marshall European Center for Security Studies. [Consulta: 2024]. Disponible en: https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0#toc-russia-strategic-initiative-rsi-

Gul, A. (2023). Militants Raid Pakistani Air Force Base After Killing 17 Soldiers Elsewhere. *Voice of America*. [Consulta: 2024]. Disponible en: https://www.voanews.com/a/militants-raid-pakistani-air-force-base-after-killing-17-soldiers-elsewhere-/7341438.html

Haines, J. R. (2016). How, Why, and When Russia Will Deploy Little Green Men – and Why the US Cannot. *Foreign Policy Research Institute*. [Consulta: 31 de enero de 2024]. Disponible en: https://www.fpri.org/article/2016/03/how-why-and-when-russia-will-deploy-little-green-men-and-why-the-us-cannot/

Kats, B. et al. (2020). *Moscow's mercenary wars*. Center for Strategic and International Studies (CSIS). [Consulta: 2024]. Disponible en: https://russianpmcs.csis.org/

Miller, G. y Belton, C. (2022). Russia's spies misread Ukraine and misled Kremlin as war loomed. *The Washington Post*. [Consulta: 2024]. Disponible en: https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/

Naciones Unidas. (s. f.). *Kit de Herramientas de la ONU sobre Drogas Sintéticas. Las plataformas de venta* [en línea]. [Consulta: 2024].

Disponible en: https://syntheticdrugs.unodc.org/syntheticdrugs/es/cybercrime/onlinetrafficking/onlinesalesplatforms.html

Vera, J. et al. (2023). Así fue la radicalización exprés de Yassine, el lobo solitario con problemas mentales de Algeciras. *La vanguardia*. [Consulta: 2024]. Disponible en: https://www.lavanguardia.com/politica/20230128/8715903/radicalizacion-expres-yasin-lobo-solitario-algeciras.html

Vick, A. (1995). Snakes in the eagle's nest: a history of ground attacks on air bases. *Rand Corporation*. [Consulta: 2024]. Disponible en: https://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR553.pdf

Watling J. et al. (2023). Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022-February 2023. *Royal United Services Institute for Defence and Security Studies (RUSI)*. [Consulta: 2024]. Disponible en: https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022

Composición del grupo de trabajo

Presidente	**D. Juan Ramón Sabaté Aragonés** *General de Brigada del Ejército de Tierra.* *Jefe de estudios de la ESFAS-CESEDEN.*
Coordinador	**D. Carlos Alberto Ramírez Sánchez** *Coronel del Ejército de Tierra.* *Director del Departamento de Inteligencia ESFAS-CESEDEN.*
Vocales:	**D. Gonzalo García Escudero** *Capitán de fragata de la Armada.* *Doctor en Historia, Geografía e Historia del Arte.* *Departamento de Seguridad Nacional.*
	D. José María Gil Armario *Teniente coronel de la Guardia Civil.* *Departamento de Inteligencia ESFAS-CESEDEN.*
	D. Antonio Alberto González *Cuerpo Nacional de Policía.*
	D. Jose María Lorenzo Tenreiro *Comandante del Ejército de Tierra.* *División de Planes del EME (DIPLA).*
	D. Álvaro Cremades Guisado *Profesor asociado en el Departamento de Seguridad y Defensa de la Universidad Antonio de Nebrija.* *Máster en Analista de Inteligencia.*
	D. Francisco Marín Gutiérrez *Teniente coronel del Ejército de Tierra.* *EMAD, Mando Conjunto del Ciberespacio.*
	D. Iván Portillo Morales *Grado en Sistemas de Información (Universidad Alcalá de Henares), Especialista Universitario en Inteligencia (UNED - Instituto General Gutiérrez Mellado), Especialista Universitario en Seguridad Informática y de la Información (Universidad de Castilla-La Mancha).*
	D. David Cuesta Vallina *Coronel del Ejército de Tierra.* *Centro de Situación del ET (CESET).*

D. Juan Luis Chulilla Cano
Dr. en CC.PP. y Sociología, esp. Antropología, premio extraordinario UCM.

D. Fernando Touceda Rodríguez
Teniente coronel del Ejército del Aire y del Espacio.
Diplomado Superior en Inteligencia de las FF. AA.
Centro de Inteligencia de las Fuerzas Armadas – Sc. IMINT.

D. Antonio José Medina Fuentes
Teniente coronel del Ejército de Tierra.
Diplomado en Geodesia Militar.
Centro de Inteligencia de las Fuerzas Armadas – Sc. IMINT.

D. Arturo Rodríguez Torres
Comandante del Ejército del Aire y del Espacio.
Especialista en Cartografía e Imagen.
Centro de Inteligencia de las Fuerzas Armadas – Sc. IMINT

D. José Luis Delgado Gamella
Ingeniero de Telecomunicación (Universidad Politécnica de Madrid). Dipl.-Ing. Elektrotechnik und Informationstechnik (Technische Universität Darmstadt, Alemania).
Máster Universitario en Dirección de Empresas, MBA (IE).

D. Álvaro Alfaro Guillén
Máster Universitario en Ingeniería Industrial (Universidad Politécnica de Madrid).

D. Vicente de Ayala Parets
Ingeniero en Informática (Universidad Pontificia de Salamanca).

D. Juan Ignacio Fernández González
Comandante del Ejército de Tierra
Grupo de Observación por Sistemas Aéros (GROSA IV/1)
Regimiento de Inteligencia (RINT 1).

D. Jaime Mata Laencina
Teniente coronel del Ejército de Tierra.
Cuartel General de la Unidad Militar de Emergencias.

D. Alberto Díaz Martín
Teniente coronel del Ejército del Aire y del Espacio.
División de Operaciones del Estado Mayor del Ejército del Aire y del Espacio. Máster en Política de Defensa y Seguridad Internacional.
Máster en Análisis de Inteligencia y Ciberinteligencia.

Normas de envío de artículos

Tema del Cuaderno de Inteligencia número 3

El próximo número del Cuaderno de Inteligencia tendrá como tema principal la innovación como palanca de cambio en inteligencia. 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 **uno 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 de entre 9.000 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*.

PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL