Inteligencia: situación actual y desafíos futuros

Cdi 1

CUADERNOS DE INTELIGENCIA

MINISTERIO DE DEFENSA

Inteligencia: situación actual y desafíos futuros

Cdi 1

CUADERNOS DE INTELIGENCIA

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de Defensa
https://publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://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 083-23-140-2 (edición en línea)

NIPO 083-23-141-8 (impresión bajo demanda)
ISBN 978-84-9091-763-3 (impresión bajo demanda)

Depósito legal M 16897-2023
Fecha de edición: septiembre de 2023
Maqueta e imprime: Imprenta Ministerio de Defensa

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

Índice

Artículo noveno

Artículo décimo

Presentación

El pasado 24 de febrero de 2022, las Fuerzas Armadas de la Federación de Rusia invadieron a su vecina Ucrania, llevando nuevamente al corazón de Europa la guerra y la destrucción. El empleo de sistemas artilleros de largo alcance, masas acorazadas y bombardeos aéreos contra objetivos estratégicos nos sitúa ante un modelo de guerra convencional que teníamos ya olvidado tras décadas de analizar las luchas insurgentes, la protección contra grupos terroristas, el control de grandes áreas con amenazas ocultas que limitaban la libertad de movimientos.

Afganistán, Iraq, Somalia, Malí y otros escenarios en África subsahariana presentaban una situación operativa en la que conocíamos las intenciones de nuestros adversarios, sabíamos con bastante certeza cuáles eran sus objetivos y qué querían atacar. En cambio, se ocultaban, se mezclaban con la población local y no sabíamos dónde poder localizarlos y neutralizarlos para impedir que actuasen.

La guerra en Ucrania nos devuelve a los años de la Guerra Fría, cuando se sabía perfectamente dónde se situaban nuestros adversarios. En cambio, se desconocía por completo las intenciones del Kremlin y del Pacto de Varsovia; no sabíamos cuándo o dónde podrían querer atacarnos con esos potentes medios que estaban siempre localizados.

El trabajo de la inteligencia no ha variado, el ciclo de inteligencia ha seguido girando sin parar, generando miles de informes año tras año, ayudando a la toma de decisiones, invirtiendo en tecnología que apoye la acción del hombre como herramienta principal del sistema. El adecuado empleo de la función de combate inteligencia, de sus procedimientos, sus herramientas y el impulso de las tendencias que, al unir la experiencia, visión y empleo de los procedimientos de los viejos analistas con sistemas de inteligencia artificial, computación cuántica y fusión de información, permiten acortar los plazos de toma de decisiones o apoyar a las unidades de primera línea.

Pero la actualidad ucraniana nos ha obligado a modificar su enfoque. Se sabe con precisión dónde están los enemigos, pero se desconocen sus intenciones. Como ejemplo, sabemos dónde tiene hoy Rusia sus armas nucleares, pero no sabemos si las utilizará o no ni cuándo o sobre qué objetivos las lanzaría en su caso.

En este escenario, la exactitud de los datos aportados es una cuestión central, ya que de nada sirven las armas de precisión sin información de precisión, de la misma forma que esos datos deben ser accesibles, en tiempo oportuno, para evitar que nuestra acción llegue tarde.

La precisión y oportunidad de la información de la que dispongan los comandantes de las unidades empeñadas en combate, o los comandantes que tienen la responsabilidad de preparar las unidades de combate en tiempo de paz, son cruciales para el éxito de las operaciones o, incluso mejor, para una disuasión eficaz que ahorra dinero y vidas.

De nada sirven los más avanzados sistemas de observación y los más experimentados analistas si no se es capaz de integrar toda la información disponible, sin dilaciones, para ofrecer en un tiempo razonable la inteligencia que necesita el comandante.

Los comandantes de las organizaciones militares han de decidir en la oscuridad, arriesgar, ser líderes, en definitiva, empeñar su prestigio en la incertidumbre. Reducir esa incertidumbre es la clave del éxito y, para ello, el sistema de inteligencia es una herramienta crucial. El no ser consciente de esto en cada nivel, supone una grave responsabilidad que se suele pagar con sangre.

Para que este sistema de inteligencia sea eficaz es preciso adaptarse a cada situación, cambiar las mentalidades siempre que sea preciso. Es necesaria una mentalidad informativa, tradicionalmente deficiente en España, que busque permanentemente la información de manera proactiva, uniendo sistemas, operadores y analistas, integrándolos en un solo sistema distribuido, fluido y flexible, que mantenga la necesaria seguridad y que no aplique de forma restrictiva el principio de necesidad de conocer sino que sea espléndido con la necesidad de compartir.

Si no se es consciente de la necesidad de este cambio, algún día veremos cómo de entre la bruma aparece un adversario que se llevará por delante nuestra rigidez, nuestro viejo sistema de mando y la banalización que a menudo se hace de la inteligencia, y con todo ello, nuestra libertad y nuestro futuro.

El hecho de que se publique una revista como esta es muestra del interés y necesidad creciente del mundo académico y del operativo por la inteligencia. Es, en cualquier caso, una buena noticia y una magnífica iniciativa.

General de división. D. Antonio Romero Losada
Director del Centro de Inteligencia de las FAS (CIFAS)

Cuaderno de Inteligencia 1

Juan Ramón Sabaté Aragonés

> «Todo el arte de la guerra consiste en llegar a lo que está al otro lado de la colina o, en otras palabras, a lo que no sabemos a partir de lo que sabemos».
>
> *El duque de Wellington (1769-1852)*

Ya desde los orígenes de la guerra, los comandantes sintieron la necesidad de obtener información lo más precisa posible sobre la situación, capacidades, intenciones y vulnerabilidades de sus adversarios. Desde entonces, la oportuna obtención de información precisa y fiable sobre la que basar sus decisiones ha constituido una de las preocupaciones esenciales del Mando.

La Inteligencia, que constituye una de las funciones conjuntas recogidas la doctrina conjunta de nuestras Fuerzas Armadas (PDC-01[A]), permite tener una visión integral, apropiada y actualizada del entorno operativo, a la vez que ayuda a identificar las condiciones requeridas para alcanzar los objetivos operacionales, a evitar efectos no deseados y a asesorar sobre el impacto que los adversarios y los actores, amigos y neutrales, pueden tener en el concepto de la operación del comandante.

Para poder desarrollar adecuadamente esta función conjunta, nuestras Fuerzas Armadas se han ido dotando progresivamente de una estructura, unos medios y unos procedimientos cada vez más sofisticados y eficientes. Sin embargo, el elemento esencial del Sistema de Inteligencia de las Fuerzas Armadas (SIFAS) lo constituyen las personas que lo integran. Para que puedan desarrollar adecuadamente sus cometidos es necesario que cuenten con una esmerada formación y que la consoliden con una adecuada experiencia práctica.

El Curso Superior de Inteligencia de las Fuerzas Armadas (CSIFAS), impartido en la Escuela Superior de las Fuerzas Armadas (ESFAS) a través del Departamento de Inteligencia (DINT), proporciona a las unidades, centros y organismos del SIFAS, así como a otros organismos ajenos al mismo, oficiales de Inteligencia con la preparación adecuada para cumplir sus cometidos.

Para la impartición del CSIFAS, el departamento de Inteligencia cuenta con la inestimable y desinteresada contribución de personal experto, que forma parte de las organizaciones de Inteligencia nacionales, tanto militares

como civiles, así como docentes de reconocido prestigio que imparten esta materia en diversas universidades. Esta circunstancia permite al director del departamento, el coronel Ángel Segundo Gómez González, establecer una amplia y sólida red de contactos entre las personas más destacadas de lo que se conoce informalmente como la «comunidad de inteligencia».

La publicación que el lector tiene entre sus manos nace con el doble propósito de servir de vehículo de intercambio de ideas entre los que constituyen esa comunidad y, a su vez, difundir 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.

Este primer cuaderno nace del empeño personal del coronel Ángel S. Gómez, que ha contado desde el primer momento con el apoyo del director de la ESFAS, el general de división Miguel Ballenilla y García de Gamarra, y con el director del Centro de Inteligencia de las Fuerzas Armadas, el general de división Antonio Romero Losada. Asimismo, esta obra no hubiese visto la luz sin el empeño desinteresado de un selecto grupo de autores que han plasmado su experiencia y conocimientos en una recopilación de artículos de variada temática que a continuación se reproducen.

En el artículo *El subsistema de inteligencia del Ejército de Tierra: presente y retos de futuro*, los autores, Miguel Sanchez de Toca Alameda, Jorge Díaz Muriana, Raul Martín Martín y Antonio Muñoz Galdeano ofrecen un repaso de la organización del subsistema de inteligencia del Ejército de Tierra (ET), como prolongación del sistema de inteligencia de las FAS (SIFAS), destacando su doble función; la primera, la elaboración de inteligencia necesaria para el apoyo a la preparación de la Fuerza y para la contribución a las necesidades del Plan Conjunto de Inteligencia Militar; la segunda, atender al adiestramiento permanente de los elementos de inteligencia para facilitar un rápido despliegue a zona de operaciones. Dentro del subsistema, ocupa un lugar relevante la cuestión de la formación del analista, un proceso largo que conjuga tanto la experiencia profesional como el aprendizaje y que requiere una especialización en una función que es, cada vez, más compleja y demandante. La formación y retención de los analistas y de los operadores de los sistemas de obtención constituirá, qué duda cabe, uno de los retos que deberá afrontar el subsistema, junto con el de la progresiva tecnificación de los medios de obtención, la integración de la inteligencia artificial a los procesos del ciclo de inteligencia y la posible unificación de los sistemas técnicos de información e inteligencia en los niveles tácticos y operacional, contribuyendo a una mayor integración y eficacia del SIFAS.

En el artículo *Inteligencia de preparación: realismo y responsabilidad*, Julio Albaladejo López parte de los conceptos de inteligencia básica y de inteligencia actual, contemplados en la doctrina conjunta nacional y en la de la Alianza Atlántica. Seguidamente, el autor sostiene que la acumulación

de conocimiento sobre los potenciales adversarios y el entorno en el que se operará es el objeto de la inteligencia básica. Esta acumulación es una actividad de preparación y, como tal, se debe desarrollar principalmente en la estructura orgánica. Finalmente, el autor concluye que la inteligencia que se desarrolla en la estructura orgánica debe priorizarse, para asegurar que las actividades de preparación reciban un apoyo adecuado, pero también como una actividad de preparación en sí de la propia estructura de inteligencia, que acumula inteligencia básica y mantiene personal experto listo para reforzar estructuras operativas cuando sea necesario.

Sergio Flores Friaza afronta el tema *de la evolución del sistema de inteligencia del Ejército del Aire y del Espacio*. Para el autor, la creación del Centro de Inteligencia de las Fuerzas Armadas (CIFAS) supuso un cambio significativo, al integrar los órganos de inteligencia militar del Ejército de Tierra, de la Armada y del, por aquel entonces, Ejército del Aire dentro de un único sistema funcional de inteligencia. El Ejército del Aire, para dar respuesta a sus necesidades de Inteligencia en coherencia con el SIFAS, implantó un Sistema de Inteligencia del Ejército del Aire y del Espacio (SINTEA), integrando todas las capacidades propias en materia de inteligencia y contrainteligencia, tanto en beneficio de las Fuerzas Armadas en general, como del EA en particular. El SINTEA está constituido por los subsistemas de Inteligencia Táctico Aéreo (SITAC) y de Contrainteligencia e Información Interna (SCIN) y se estructura en dos niveles, superior y nivel básico, vinculados respectivamente con los escalones intermedio y básico del SIFAS. Con la promulgación de una Instrucción General del JEMA, sobre Organización y Funciones del Sistema de Inteligencia del Ejército del Aire y del Espacio (SINTEA), se adapta éste a los últimos cambios organizativos acontecidos en el seno del EA y se alinea con la estructura del CIFAS.

A raíz de la derrota de las fuerzas contrainsurgentes en Afganistán, José Lorénzo-Penalva Lucas se cuestiona si se emplearon las herramientas de análisis adecuadas, tanto en el planeamiento como en la valoración de la eficacia de las acciones ejecutadas durante las campañas. En el artículo *Inteligencia estratégica, transdisciplinariedad y sistemas complejos adaptativos*, el autor sostiene que la insurgencia, el terrorismo o el extremismo violento son fenómenos que pueden tipificarse como problemas interactivamente complejos no lineales y propone abordarlos mediante estrategias basadas en sistemas complejos adaptativos y en la transdisciplinariedad.

En su artículo, María del Carmen Ariñez Fernández aborda el tema del empleo de la inteligencia sanitaria en ámbito de la seguridad, tanto nacional como internacional. Para la autora, la experiencia en la gestión de crisis sanitarias ha puesto de manifiesto la necesidad de disponer de información temprana, fiable y predictiva, así como de un sistema de inteligencia robusto y ágil. La inteligencia sanitaria es una herramienta que apoya la toma de

decisiones de políticos y mandos militares. La preparación del Ministerio de Defensa para afrontar futuras posibles crisis sanitarias incluye la mejora y el refuerzo de las capacidades actuales de Sanidad Militar y la potenciación de la Sanidad Operativa. La mejora de la recopilación de información, utilización de fuentes, metodología de análisis y elaboración de productos de inteligencia sanitaria precisa una formación continuada del personal sanitario y una colaboración estrecha con los analistas de inteligencia del Centro Militar de Inteligencia de las FAS. La inteligencia sanitaria militar es una herramienta que puede contribuir a la respuesta nacional a la Seguridad Nacional e Internacional.

En el trabajo *El proceso IRM&CM en el Ejercicio JFX-22; las claves del éxito*, *Álvaro Álvarez Álvarez*, *Francisco Javier López Cuevas y Pablo Caneda López consideran que las Fuerzas Armadas deben incorporar nuevas tecnologías y adoptar nuevas estrategias que les permitan afrontar una gran variedad de amenazas nuevas e imprevisibles. En este contexto, los autores analizan la ejecución del ejercicio JFX-22, en el que se adiestró a la Estructura Operativa de las Fuerzas Armadas en el planeamiento y conducción de una operación de alta intensidad, a la vez que se utilizaron herramientas como la suite* SAPIIEM para gestionar la obtención y explotación de la información. Los autores consideran que una estructura eficiente, un *software* de gestión actualizado, un personal familiarizado con el funcionamiento de la organización y adecuadamente adiestrado en el empleo de las herramientas disponibles fueron claves para el éxito del proceso IRM&CM.

Jesús Antonio Vicente Montaña aborda el tema de la importancia de la inteligencia económica, tanto para España como para sus empresas. Desde 1995, la Comisión Europea ha pretendido fomentar la innovación para mejorar la competitividad y el empleo en Europa, estableciendo el concepto de inteligencia económica como una herramienta útil para la toma de decisiones. La inteligencia económica implica la coordinación de acciones de investigación, tratamiento y distribución de información útil para los agentes económicos, incluyendo la protección de la información considerada sensible. En España, la Estrategia de Seguridad Nacional de 2011 incluyó la creación de un Sistema de Inteligencia Económica (SIE) para analizar la información relevante y facilitar la acción del Estado. Lamentablemente, el proyecto no dio los frutos esperados debido a la falta de claridad en su definición, objetivos y mecanismos de actuación, así como la inconcreción de su propósito. En su artículo, el autor propone una serie de medidas para posibilitar la efectividad del SIE español, considerando que la falta de una estructura coordinada y eficaz de inteligencia económica en España limita la capacidad del país para competir en un contexto globalizado.

El subsistema de inteligencia del Ejército de Tierra: presente y retos de futuro

Miguel Sánchez de Toca Alameda
Jorge Díaz Muriana
Raúl Martín Martín
Antonio Muñoz Galdeano

Resumen

En los últimos conflictos hemos sido testigos de la evolución tecnológica y su repercusión en el campo de batalla. Uno de los aspectos con mayor impacto en el planeamiento y conducción de las operaciones militares terrestres es, sin duda, la obtención y difusión oportuna de la inteligencia en todos los escalones, que permita una acertada toma de decisiones por el *mando* a todos los niveles y una respuesta adecuada a la evolución del combate. Para ello se requiere que desde tiempo de paz, que el sistema de inteligencia esté «engrasado» y los medios, procedimientos y la organización del propio sistema, sea capaz de adaptarse al nuevo entorno operacional y cumplir con sus objetivo. En los siguientes apartados se pretenden dar una visión global de la organización del subsistema de inteligencia terrestre, sus capacidades y los retos futuros que debe acometer dentro del proyecto de «Fuerza 35».

Palabras clave

Inteligencia, SIFAS, SUINTE, CEFIET, COEMET, CIDI/ASC, sistemas de información, IMINT, GEOINT, SIGINT, OSINT, HUMINT, ISTAR, ZRI, Fuerza 35, sensores.

The Army Intelligence Subsystem: Present and Future Challenges

Abstract

Recent conflicts have witnessed the evolution of technology and its impact on the battlefield. One of the aspects with the greatest impact on the planning and conduct of military operations on the ground is undoubtedly the timely acquisition and dissemination of intelligence at all levels, enabling correct decision making by commanders at all levels and an adequate response to the evolution of the battle.

Keywords

Intelligence, SIFAS, SUINTE, CEFIET, COEMET, CIDI/ASC, information systems, IMINT, GEOINT, SIGINT, OSINT, HUMINT, ISTAR, ZRI, Force 35, sensors.

1. Introducción

La sorpresa del contraataque ucraniano al recién tomado aeropuerto de Hostomel por los rusos, recorrió todos los centros de inteligencia militares, excepto, de aquellos que lógicamente habían contribuido. La aparente falta de detección de un volumen de fuerzas de esa entidad, o el cálculo erróneo de la reacción, las probabilidades e intenciones al fin y al cabo, han vuelto a poner sobre la mesa la siempre antigua y siempre nueva necesidad de información y de su valoración. Cinco meses después, el 7 de septiembre Ucrania volvió a sorprender con una acumulación de fuerzas en el frente Este que rompió el dispositivo ruso. En la guerra ruso-ucraniana se están utilizando tácticas de hace cien años, pero alteradas por la tecnología y por el acceso a información privilegiada, y se espera aprender mucho sobre inteligencia. La revolución de las aplicaciones informáticas, la posibilidad de «apagar» y «encender» digitalmente a través de una compañía comercial un entorno virtual paralelo, está igualando puntualmente el desequilibrio de los dos contendientes. Es un momento de seguimiento, acopio de observaciones y análisis de las funciones de combate, particularmente de la inteligencia, y en el que el ET debe tratar de zambullirse al máximo. Como se puede imaginar, en una guerra tan esencialmente terrestre como la actual, la inteligencia en apoyo de las operaciones terrestres se pone a prueba y nos recuerda la importancia de tener un buen sistema de inteligencia desde tiempo de paz.

En este artículo se hace un repaso sobre la organización de la inteligencia en el ET y sus perspectivas, todo en un contexto desclasificado.

2. Organización y estructura

El Ejército de Tierra (ET) desarrolla su arquitectura de inteligencia según un modelo sistémico, como prolongación del sistema único de las Fuerzas Armadas, el Sistema de Inteligencia de las Fuerzas Armadas (SIFAS). Lo hace prolongando aquel con sus medios humanos, de obtención, procedimientos y sistemas lógicos y tecnológicos hasta constituir un subsistema específico ramificado en todos los escalones de la fuerza. Del mismo modo que el SIFAS, se articula en tres niveles que se desdoblan, a su vez, en órganos de dirección y de ejecución a los que distribuye responsabilidades y cometidos:

— El nivel terrestre superior corresponde al Estado Mayor del Ejército en cuanto al planeamiento, dirección, control y ejecución al nivel global del ET. Los órganos de ejecución son: el Centro de Fusión e Integración de Inteligencia del ET (CEFIET) y el Centro de Operaciones Electromagnético del ET (COEMET), orgánico de la Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica (JCISAT).

— El nivel terrestre intermedio se corresponde con los mandos de primer nivel de las unidades de la Fuerza del ET. Los órganos de ejecución son los Centros de Integración y Difusión de Inteligencia (CIDI) y los Centros de fusión de inteligencia de dichos mandos.
— El nivel terrestre básico se corresponde con las unidades subordinadas a los mandos de primer nivel que componen el nivel intermedio. Los órganos de ejecución, en este nivel, son todas las pequeñas unidades que cuenten con Centros de Integración y Difusión de Inteligencia (CIDI), y con capacidad de obtención. Son los verdaderos «músculos» de obtención y análisis del ET.

Todo el trabajo de este subsistema se orienta en dos esfuerzos principales: elaborar la inteligencia necesaria para apoyar la preparación de la fuerza y satisfacer las necesidades del Plan Conjunto de Inteligencia Militar (PCIM) a través del Programa de Obtención del ET (PROBET). Estos últimos son los que se elaboran en la cúspide del sistema y orientan todas las actividades de obtención y análisis.

El sistema está diseñado para adiestrarse en permanencia en la labor propia de inteligencia y poder generar y desplegar con relativa facilidad un elemento de inteligencia en zona de operaciones en apoyo de un contingente.

3. Los órganos de ejecución

El órgano de ejecución de inteligencia por excelencia, el «músculo», es el Centro de Integración y Difusión de Inteligencia (CIDI /ASC[1]). Es el elemento de gestión de inteligencia, contrainteligencia y seguridad para la elaboración de información procedente de todo tipo de fuentes; la difusión; la gestión de las necesidades de inteligencia y contrainteligencia y la coordinación de la obtención.

Participa en todas las fases del ciclo de inteligencia y algunos de sus cometidos son: el desarrollo y actualización del programa de obtención durante la fase de dirección; asignar misiones a los órganos de obtención en la fase de obtención; la compilación, evaluación, análisis, integración e interpretación de información durante la elaboración; finalizando con la difusión oportuna de los documentos en la fase de difusión.

El CIDI /ASC forma parte del elemento de apoyo de la Unidad de Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimiento (UISTAR, en inglés) y su articulación funcional viene determinada por:

— un jefe de CIDI
— un elemento de elaboración de información y difusión de inteligencia

[1] ASC: All Sources Cell.

— una célula o centro de gestión de las necesidades de inteligencia y coordinación de la obtención (CGNICO / CCIRM[2])
— un elemento de apoyo compuestos por especialistas en diversas ramas como la GEOINT[3], IMINT[4], METEO, OSINT[5] o administración de sistemas, por nombrar algunas de ellas.

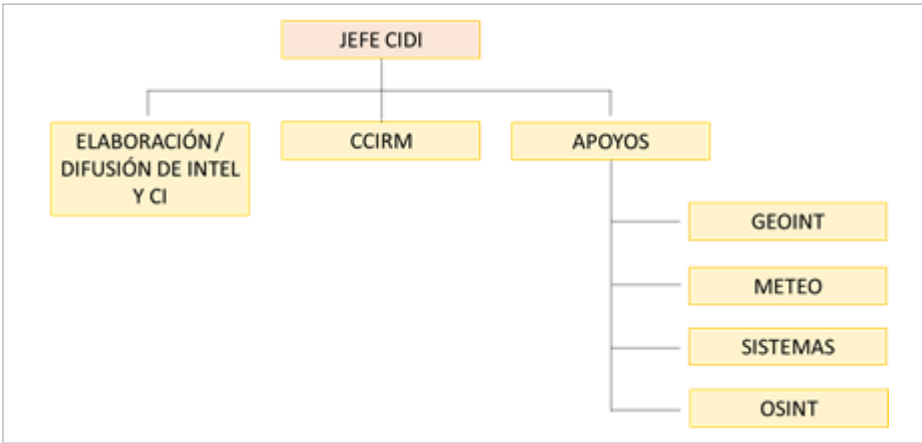


Figura 1. Estructura genérica CIDI /ASC

Como se ha indicado anteriormente, los CIDI/ASC son los órganos de ejecución de los niveles terrestre intermedio y básico del Subsistema de Inteligencia del ET (SUINTE), existiendo una relación funcional entre los CIDI/ASC del nivel terrestre intermedio y sus órganos de ejecución subordinados en el nivel terrestre básico. La propia jerarquía entre estos nodos de la malla de inteligencia es la que determina quién carga datos en el sistema y qué órgano superior los valida, bien añadiendo la valoración, bien filtrándola o depurándola.

4. Los sistemas de información

Todo sistema de inteligencia se debe apoyar en un sistema de información que haga posible el flujo de información/inteligencia entre los diferentes escalones, y el acceso a una base de datos común siguiendo los criterios de «necesidad de conocer» y «necesidad de compartir».

La experiencia indica que los datos, que proporcionan una información determinada, deben estar disponibles y accesibles en una base de datos

[2] CCIRM: Collection Center Intelligence Requirements Management.
[3] GEOINT: Inteligencia Geográfica.
[4] IMINT: Inteligencia de Imágenes.
[5] OSINT: Inteligencia de Fuentes Abiertas.

común para todos los analistas, desde los de nivel táctico hasta los de nivel estratégico. Esto se explica porque los mismos datos podrían dar una información diferente dependiendo del prisma táctico o estratégico con que el analista los analice. Dicho esto, no debemos olvidar que los diferentes niveles de inteligencia no tienen por qué tener las mismas necesidades a la hora de pensar en las capacidades que debemos pedir a un sistema de información. De tal manera que el despliegue sencillo y rápido, el reducido ancho de banda para operar y la supervivencia y robustez necesarios para el nivel táctico, no tiene por qué ser compartidos por otros niveles de inteligencia.

Actualmente en el ET se usa el Sistema de Información de Superficie (SIS) para sus necesidades tácticas. El nivel operacional usa el sistema de inteligencia de las Fuerzas Armadas (FAS) que es potencialmente interoperable con el SIS, lo que facilitará en el futuro una posible integración y satisfacer así la aspiración de un sistema de información común que permita interactuar a los analistas de diferentes niveles de inteligencia; que contenga una base de datos común que proporcione acceso a la información existente y que al mismo tiempo tenga en cuenta las necesidades operativas las Unidades usuarias.

Dos ejemplos muy interesantes en el ámbito de OTAN son INTEL-FS[6] y BICES[7]. A grandes rasgos, el primero proporciona acceso a una gran base de datos y el segundo, además de disponer de una base de datos, permite interactuar y compartir información con otros usuarios.

5. Las especialidades de Inteligencia

Las especialidades de inteligencia nacen del desarrollo de la tecnología de los medios de obtención y, en muchos casos, proporcionan una información relevante que enriquece los productos de inteligencia. Tradicionalmente el conocimiento del terreno era lo fundamental para el planteamiento de una operación pero, hoy en día, habría que añadir el conocimiento del entorno y las actividades desarrolladas en un área concreta. Las especialidades más desarrolladas en el ET son la Inteligencia de Imágenes (IMINT), Geoespacial (GEOINT), de señales electromagnéticas, acústicas y espectrales (SIGINT) y procedente de fuentes abiertas (OSINT).

La Inteligencia de imágenes (IMINT), se obtiene desde multitud de sensores y plataformas, (satélite, aérea, drones...). Estas plataformas pueden proporcionar información sobre personas, actividades, etc., de una manera discreta y, en la inmensa mayoría de los casos, sin necesidad de exponer a nuestro personal ni el material. La inteligencia Geoespacial (GEOINT), no solo puede proporcionar el posicionamiento geoespacial en un momento

[6] INTEL-FS: Intelligence - Functional Services.
[7] BICES: Battlefield Information Collection and Explotation System.

determinado o en un periodo de tiempo, sino que también permite la visualización de unidades, materiales, incidentes, etc., con sus características. Tanto una como otra están estrechamente unidas y son de gran relevancia tanto en el ámbito militar como civil. Sin embargo, y debido al elevado coste tecnológico y de formación, la captación y explotación de esos recursos se encuentran centralizadas, al disponer de sistemas informáticos que facilitan la solicitud y acceso a los productos e informes generados.

La inteligencia de señales (SIGINT) puede captar información desde distancias muy lejanas, pero requiere determinada infraestructura y mucho apoyo técnico, que el ET ha agrupado en unidades de entidad regimental. Según su desplegabilidad y alcance se puede alimentar la inteligencia conjunta, principalmente de nivel estratégico/operacional, o bien nivel operacional/ táctico, cuyos productos pueden ir en beneficio de la unidad en la cual integran sus equipos, aunque se aprovechen también para obtener inteligencia de mayor nivel.

La inteligencia de fuentes abiertas (OSINT) es quizás la subdisciplina más reciente de la inteligencia, pero tiende a acaparar cada vez mayor protagonismo y a demandar dedicación y especialización si se quiere obtener rendimiento. Los CIDI son los encargados de explotar esta especialidad con herramientas que anonimizan, deslocalizan y facilitan la navegación para poder generar productos de suficiente calidad y credibilidad. Otro papel fundamental de esta especialidad es el apoyo a otras disciplinas de inteligencia para confirmar o desechar hipótesis.

6. Las capacidades de obtención

La valía del sistema de inteligencia la da el producto final, pero para tener un *output* de calidad, debe haber un *input* valioso proporcionado por los medios de obtención, bien por la potencia de sus capacidades, bien por la oportunidad de su despliegue.

Los medios de obtención en el nivel táctico, agrupados en el marco de las Unidades de Inteligencia (ISTAR[8] por su acrónimo en inglés), deben responder a las necesidades de información que los elementos de inteligencia de cada escalón de mando requieran, tanto para apoyar el planeamiento como la conducción.

Cada nivel de mando tiene asignada una Zona de Responsabilidad de Inteligencia (ZRI), en la que su jefe responde de la producción de inteligencia que realizará gracias a la información obtenida en las misiones de inteligencia, vigilancia y reconocimiento (ISR por su acrónimo en inglés) de sus unidades subordinadas. Por esta razón las características técnicas

[8] *Intelligence Surveillance Target Acquisition and Reconnoissance.*

de los medios de obtención de cada escalón deben estar acorde con las dimensiones de su zona de responsabilidad y el tipo de información que deben captar. Esto obliga a un escalonamiento de los medios de obtención ligado a sus capacidades y particularidades técnicas.

De este modo, en el caso de los Sistemas de aeronaves no tripuladas (UAS), en los escalones superiores, nos encontraríamos con los tipo II, de gran autonomía y alcance, los tipo I *small* corresponderían al nivel brigada y los tipos micro y mini con escalones batallón compañía o incluso unidades más pequeñas en misiones ISR.

Este criterio sería el mismo para otros medios de obtención SIGINT, como los equipos ligeros de guerra electrónica (LEWT) o como el Vehículo de Exploración y Reconocimiento Terrestre (VERT) de las Unidades de Caballería, y el futuro Vehículo de Vigilancia Terrestre (VVT), que estará de dotación en las compañías de inteligencia. Este último potenciará las capacidades de obtención a nivel brigada, integrando en un único sistema los sensores electroópticos y un radar de vigilancia terrestre que proporcionarán información de explotación inmediata en beneficio de la brigada. Todas estas capacidades multiplicarán las posibilidades del escalón brigada, ampliando el alcance de su zona de responsabilidad de inteligencia en decenas de kilómetros.

El aumento de la obtención estará acompañado del auxilio de la inteligencia artificial (IA) en el análisis que le permita hacer frente a las amenazas de los entornos operativos esperables en el futuro, desde la ambigüedad de la «zona gris» hasta el combate de alta intensidad con un enemigo con capacidades parejas. En este sentido, se trabaja en el desarrollo de *software* cada vez más potentes que puedan procesar y facilitar la obtención de productos en tiempos cada vez más cortos.

7. La formación

La formación del analista de inteligencia es un proceso largo en el que se conjuga experiencia y aprendizaje. Complementado por el adiestramiento y la instrucción de las unidades, el ET contempla un modelo multiescalón, desde los niveles tácticos más bajos hasta la especialización:

- Cursos enfocados al planeamiento, gestión y ejecución de la obtención, que son el curso de inteligencia para oficiales, dirigido a capitanes que van a ejercer el mando de unidades de inteligencia y obtención, y el curso de inteligencia para suboficiales dirigido a sargentos primeros destinados en dichas unidades.
- Cursos enfocados a la dirección, planeamiento y elaboración de inteligencia en los niveles de pequeñas unidades y Brigada, como son el Curso de Especialista Militar en inteligencia, dirigido a coman-

dantes, y el Curso de Técnico Militar en inteligencia, dirigido a formar brigadas y subtenientes.
— Cursos de especialización como son los de Analista Geógrafo, Analista de Imágenes u Operador HUMINT[9].

Este escalonamiento de los cursos se completaría en su cúspide con el Curso Superior de Inteligencia de las Fuerzas Armadas, de carácter conjunto.

En cuanto a la formación en las especialidades de la inteligencia (IMINT, OSINT, SIGINT, GEOINT...), es un camino largo de recorrer que en determinadas ocasiones se contrapone con las políticas de personal propias de la administración del ET. Es la tradicional contraposición entre el modelo de personal con una vía generalista frente al requerimiento de experiencia, permanencia y formación continua de las especialidades.

8. Los retos y el futuro

Los retos a los que se enfrenta la función de combate de inteligencia para poder seguir proporcionando de forma permanente el conocimiento de la situación, son muchos y variados. Quizás el primero y más importante es el de su personal, no solo conseguir que se completen sus filas, sino que se conviertan en expertos. La clave en la producción de inteligencia es el aporte humano a la obtención, y eso requiere capacitación y experiencia. Se necesitaría que las diferentes políticas de personal, orientadas, en general a la gestión del volumen de personal, contemplasen a nuestros analistas bajo el prisma del experto. Cuesta mucho formar a un buen analista como para que en poco tiempo, o sujeto a las vicisitudes militares, se pierda. Se trata tanto de retener el talento como de captarlo al principio.

El segundo gran reto es el material; sin capacidades de obtención los analistas beben de fuentes secundarias y ya previamente orientadas. Los medios de obtención están ya en los mercados, pero los grandes programas militares demoran su incorporación a las armas a través de procesos lentos y requisitos muy difíciles de satisfacer en economías moderadas. Hace mucho que los RPAS están disponibles, baratos y con unas prestaciones crecientes por no hablar de los RPAS[10] militares de países en vías de desarrollo que se han experimentado en el conflicto de Nagorno Karabaj y de Ucrania. Lo mismo se podría decir de las capacidades de observación terrestre táctica, las posibilidades de las cámaras y sensores en vehículos de alta movilidad. El verdadero problema de los retrasos de las entradas en servicio de estas capacidades no sólo es la falta de ellas en el ínterin, sino que no llega a adquirirse el conocimiento como para su mejora y como para

[9] HUMINT: Inteligencia Humana.
[10] RPAS: *Remotely Piloted Aircraft System*.

avanzar en procedimientos. Habrá que hacer una profunda reflexión sobre si mantener las capacidades actuales dispersas o iniciar un proceso de concentrarlas en unidades específicas a modos de repositorios, donde puedan adiestrarse mejor. Al mismo tiempo, esos *pool* de capacidades se agregarían al generarse capacidades operativas que las requiriesen.

Otro aspecto clave que debe resolverse es el de un sistema técnico de información e inteligencia común a la parte táctica y operacional. Hasta ahora funcionamos en dos sistemas, o más bien en uno, en el táctico. Los dos sistemas —técnicos— tienen requisitos necesariamente distintos de desplegabilidad y conectividad aunque interoperables. Siendo lo ideal un sistema único, existen soluciones transitorias de interoperabilidad, pasarelas o compartición de BBDD[11]. Lo que está claro es que los sistemas de información son el tejido nervioso que permite al analista catalizar la producción y relaciona.

Un cariz a examinar de los sistemas es la organización en estructuras. Las actuales son, quizás, demasiado jerárquicas y deberían tender a organizaciones de mallas y nodos por capas. Los sistemas de hoy en día lo permiten ya, este reto está más relacionado con un cambio de mentalidad y de procedimientos de relación que se puede ir acometiendo desde hoy.

En cuanto al «músculo», las capacidades de los CIDI de Brigada no serán suficientes para integrar toda la información necesaria del campo de batalla, por lo que será necesario recurrir a capacidades no desplegadas que, desde territorio nacional, apoyen a las unidades desplegadas en zona de operaciones, reforzando el análisis y elaboración de productos específicos de inteligencia.

Por último, hay que incorporar la IA a los procesos de los CIDI para ser capaces de analizar el gran volumen de datos consecuencia de la era digital en la que nos encontramos, tanto en modo desplegado como en *reach back* (apoyo desde la retaguardia). Hay un campo creciente para su implementación y para que complemente al analista. Sin embargo junto a la IA aparece un riesgo no despreciable de que finalmente lo suplante: ya hay programas de IA que se han presentado a elecciones, con una capacidad de aprendizaje que, lejos de ser humana, es creciente y podría alcanzarla. Los retos a los que se enfrentará el analista podrían ser rebatir o aplicar su pensamiento crítico a las propuestas que le haga.

9. Conclusión

La inteligencia en el ET comprende el conjunto de actividades encaminadas a satisfacer las necesidades de conocimiento del jefe relativas al entorno

[11] BBDD: Base de Datos.

operativo y la situación táctica, necesarias para el planeamiento y ejecución de las operaciones, así como para la identificación de las amenazas contra las fuerzas propias y el cumplimiento de la misión. Constituida como una prolongación del SIFAS, desde el punto de vista sistémico está organizada desde tiempo de paz para poder nutrir de manera permanente la estructura del ET y pasar sus órganos de ejecución (CIDI), sin apenas transición, a las estructuras operativas que se generen.

Las capacidades de obtención del ET son adecuadas pero precisan el salto adelante que las colocará en la transición a la «Fuerza 2035[12]». La entrada en servicio de los nuevos RPAS y del VERT puede marcar ese despegue y constituir un revulsivo para mejorar las capacidades de los analistas.

La formación en inteligencia, herramienta fundamental para la integración del personal, tiende a construir una pirámide lógica en la que, tanto verticalmente como horizontalment,e el analista va adquiriendo capacidades y especialidades de inteligencia, desde el nivel básico hasta los niveles directivos más altos del sistema. Sin embargo, las políticas de gestión de personal podrían malograr el rendimiento de los analistas a medio plazo.

Por último, nos enfrentamos a la integración en un sistema de comunicaciones que incorpore a todos los niveles, que permita cargar colaborativamente y explotar en cada estrato a partir de la misma información.

Quizás para cuando se cumplan estas condiciones ya no se hablará de inteligencia específica ni subsistemas, sino que todo el personal de inteligencia pertenecerá a un mismo cuerpo que atienda las necesidades conjuntas de las FAS.

[12] Fuerza 35: proyecto de transformación de las fuerzas terrestres del ET con horizonte en el año 2035.

Inteligencia de preparación: realismo y responsabilidad

Julio Albaladejo López

Resumen

La guerra de Ucrania es una demostración palpable de que hoy en día no podemos descartar la posibilidad de vernos envueltos en un conflicto de alta intensidad con adversarios con capacidades avanzadas equiparables a las nuestras, y de que la transición entre crisis y guerra puede ser muy rápida. Ante este escenario se están intensificando las llamadas a aumentar el alistamiento y disponibilidad de capacidades militares, para lo que resultará fundamental una mejor preparación de la fuerza.

Aunque no esté claramente definida, existe una inteligencia de y para la preparación que se debe desarrollar principalmente en la estructura orgánica. Esta inteligencia es fundamentalmente inteligencia básica, menos visible y más alejada de sus clientes que la inteligencia actual, aunque tiene la ventaja de acceder con más facilidad a redes de expertos. Es menos conocida y entendida que la inteligencia en el planeamiento y conducción de operaciones, pero es igualmente operativa e imprescindible para garantizar la superioridad frente a potenciales adversarios y la seguridad de nuestras fuerzas.

En el actual contexto, es necesaria más y mejor preparación, y por ese motivo, la inteligencia que se desarrolla en la estructura orgánica debe priorizarse, para asegurar que las actividades de preparación reciben un apoyo adecuado, pero también como una actividad de preparación en sí, que acumula inteligencia básica y mantiene personal experto listo para reforzar estructuras operativas.

Palabras clave

Inteligencia, preparación, estructura orgánica, inteligencia básica.

Readiness intelligence: realism and responsibility

Abstract

The war in Ukraine is a tangible demonstration that today we cannot rule out the possibility of being involved in a high-intensity conflict with adversaries with advanced capabilities comparable to our own, and that the transition between crisis and war can be very rapid. In the face of this scenario, there are growing calls for increased recruitment and availability

of military capabilities, for which better preparation of the armed forces will be essential.

Although not clearly defined, there is an intelligence of and for the preparation that must be developed mainly in the organic structure. This intelligence is essentially basic intelligence, less visible and more remote from its clients than current intelligence, although it has the advantage of easier access to networks of experts. It is less known and understood than the intelligence used in the planning and conduct of operations, but it is just as operational and essential to ensuring superiority over potential adversaries and the safety of our forces.

In the current context, more and better preparation is needed, and for this reason, intelligence developed in the organisational structure must be prioritised to ensure that preparedness activities receive adequate support, but also as a preparedness activity in itself, accumulating basic intelligence and keeping expert personnel at the ready to reinforce operational structures.

Keywords

Intelligence, preparation, organic structure, basic intelligence.

La crisis de Ucrania es una demostración palpable de que hoy en día no podemos descartar la posibilidad de vernos envueltos en un conflicto de alta intensidad con adversarios con capacidades avanzadas equiparables a las nuestras, y de que la transición entre crisis y guerra puede ser muy rápida. Ante este escenario se están intensificando las llamadas a aumentar el alistamiento y disponibilidad de capacidades militares, para lo que resultará fundamental una mejor preparación de la fuerza. Ahora más que nunca se debe contar con inteligencia para el apoyo a una preparación realista, pero también se debe de contar con la inteligencia como una actividad de preparación prudente y responsable.

1. La Inteligencia de preparación existe

Aunque no se trate de un concepto claramente establecido en la normativa y doctrina, la inteligencia en apoyo a la preparación y como actividad de preparación ya existen y se practican. Antes de revisar algunas de sus características y de discutir por qué ahora se debe priorizar, veamos a qué nos referimos con «inteligencia de preparación».

1.1. Inteligencia

En el ámbito académico no existe una definición de inteligencia sobre la que se haya alcanzado un amplio consenso. En cualquier caso, con distintas aplicaciones y alcances se acepta que el propósito de la inteligencia es reducir la incertidumbre en la toma de decisiones ocasionada por elementos fuera de nuestro control[1]. La inteligencia, por tanto, se debe orientar a las necesidades de sus «clientes», los que deben tomar decisiones.

En nuestro caso, la doctrina conjunta establece que:

> «La inteligencia se define como el resultado de la obtención dirigida y la elaboración de la información, relativa al entorno y capacidades e intenciones de los actores, con el fin de identificar las amenazas existentes y facilitar al Comandante decidir con oportunidad»[2].

En esta definición «el comandante» se debe entender como cualquier mando que deba tomar decisiones relativas a la dirección política o estratégica de las FAS, a la preparación de las fuerzas o al planeamiento o conducción de operaciones.

La doctrina conjunta OTAN y nacional dividen la inteligencia en dos tipos o categorías: inteligencia básica y actual. La inteligencia básica se orienta

[1] Fingar, T. (2011). *Reducing Uncertainty: Intelligence Analysis and National Security*. Stanford, California: Stanford University Press.

[2] España. Estado Mayor de la Defensa. (2021). *PDC-00 Glosario de Terminología de uso Conjunto*. Ministerio de Defensa (21 de julio).

a tener el mejor conocimiento de base del entorno y actores. Este conocimiento se adquiere de forma acumulativa; revisándose y actualizándose de forma continua para mantenerlo válido y disponible para cuando sea necesario. Por otra parte, la inteligencia actual refleja la situación en el momento, es de uso inmediato por los decisores y pierde su valor con el tiempo.

A la vista de estas definiciones, se desprende que debe existir una inteligencia en apoyo de los mandos que toman las decisiones de preparación, pero también que la inteligencia básica es fundamentalmente una actividad de preparación para decisiones futuras. Existe una inteligencia para la preparación y una inteligencia de preparación.

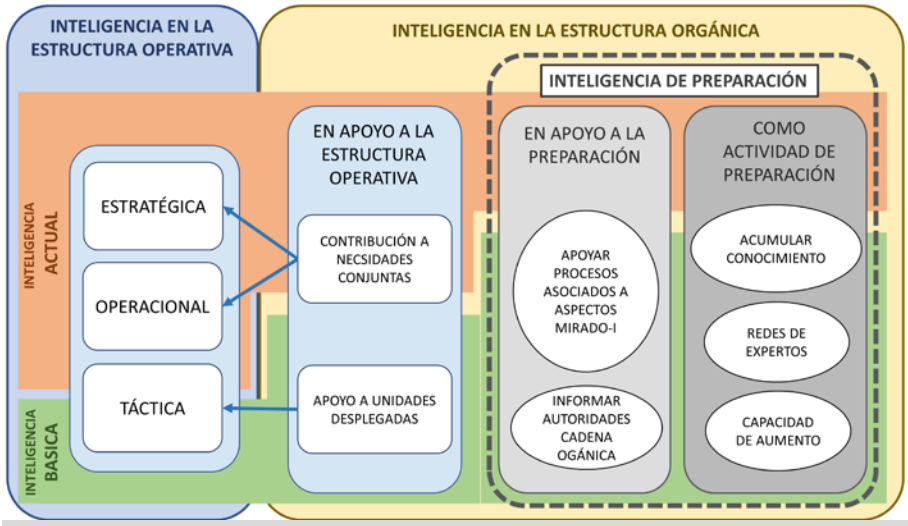


Figura 1. Inteligencia de preparación. Fuente: elaboración propia.

1.2. Preparación

> «*Las Fuerzas Armadas se organizan en dos estructuras: una orgánica, para la preparación de la Fuerza, y otra operativa, para su empleo en las misiones que se le asignen*» (artículo 11 LO 5/2005).

El término preparación no está definido en la doctrina conjunta, no obstante, asumiendo que lo que se prepara es la Fuerza como un conjunto de capacidades, se pueden entender que la preparación debe alcanzar a todos los elementos que definen una capacidad militar: material (M), infraestructura (I), recursos humanos (R), adiestramiento (A), doctrina (D), organización (O) e interoperabilidad (I) (MIRADO-I)[3]. Aunque el adiestramiento es

[3] España. Estado Mayor de la Defensa. (2018). *PDC-01(A) Doctrina para el Empleo de las FAS*. Ministerio de Defensa (27 de febrero).

una parte fundamental de la preparación, también resultan imprescindibles las acciones de alistamiento del material, dotación de personal en calidad y cantidad, organización, y doctrina, entre otras.

Al igual que el acopio de repuestos, combustible y munición forman parte de la preparación, es necesario acopiar conocimiento sobre los potenciales adversarios y el entorno en el que se operará. Acumular este conocimiento es el objeto de la inteligencia básica, es una actividad de preparación, y como tal, se debe desarrollar principalmente en la estructura orgánica. Esta orientación de los órganos de la estructura orgánica a la inteligencia básica (*foundational intelligence*) también se puede observar en la inteligencia específica de las fuerzas armadas de Estados Unidos. No en vano el lema del National Ground Intelligence Centre es «inteligencia hoy para la lucha de mañana»[4].

La preparación de la Fuerza tiene como finalidad su posterior empleo en las misiones que se le asignen y por ese motivo es una actividad plenamente relacionada con las operaciones. La estructura orgánica prepara fuerzas para su empleo en operaciones y la estructura operativa las planea y conduce.

La organización de la inteligencia militar se sustenta en el Sistema de Inteligencia de las FAS (SIFAS). Forman parte del sistema cada uno de los órganos de inteligencia pertenecientes a las estructuras operativa y orgánica de las FAS, con el objetivo de que su empleo integrado sirva a ambas estructuras[5]. De este modo, las necesidades de inteligencia de preparación deben ser atendidas por el SIFAS, no solo por los órganos del Ejército o Armada que las identifiquen.

2. Características de la inteligencia de preparación

2.1. *La difícil relación cliente-órgano de inteligencia*

La organización y doctrina para el planeamiento y conducción de operaciones integra plenamente la inteligencia con sus clientes en los Estados Mayores y unidades. Sin embargo, en la estructura orgánica, la relación de los órganos de inteligencia y sus clientes está menos estructurada y es más distante.

---

[4] Drauschak, N., Rupe, R. y Massine, P. (2020). Building the Base: Using the Army's Intelligence Program of Analysis to Drive Foundational Intelligence. *Military Intelligence Professional Bulletin* 34, n.º 20-1 (marzo). Disponible en: https://mipb.army.mil/archive/jan-mar-2020.

[5] Romero Losada, A. (2022). El Valor de Prevenir. *Revista Española de Defensa* 35, n.º 397 (septiembre), pp. 40-43.

En los procesos de preparación raramente se identifican necesidades de inteligencia y por lo general las que se generan se satisfacen por los responsables de cada proceso con sus propios medios, sin apoyarse en el sistema de inteligencia. El potencial cliente no siente la necesidad de usar este «servicio» o desconoce que está a su disposición.

Por otra parte, dado que la inteligencia básica se acumula para un uso posterior, en ocasiones, el futuro cliente todavía no se ha planteado la necesidad. En este caso, la inteligencia se debe anticipar a unas necesidades que se establecerán más adelante o que, en el mejor de los casos, están definidas en términos muy generales[6]. El cliente todavía no ha establecido sus necesidades.

La inteligencia de y para la preparación debe buscar y presentarse a sus clientes y anticiparse a sus necesidades[7]. Esta ausencia de un contacto estrecho entre órganos de inteligencia y clientes no solo resta visibilidad, sino que puede comprometer el acierto, eficacia y oportunidad de los productos elaborados.

2.2. *El difícil balance entre inteligencia actual y básica*

Como hemos visto, la inteligencia en la estructura orgánica es fundamentalmente inteligencia básica, pero no exclusivamente, también se contribuye a la inteligencia actual conjunta y se ofrece apoyo especializado a todos los niveles de la estructura operativa. Además de la elaboración de inteligencia básica, los órganos de inteligencia en la estructura orgánica deben efectuar un seguimiento de la situación actual, necesario para mantener al día a autoridades y mandos de su estructura y también como ingrediente necesario para elaborar inteligencia básica.

Los productos de inteligencia actual, fruto de este seguimiento, requieren un esfuerzo considerable, y en muchos casos, son el único resultado visible de la inteligencia en la estructura orgánica. Los órganos de inteligencia tienden a priorizar la inteligencia de uso inmediato, para evitar que sus clientes sean sorprendidos, a costa de análisis más profundos necesarios para acumular conocimiento[8]. Una excesiva atención a la elaboración de productos de inteligencia actual, de carácter perecedero, puede dejar sin recursos de análisis a la inteligencia básica. La estructura orgánica debe de ser capaz de distribuir sus recursos de manera que se priorice la inteligencia

---

[6] Cardillo, R. (2010). Intelligence Community Reform: A Cultural Evolution. *Studies in Intelligence* 54, n.º 3 (septiembre). Disponible en: https://www.cia.gov/resources/csi/studies-in-intelligence/.

[7] Oleson, P. C. y Cothron, T. (2016). Leading and Managing Intelligence Organizations. *American Intelligence Journal* 33, n.º 1, pp. 6-16.

[8] Fingar, *Reducing Uncertainty: Intelligence Analysis and National Security*.

básica de preparación sobre otros productos más visibles, que pueden ser proporcionados por otros y son menos necesarios.

2.3. El difícil encaje en los niveles de conducción de operaciones

Cuando la inteligencia se define en los niveles de conducción de operaciones, la preparación no se menciona de forma expresa. La inteligencia en el nivel estratégico se orienta a la formulación de políticas, el planeamiento militar e indicadores y alertas, mientras que en los niveles operacional y táctico lo hace al planeamiento y conducción de campañas y operaciones respectivamente. Aunque se podría argumentar que la preparación de la fuerza está en el nivel táctico en el que operará, los productos de la inteligencia básica suelen ser de utilidad en todos los niveles de planeamiento y conducción de operaciones. De hecho, con frecuencia, conocer las capacidades de determinados sistemas o unidades tiene un impacto que va de lo táctico a lo estratégico. Por ejemplo, la aparente falta de inteligencia básica sobre las capacidades de las aeronaves no tripuladas ucranianas por parte de las fuerzas rusas ha tenido un impacto en la campaña que va más allá de lo táctico[9].

Esta dificultad a la hora de encajar la inteligencia de preparación en los niveles de conducción de operaciones causó cierta confusión cuando se creó el Centro de Inteligencia de las Fuerzas Armadas (CIFAS). En la Orden que desarrollaba de la estructura del Estado Mayor de la Defensa en el año 2005 se establecía que el CIFAS sería «único en materia de información e inteligencia militar en los niveles estratégico y operacional», consecuentemente los órganos de inteligencia de los Ejércitos y la Armada se situaban exclusivamente en el nivel táctico. También se establecía que el CIFAS proporcionaría «la inteligencia necesaria para el desarrollo de las actividades de preparación de la Fuerza»[10]. En estas circunstancias parecía no ser necesario mantener una capacidad de elaboración de inteligencia en la estructura orgánica, que consecuentemente se redujo mucho. Con el tiempo se han tenido que tomar medidas para recuperar esta capacidad.

Se puede concluir que resulta difícil y confuso referir la inteligencia de preparación a los niveles de planeamiento y conducción de operaciones, por lo que se debe evitar utilizarlos al tratar la inteligencia en la estructura orgánica.

---

[9] Neveen Shaaban Abdalla *et al.* (2022). Intelligence and the War in Ukraine: Part 2. *War on the Rocks* (19 de mayo). Disponible en: https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-2/.

[10] España. Ministerio de Defensa. (2005). Orden DEF/1076/2005 por la que se desarrolla la estructura del Estado Mayor de la Defensa (abril).

2.4. La estructura orgánica permite desarrollar una red de expertos

El estudio de las capacidades de los potenciales adversarios es complejo, y debe incluir todos los aspectos que componen una capacidad. El analista que efectúe este trabajo debe aunar conocimientos técnicos y tácticos sobre la capacidad en análisis, así como sobre los procesos de inteligencia. El conocimiento sobre los aspectos navales y marítimos de los conflictos, en la mayoría de los casos, se encuentra en la estructura de la Armada[11], donde se pueden desarrollar redes de expertos dentro y fuera de la comunidad de inteligencia[12]. Con la excepción de los asuntos que conciernen a las operaciones permanentes, en la estructura orgánica es donde se encuentran estos expertos. Por ejemplo, para evaluar la amenaza de minas a la deriva, la fuerza de guerra de minas tiene los expertos en el arma, el Instituto Hidrográfico, los expertos en corrientes y la Sección de Inteligencia de la flota, los analistas navales con capacidad de integrar toda la información y producir inteligencia.

3. La Inteligencia de preparación debe priorizarse en el entorno actual

3.1. *El entorno y las estrategias requieren más preparación*

La Estrategia de Seguridad Nacional ya adelanta que ante un «clima de creciente tensión internacional, donde determinados actores se rearman para fortalecer sus aspiraciones estratégicas, España requiere una capacidad de disuasión creíble y efectiva y una capacidad de defensa autónoma, frente a diferentes formas de agresión: desde las estrategias híbridas hasta el conflicto convencional»[13]. El Concepto de Empleo de la FAS indica que, «disuasión y Defensa, han retomado mucho del protagonismo perdido durante las últimas décadas, debiendo ocupar un lugar prioritario en el desarrollo de la Estrategia Militar»[14].

Documentos posteriores a la crisis de Ucrania como son «Una Brújula para Seguridad y Defensa de la Unión Europea»[15] y el «Concepto Estratégico de la OTAN de 2022»[16], son más apremiantes sobre la necesidad de

[11] Robb, J. J. (2013). A Lack of Process; Why the Intelligence Community Finds It Difficult to Assess Military Threat». *American Intelligence Journal* 31, n.º 1, pp. 91-95.
[12] Weinbaum, Cortney *et al*. (2018). *Surging Intelligence in an Unpredictable World*. RAND Corporation. Disponible en: http://www.jstor.org/stable/resrep20002.8.
[13] España. Presidencia del Gobierno. (2021). *Estrategia de Seguridad Nacional 2021*. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021.
[14] España. Estado Mayor de la Defensa. (2021). *Concepto de Empleo de las Fuerzas Armadas 2021* (14 de octubre).
[15] European Union External Action. (2022). *A Strategic Compass for Security and Defence*. European Union (marzo).
[16] Cumbre de Madrid del Consejo Atlántico. (2022). *NATO 2022 Strategic Concept* (30 de junio). Disponible en: https://www.nato.int/strategic-concept/.

prepararnos ante la posibilidad de conflictos convencionales contra adversarios equiparables. También se insiste en ambos documentos en la necesidad de mejorar nuestra capacidad de responder con poco o sin aviso previo.

Ante esta situación, un ejercicio de realismo conduce a la conclusión de que es necesaria más y mejor preparación. En esta línea, aunque la retirada de Estados Unidos de Afganistán tiene múltiples explicaciones, en ocasiones se relaciona con la necesidad de eliminar cargas operativas que dificultaban relanzar y reorientar la preparación[17]. En nuestro caso, quizás también deberíamos poner en perspectiva las operaciones actuales, para poder priorizar la preparación de operaciones futuras.

3.2. La inteligencia se hace más importante en la preparación

Cuando se tiene una gran superioridad sobre los potenciales adversarios, como ha sido el caso en las últimas décadas, el conocimiento de sus capacidades, que en cualquier caso son siempre muy inferiores, no es prioritario. No obstante, cuando las capacidades comienzan a ser equiparables, un conocimiento profundo del adversario se hace imprescindible[18]. La preparación contra adversarios equiparables necesita más y mejor inteligencia.

En esta línea, en su «Plan de Navegación de 2021» el CNO de la Marina de Estados Unidos indicó que «todo nuestro planeamiento (estratégico, operacional y táctico) se completará con un conocimiento profundo de las capacidades y forma de pensar de nuestros adversarios [...]. Alinearemos nuestros ejercicios, experimentos y formación para entender mejor los requisitos para derrotar al adversario»[19].

Una de las prioridades debe ser anticiparse al desarrollo de las crisis, ya que una detección temprana permite tomar medidas cuando nos encontramos en la zona gris y así evitar escalar a un enfrentamiento abierto. Una detección temprana también proporciona un margen de tiempo para activar planes y elevar el alistamiento de las fuerzas. Es necesario, por tanto, perfeccionar el sistema de indicadores y alertas que es parte de la inteligencia actual. No obstante, la anticipación que se puede esperar no permitirá suplir una preparación insuficiente.

Cuando se desencadena una crisis las necesidades de inteligencia actual se disparan dejando pocos recursos para completar la inteligencia básica

---

[17] Felbab-Brown, V. (2021). The US Decision to Withdraw from Afghanistan Is the Right One. Blog *Brookings* (15 de abril). Disponible en: https://www.brookings.edu/blog/order-from-chaos/2021/04/15/the-us-decision-to-withdraw-from-afghanistan-is-the-right-one/.

[18] Arena P. y Wolford S. (2012). Arms, Intelligence, and War. *International Studies Quarterly* 56, n.º 2, pp. 351-65.

[19] Chief of Naval Operations. (2021). *CNO NAVPLAN* (enero).

no acumulada previamente. Por otra parte, en esos momentos los estados mayores operativos demandan al personal experto de aumento que en muchos casos proceden de los órganos de inteligencia de la estructura orgánica. En una crisis, con toda probabilidad, se producirá un aumento de las necesidades de inteligencia que deben ser atendidas por la estructura orgánica y una disminución de la capacidad de satisfacerlas. Es, por tanto, necesario contar con una inteligencia básica solida construida previamente y una estructura orgánica dotada de suficiente personal en calidad y cantidad[20].

Los periodos de plena normalidad deben de aprovecharse para la preparación. Por otra parte, en estos mismos periodos, las operaciones permanentes dirigen sus esfuerzos de inteligencia al conocimiento del entorno en el que se desarrollan y a la inteligencia actual que permite su conducción. En ocasiones, dentro del mismo espacio en el que se desarrollan las operaciones permanentes, tienen lugar actividades de inteligencia de preparación dirigidas a satisfacer otras necesidades. Se deben poner en contexto ambas y articular procedimientos para que se produzca la mejor coordinación, sin perder de vista que la preparación es también una actividad operativa y que no siempre será menos prioritaria que le desarrollo de las operaciones permanentes. Es necesario, por tanto, alinear la estructura orgánica y operativa, y alcanzar un funcionamiento integrado como claves del éxito.

4. Conclusión

Aunque no esté claramente definida, existe una inteligencia de y para la preparación que se debe desarrollar principalmente en la estructura orgánica. Esta inteligencia es fundamentalmente inteligencia básica, menos visible y más alejada de sus clientes que la inteligencia actual, aunque tiene la ventaja de acceder con más facilidad a redes de expertos. Es menos conocida y entendida que la inteligencia en el planeamiento y conducción de operaciones, pero es igualmente operativa e imprescindible para garantizar la superioridad frente a potenciales adversarios y la seguridad de nuestras fuerzas. Por otra parte, en el contexto actual y con cierta urgencia, es necesaria más y mejor preparación; por ese motivo, la inteligencia que se desarrolla en la estructura orgánica debe priorizarse, para asegurar que las actividades de preparación reciben un apoyo adecuado, pero también como una actividad de preparación en sí, que acumula inteligencia básica y mantiene personal experto listo para reforzar estructuras operativas.

[20] Weinbaum, C. et al. *Surging Intelligence in an Unpredictable World*.

Bibliografía

Abdalla, Neveen Shaaban, et al. (2022). Intelligence and the War in Ukraine: Part 2. *War on the Rocks*, [Consulta: 19 de mayo de 2022]. Disponible en: https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-2/.

Arena, Philip y Wolford, Scott. (2012). Arms, Intelligence, and War. *International Studies Quarterly* 56, n.º 2, pp. 351-65.

Betts, Richard K. (2007). Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD. *Political Science Quarterly* 122, n.º 4, pp. 585-606.

Cardillo, Robert. (2010). Intelligence Community Reform: A Cultural Evolution. *Studies in Intelligence* 54, n.º 3 [Consulta: septiembre de 2010. Disponible en: https://www.cia.gov/resources/csi/studies-in-intelligence/.

Chief of Naval Operations. (2022). CNO Navigation Plan.

— (2021) CNO NAVPLAN.

Cumbre de Madrid del Consejo Atlántico. (2022) NATO 2022 Strategic Concept. [Consulta 30 de junio de 2022]. Disponible en: https://www.nato.int/strategic-concept/.

Defense Intelligence Agency. (2021). Defense Intelligence Strategy. Disponible en: https://www.dia.mil/.

Díaz Matey, Gustavo. (2017). *La esencia de la inteligencia: hacia una correcta relación entre producción y consumo de inteligencia*. Instituto Español de Estudios Estratégicos (11 de mayo).

Directiva de Defensa Nacional. (2020). Presidencia del Gobierno (11 de junio).

Director of National Intelligence. (2019). National Intelligence Strategy of USA. Disponible en: https://www.dni.gov/index.php.

Dismukes, Bradford. (2020).The Return of Great-Power Competition—Cold War Lessons about Strategic Antisubmarine Warfare and Defense of Sea Lines of Communication 73, n.º 3, pp. 28.

Drauschak, Nicholas, Rupe, Robert y Massine, Philip. (2020). Building the Base: Using the Army's Intelligence Program of Analysis to Drive Foundational Intelligence. *Military Intelligence Professional Bulletin* 34, n.º 20-1 (marzo). Disponible en: https://mipb.army.mil/archive/jan-mar-2020.

Dunn, Jennifer. (2020). Training Today's Army for Tomorrow's Threats. *Military Intelligence Professional Bulletin* 34, n.º 20-4 (diciembre). Disponible en: https://mipb.army.mil/archive/oct-dec-2020.

España. (2005). Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

España (2005). Orden DEF/1076/2005 por la que se desarrolla la estructura del Estado Mayor de la Defensa Ministerio de Defensa.

España. (2020). Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas.

Estado Mayor de la Defensa. (2021) Concepto de Empleo de las Fuerzas Armadas 2021 (14 de octubre).

— (2021). PDC-00 Glosario de Terminología de uso Conjunto Ministerio de Defensa (21 de julio).

— (2018). PDC-01(A) Doctrina para el Empleo de las FAS. Ministerio de Defensa (27 de febrero).

Estrategia de Seguridad Nacional 2021. (2021). Presidencia del Gobierno (diciembre). Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021.

European Union External Action. (2022). *A Strategic Compass for Security and Defence*. European Union (marzo).

Felbab-Brown, Vanda. (2021). The US Decision to Withdraw from Afghanistan Is the Right One. Blog *Brookings* . [Consulta: 15 de abril de 2021]. Disponible en: https://www.brookings.edu/blog/order-from-chaos/2021/04/15/the-us-decision-to-withdraw-from-afghanistan-is-the-right-one/.

Fingar, Thomas. (2011). *Reducing Uncertainty: Intelligence Analysis and National Security*. Stanford, California: Stanford University Press.

Gómez González, Ángel Segundo. (2021). *Tendencias de evolución de la inteligencia militar*. Instituto Español de Estudios Estratégicos (22 de marzo).

Kerbel, Josh. (2017). Are the Analytic Tradecraft Standards Hurting as Much as Helping?. *Research Shorts and Notes*. National Intelligence University. [Consulta:14 de septiembre de 2017]. Disponible en: https://ni-u.edu/wp/research-shorts-and-notes/

Kringen, John A. (2015). Rethinking the Concept of Global Coverage in the US Intelligence Community. *Studies in Intelligence* 59, n.º 3, p.10.

Oleson, Peter C. y Tony Cothron. (2016). Leading and Managing Intelligence Organizations. *American Intelligence Journal* 33, n.º 1, pp. 6-16.

Packard, Wyman. (1996). *A Century of U.S. Naval Intelligence*. Kindle. Naval Historical Centre.

Romero Losada, António. (2022). El Valor de Prevenir. *Revista Española de Defensa* 35, n.º 397 (septiembre), pp. 40-43.

Robb, John J. (2013). A Lack of Process; Why the Intelligence Community Finds It Difficult to Assess Military Threat. *American Intelligence Journal* 31, n.º 1, pp. 91-95.

Rovner, Joshua. (2022). Intelligence and War: Does Secrecy Still Matter? *War on the Rocks*. [Consulta: 23 de mayo 2022]. Disponible en: https://warontherocks.com/2022/05/intelligence-and-war-does-secrecy-still-matter/.

US Joint Chiefs of Staff. (2013). *JP 2-0 Joint Intelligence* (22 de octubre).

Watling, Jack. (2021). Preparing Military Intelligence for Great Power Competition: Retooling the 2-Shop. *The RUSI journal* 166, n.º 1, pp. 68-80. Disponible en: https://doi.org/10.1080/03071847.2021.1923408

Weinbaum, Cortney, *et al*. (2018). *Surging Intelligence in an Unpredictable World*. RAND Corporation. Disponible en: http://www.jstor.org/stable/resrep20002.8.

La evolución del sistema de inteligencia del Ejército del Aire y del Espacio

Sergio Flores Friaza

Resumen

El *ámbito aeroespacial* es un ámbito físico que envuelve a los ámbitos terrestre y marítimo, y que ofrece la posibilidad de utilizar la tercera dimensión sobre la superficie, con un amplio espectro de alcances y altitudes. Sus características limitan, en el ámbito aéreo, la permanencia para operar en él y requiere disponer de bases en superficie.

Este ámbito proporciona a las Fuerzas Armadas las capacidades de penetración, aplicando potencia de fuego a grandes distancias con precisión, de proyección rápida y de obtención de información con rapidez y perspectiva. En él operan principalmente los medios aeroespaciales y los balísticos.

Tradicionalmente, la Inteligencia ha jugado un papel esencial en el eficaz empleo del poder aeroespacial, principalmente a través de la detección, localización, identificación y evaluación de objetivos, riesgos y amenazas en el ámbito aeroespacial, así como en la contribución a la superioridad en la toma de decisiones.

También, el ámbito aeroespacial ha sido, a través del tiempo, el lugar prioritario desde el que realizar actividades de vigilancia y reconocimiento para permitir a los comandantes aéreos adquirir y mantener un adecuado conocimiento de la situación.

En el ámbito de las Fuerzas Armadas, la creación del Centro de Inteligencia de las Fuerzas Armadas (CIFAS), como «órgano responsable de facilitar la inteligencia militar precisa para alertar sobre situaciones de interés militar con riesgo potencial de crisis, procedentes del exterior, y prestar el apoyo necesario en su ámbito a las operaciones», supuso un cambio significativo al integrar los órganos de inteligencia militar de los Ejércitos y de la Armada dentro de un único sistema funcional de inteligencia.

De esta forma, se ha establecido el Sistema de Inteligencia de las Fuerzas Armadas (SIFAS)[1], como única arquitectura, de carácter funcional en el área de inteligencia.

[1] Directiva del JEMAD 02/21 de 13 mayo 2021.

El Ejército del Aire, para dar respuesta a sus necesidades de Inteligencia en coherencia con el SIFAS entonces vigente, emitió la Directiva 23/07 del JEMA estableciendo acciones y responsabilidades conducentes a implantar un Sistema de Inteligencia del Ejército del Aire y del Espacio (SINTEA).

Palabras clave

Aeroespacial, inteligencia, organización, normativa.

The evolution of the Air and Space Army intelligence system

Abstract

The air domain is a physical domain that encompasses the land and sea domains and offers the possibility of using the third dimension on the surface, with a wide range of ranges and altitudes. Its characteristics limit the permanence of operations in the air domain and require the availability of land bases.

This domain provides the armed forces with the ability to penetrate, to apply firepower with precision at long ranges, to project it rapidly and to obtain information rapidly and accurately. Aerospace and ballistic assets are the primary means used in this domain.

Traditionally, intelligence has played an essential role in the effective use of air and space power, primarily through the detection, location, identification and assessment of air and space targets, risks and threats, and in contributing to superiority in decision making.

In addition, the air domain has historically been the primary location from which to conduct surveillance and reconnaissance activities to enable air commanders to gain and maintain adequate situational awareness.

In the field of the Armed Forces, the creation of the Armed Forces Intelligence Centre (CIFAS) as "the body responsible for providing the military intelligence required to warn of situations of military interest with a potential risk of crisis coming from abroad, and to provide the necessary support in its field to operations" represented a significant change, integrating the military intelligence services of the Army and the Navy into a single functional intelligence system.

Thus, the Armed Forces Intelligence System (SIFAS) was established as a single functional intelligence architecture.

In order to meet its intelligence requirements in accordance with the SIFAS in force at the time, the Air Force issued JEMA Directive 23/07, which defined the actions and responsibilities leading to the implementation of an Air Force and Space Intelligence System (SINTEA).

Keywords

Aerospace, intelligence, organization, regulatory.

1. Introducción

La Instrucción 37/2021 de 1 de julio, del Jefe de Estado Mayor del Ejército del Aire y del Espacio, por la que se desarrolla la organización del Ejército del Aire y del Espacio (EA), incluye, entre otras, las siguientes UCO relacionadas con la Inteligencia y la Contra-Inteligencia (CI) en el EA, que se destacan a continuación:

- La Sección de Inteligencia (SINTE), encuadrada en la División de Operaciones (DOP) del EMA, constituye el órgano de dirección de inteligencia del EA en el escalón intermedio del SIFAS, estableciendo relaciones funcionales de coordinación, cooperación y apoyo con los órganos que integran los diferentes escalones del SIFAS.
- La Sección de Información Interna (SEININ) pasa a denominarse Sección de Contrainteligencia e Información Interna (SECIN), encuadrándose en la División de Operaciones (DOP) del EMA. La SECIN se constituye como el órgano de dirección de la contrainteligencia del EA en el Escalón Intermedio del SIFAS, estableciendo relaciones funcionales de coordinación, cooperación y apoyo con los órganos que integran los diferentes escalones del SIFAS. Además, podrá establecer y coordinar con otros organismos de contrainteligencia, las actuaciones y necesidades informativas en beneficio de la seguridad del EA.
- La Sección de Inteligencia, Vigilancia y Reconocimiento (A2), encuadrada en la Dirección de Operaciones (DIROPS) del Estado Mayor del Mando Aéreo de Combate (MACOM), constituye el órgano de dirección de inteligencia del E.A en el escalón Básico del SIFAS. En base a ello es responsable de la fase de dirección del ciclo de inteligencia en el ámbito aeroespacial. Igualmente, y como parte del proceso JISR, es responsable en coordinación con el Centro de Operaciones Aeroespaciales (AOC) del planeamiento y programación del empleo de los medios ISR de carácter aeroespacial, específicos o conjuntos asignados al GJMACOM/CMOA.
- El Centro de Inteligencia y Targeting Aeroespacial (CINTAER), encuadrado en la estructura del Mando Aéreo de Combate (MACOM), constituye el órgano principal de referencia del GJMACOM en materia de inteligencia y *targeting* en el ámbito aeroespacial. Bajo la dirección de la Sección ISR (A2) de la DIROPS del Estado Mayor del MACOM, el CINTAER es responsable de la elaboración y difusión de los productos de inteligencia necesarios para el planeamiento y la conducción de las operaciones aeroespaciales y aquellos requeridos por el proceso de *targeting*, en el ámbito de sus competencias.

- El Centro de Operaciones de Vigilancia Espacial (COVE), encuadrado en la Jefatura del Sistema de Vigilancia y Control Aeroespacial (JSVICA), tiene como misión la vigilancia y conocimiento de la situación espacial de interés y la provisión de servicios en apoyo a las operaciones de las FAS.
- El Centro de Apoyo Técnico Avanzado del Ejército del Aire y del Espacio (CATA-EA), encuadrado en la Jefatura de Servicios Técnicos y Ciberespacio (JSTCIBER), es responsable de la monitorización de las redes y sistemas específicos y aquellos que se le encomienden, articulando los mecanismos oportunos y desarrollando las capacidades necesarias, para llevar a cabo la ciberdefensa de los mismos y protegerles ante posibles ataques que puedan afectar a cualquiera de las dimensiones (confidencialidad, integridad y disponibilidad) de la información que manejan o ante cualquier acción que sobre ellos se desarrolle y que sea contraria a los intereses del Ejército del Aire y del Espacio.

Además, el CATA-EA está integrado en el Sistema de Inteligencia del EA y coordina con el EMA/DOP los aspectos relativos a la ciberseguridad, cuando las acciones hostiles tengan como origen o destino el EA.

2. Exposición

El SINTEA constituye el conjunto integrador de todas las capacidades propias en materia de inteligencia y contrainteligencia, tanto en beneficio de las Fuerzas Armadas en general, como del EA en particular.

El SINTEA constituye la aportación del EA en el escalón Intermedio y básico del SIFAS, formando parte intrínseca del mismo, como arquitectura única de inteligencia en el ámbito de las FAS.

El SINTEA, bajo la dirección del Estado Mayor del Ejército del Aire y del Espacio (EMA), a través de la División de Operaciones (DOP), está constituido por dos subsistemas, a través de los cuales se dirigen, gestionan y ejecutan las actividades de inteligencia y contrainteligencia, respectivamente, en el Ejército del Aire y del Espacio:

— Subsistema[2] de Inteligencia Táctico Aéreo (SITAC)

— Subsistema de Contrainteligencia e Información Interna (SCIN)

Ambos subsistemas establecen sus relaciones funcionales a través de la estructura orgánica del EA, desde el escalón básico (UCO, Direcciones, Jefaturas y Mandos) al escalón intermedio, el EMA/DOP, del SIFAS. Además,

[2] El término Subsistema, referido tanto al SITAC como al SCIN, puede aparecer en otros documentos normativos como «Sistema».

sus aportaciones contribuyen a la generación de inteligencia y contrainteligencia en los niveles operacional y estratégico.

El SITAC proporciona la información/inteligencia necesaria para la preparación, el planeamiento y la conducción de las misiones y operaciones aeroespaciales del EA en el nivel táctico.

El SCIN proporciona la contrainteligencia necesaria para identificar, analizar y contrarrestar las amenazas a la seguridad planteadas por los Servicios de Inteligencia Hostiles (SIH) y las organizaciones o individuos involucrados en las acciones TESSCO, así como para establecer y coordinar las actuaciones y necesidades de información interna en beneficio de la seguridad del EA en el nivel táctico.

El SINTEA tiene como finalidad principal contribuir al esfuerzo de inteligencia y contrainteligencia militar de carácter conjunto, derivado del Plan de Inteligencia Militar (PIM). Para ello, se integrará como Sistema de inteligencia específico del EA dentro del sistema de inteligencia de las FAS (SIFAS).

El Plan de Inteligencia Militar (PIM) constituye el documento marco en el que se materializan:

— Los objetivos de interés de inteligencia de las FAS (OIIFAS) que han sido definidos tomando como referencia la situación geoestratégica actual.

— Las áreas y temas de interés de inteligencia (ATII).

— Las necesidades prioritarias de inteligencia (NPI).

Los objetivos del SINTEA son los siguientes:

— La difusión y empleo efectivo de la inteligencia y contrainteligencia provenientes del SIFAS.

— La gestión eficaz de las necesidades y la elaboración de inteligencia de carácter aeroespacial (nivel táctico), así como su difusión tanto a las UCO del EA como al escalón superior (CIFAS) y a otros órganos de la estructura del SIFAS que se determinen.

— Contribuir a la protección de la fuerza a través de actividades de contrainteligencia, información e inteligencia.

— Participar en el planeamiento y conducción de operaciones y ejercicios con aquellos elementos o estructuras operativas que en cada caso se establezcan.

— Desarrollar y definir, en el ámbito de sus competencias, la doctrina y normativa de inteligencia y contrainteligencia aplicables a las operaciones y misiones específicas del EA.

Definir, desarrollar e implantar la normativa relativa al apoyo de inteligencia al planeamiento y conducción de operaciones (en las áreas de CPOE[3], *Targeting*, InfoOPS, PsyOps, etc.), en el ámbito del EA, para su aplicación en el SITAC y el SCIN.

El SINTEA engloba la estructura, organización, procedimientos, relaciones, productos, sistemas de información y, en general, los recursos humanos y materiales que el EA, de forma permanente u ocasional, dedica a funciones de inteligencia y contrainteligencia.

Aunque no forman parte del SINTEA, contribuyen a este, los centros docentes del Ejercito del Aire y del Espacio que imparten formación en materia de inteligencia aeroespacial y contrainteligencia, así como las unidades cuyos cometidos están relacionados con la inteligencia geoespacial (GEOINT), los sistemas de información y comunicaciones, la ciberdefensa o las relaciones internacionales.

El SINTEA, está compuesto por los subsistemas SITAC y SCIN. Cada uno de estos subsistemas, se estructuran en dos niveles: un nivel superior y un nivel básico en el EA, vinculados respectivamente con los escalones intermedio y básico del SIFAS.

En el nivel superior, la dirección, coordinación y control del SINTEA corresponde al EMA, a través de la DOP. Para ello, cuenta con la Sección de Inteligencia (SINTE) para asuntos de inteligencia, y con la Sección de Contrainteligencia e Información Interna (SECIN) para asuntos de contrainteligencia e información interna.

El Subsistema de Inteligencia Táctico Aéreo (SITAC) comprende su estructura, arquitectura CIS, los procesos y procedimientos y los productos derivados de los mismos, los sistemas de información; en general, los recursos de personal y de material que el EA dedica a satisfacer las necesidades de información/inteligencia proveniente de los ámbitos específico o conjunto, además de aquellas otras que puntualmente le puedan ser encomendadas.

De acuerdo con las instrucciones y directrices recibidas del Estado Mayor del EA, el MACOM, como autoridad funcional en materia de inteligencia en el EA, encuadrado en el nivel básico del SINTEA, ejercerá la dirección del SITAC, cuya coordinación y control se llevará a cabo a través de la Sección ISR (A2) de su Estado Mayor.

Dentro del nivel básico del SINTEA, los órganos de ejecución del SITAC están constituidos por las UCO del EA dotadas de capacidades que les permiten desempeñar los cometidos de obtención y/o explotación, análisis y producción y difusión de productos. Para ello, estas UCO (con capacidad

[3] CPOE: Comprehensive Preparation of the Operational Environment.

ISR o NTISR[4]) estarán organizadas de manera que cuenten con los órganos o elementos necesarios para la realización de los citados cometidos.

En el marco del SITAC se establecerán relaciones funcionales entre los órganos del subsistema (dirección y ejecución) y aquellas Unidades de la Fuerza del EA[5] que dispongan en su estructura de órganos de inteligencia (secciones o negociados Intel), necesarios en su preparación para la realización de operaciones militares de carácter aeroespacial, y en su caso, ejecutar las que se les encomienden. A efectos operativos, los citados órganos de inteligencia estarían encuadrados en el SITAC.

Entre las funciones que corresponde al SITAC:

— Contribuir a satisfacer las necesidades de inteligencia militar de ámbito aeroespacial (nivel táctico) y aquellas otras derivadas del Plan de Inteligencia Militar (PIM) y asignadas en el Programa General de Obtención de Inteligencia (PROGINT) al EA. Todas estas necesidades de inteligencia militar estarán recogidas en un plan de obtención y elaboración (ICP[6]) específico del EA, cuya elaboración y actualización será responsabilidad del MACOM (con las directrices que pueda dar el EMA), como órgano de dirección del SITAC.

— Proporcionar y gestionar las necesidades de información/inteligencia de carácter táctico necesarias para el planeamiento y la conducción de las operaciones aeroespaciales, así como aquellas provenientes de las UCO integradas en el SITAC.

— Gestionar la respuesta de aquellas necesidades de información/inteligencia proveniente de elementos ajenos al SITAC, pero integrados en cualquiera de los escalones del SIFAS.

— Gestionar de manera eficaz la información/productos de inteligencia proveniente de cualquier órgano del SIFAS, facilitando su explotación a través de la integración en el ciclo de inteligencia específico del SITAC.

— Dirigir y ejecutar el proceso (J)ISR en el ámbito aeroespacial de acuerdo a los requerimientos establecidos en los correspondientes planes de obtención de inteligencia (ICP), para el desempeño de las misiones de carácter permanente asignadas al MACOM a través del Mando Operativo Aeroespacial (MOA) y, cuando se constituya, las asignadas al Mando Componente Aeroespacial (JFAC[7]).

---

[4] NTISR, Non Taditional ISR.

[5] Unidades aéreas de combate, de apoyo al combate, de acción del Estado y del sistema de vigilancia y control aeroespacial.

[6] ICP, Intelligence Collection Plan.

[7] JFAC: Joint Force Air Component.

— Contribuir, cuando se requiera, a la constitución de aquellas estructuras operativas (División ISR del Mando Componente Aeroespacial) que proporcionen el necesario apoyo en materia JISR para el planeamiento concurrente y la conducción de operaciones en los niveles táctico y operacional.

— Coordinar la elaboración de los productos de inteligencia en apoyo al targeting requeridos para el planeamiento y conducción de las operaciones y/o la elaboración o actualización de los planes que se determinen.

— Generar y supervisar la documentación necesaria para regularizar los procesos de apoyo al targeting conjunto de los que MACOM sea responsable.

El desarrollo en detalle del SITAC está contemplado en el «Concepto operativo y estructura del Subsistema de Inteligencia Táctico Aéreo», documento que será revisado periódicamente por el EMA, en coordinación con el MACOM, para asegurar la máxima eficacia de este Subsistema.

Corresponde al SCIN:

— Contribuir con sus medios a satisfacer en tiempo las necesidades de contrainteligencia militar recogidas en el ICP y aquellas otras que estén asignadas en el PROGINT al EA.

— Detectar y posibilitar la neutralización de amenazas contra la seguridad, cuyo origen o destino sea el Ejército del Aire y del Espacio, llevadas a cabo por servicios de inteligencia hostiles u organizaciones o individuos involucrados en actividades TESSCO, así como establecer y coordinar las actuaciones y necesidades informativas en beneficio de la seguridad del EA.

— En coordinación con la Sección de Protección de la Fuerza del EMA y con la colaboración de las Fuerzas y Cuerpos de Seguridad del Estado y otros servicios de información/inteligencia, mantener actualizado el mapa de riesgos que afecta al Ejército del Aire y del Espacio en territorio nacional, de forma que permita la gestión de la amenaza TESSCO en el ámbito del EA.

— Facilitar el intercambio y la explotación inmediata de la información de contrainteligencia con el escalón superior u otros órganos del SIFAS, colaborando con ellos y compartiendo la propia que pueda ser de interés.

— Colaborar con el escalón Superior u otros órganos del SIFAS en la continua actualización del mapa de riesgos que afecta al Ejército

del Aire y del Espacio en aquellas zonas de operaciones donde se encuentre desplegado.

El SCIN, se compone de los siguientes órganos:

— Como órganos de dirección, los Negociados y los Subnegociados de Contrainteligencia e Información Interna (NEININ / SUBNEININ) de los Mandos Aéreos, Agrupación del Cuartel General, Jefaturas y Direcciones del Ejército del Aire y del Espacio.

— Como órganos de ejecución, las Delegaciones de Contrainteligencia e Información Interna (DEININ), dependientes de los NEININ / SUBNEININ, y pertenecientes a las UCO del Ejército del Aire y del Espacio.

— Otros órganos de ejecución que se determinen y que cuenten con capacidad de llevar a cabo misiones de obtención de información de CI/HUMINT con dependencia funcional de la SECIN.

3. Conclusiones

— Tomando como referencia lo anteriormente expuesto, se pueden extraer las siguientes conclusiones:

— Resultaba necesario adaptar el Sistema de Inteligencia del Ejército del Aire y del Espacio (SINTEA) a los cambios organizativos acontecidos en el seno del EA.

— Para proporcionar el adecuado nivel de regulación orgánica a la revisión del SINTEA, se consideró promulgar una Instrucción General del JEMA, sobre Organización y Funciones del Sistema de Inteligencia del Ejército del Aire y del Espacio (SINTEA).

— La IG, establece los principios y criterios generales que definen la arquitectura y funcionamiento del SINTEA.

— De esta manera, la estructura del EA se alinea con la estructura del CIFAS.

Inteligencia estratégica, transdisciplinariedad y sistemas complejos adaptativos

José Lorenzo-Penalva Lucas

Resumen

El fracaso de la campaña Afganistán pone de manifiesto la necesidad de emplear aproximaciones diferentes a problemas como la insurgencia, el terrorismo o el extremismo violento. Estos fenómenos caen dentro de los problemas tipificados como interactivamente complejos no lineales.

La inteligencia asociada a la toma de decisiones, el planeamiento, la ejecución de operaciones, así como la valoración de la eficiencia de las acciones llevadas a cabo en la campaña deben emplear unas herramientas adecuadas al tipo de problema al que se enfrentan. Los sistemas complejos adaptativos y la transdisciplinariedad son dos estrategias de afrontamiento necesarias en la actual lucha contra la insurgencia, el terrorismo y el extremismo violento.

Palabras clave

Terrorismo, extremismo violento, sistemas complejos adaptativos, transdisciplinariedad, toma de decisiones.

Strategic intelligence, transdisciplinarity and complex adaptive systems

Abstract

The failure of the Afghanistan campaign highlights the need for new strategies to deal with problems such as insurgency, terrorism or violent extremism. These phenomena fall into the category of interactively complex non-linear problems.

The intelligence community involved in decision-making, planning and executing operations, as well as evaluating the effectiveness of actions taken during the campaign, must use tools appropriate to the nature of the problems they face. Complex adaptive systems and transdisciplinarity are two necessary coping strategies in the current fight against terrorism.

Keywords

Terrorism, violent extremism, complex adaptive systems, transdisciplinarity, counterterrorism, violent radicalization, decision making.

1. Introducción

Emplear las herramientas apropiadas al tipo de sistema, problema o entorno ayuda a resolverlo adecuadamente. Nadie con conocimiento de causa trataría de resolver un problema de mecánica cuántica con leyes de la mecánica clásica; sin embargo, para tratar de resolver el problema de la insurgencia, el terrorismo o el extremismo violento se están empleando las mismas herramientas que para hacer frente a un enemigo convencional, cuando las leyes que rigen el combate convencional distan mucho de las que rigen el conflicto asimétrico o irregular.

Tratar de resolver problemas complejos o caóticos con herramientas de resolución de problemas o de toma de decisiones de otro tipo, es una fórmula con una probabilidad de fracaso casi cierta. El fiasco de Afganistán es prueba de ello. Después de veinte años de conflicto violento, miles de millones de dólares gastados, cientos de miles de muertos (entre civiles, militares e insurgentes), cientos de miles de desplazados, se ha vuelto a la situación inicial: los talibanes en el gobierno y al-Qaeda con bases y santuarios en el país[1].

Este artículo profundiza en los riesgos de no emplear las herramientas adecuadas al tipo de problema al que la inteligencia se enfrenta. En concreto, se trata de responder a qué tipo de problema es el terrorismo, el extremismo violento o la insurgencia y cuáles son las estrategias de afrontamiento más adecuadas desde el punto de vista de la inteligencia asociada a la toma de decisiones.

A pesar de que el terrorismo, la insurgencia o el extremismo violento son fenómenos muy diferentes, los tres tienen un común denominador: pertenecer a la misma categoría de problema, lo que hace que el marco general de resolución de estos tres fenómenos sea el mismo, aunque luego se emplee un remedio específico para cada uno de ellos.

2. Tipos de problemas

Por un lado, los problemas pueden sintetizarse en cuatro grandes grupos: simples, complicados, complejos y caóticos.

Los problemas o entornos simples se caracterizan por tener pocas partes constituyentes. Todos los parámetros son conocidos y además, en estos entornos, rige la lógica formal, el principio de causalidad y el principio de linealidad.

[1] El director de investigación del Instituto de Estudios Estratégicos del Colegio de Guerra del Ejército de los Estados Unidos, Metz (2017), exponía la necesidad de cambiar la aproximación de la táctica y la estrategia de Estados Unidos frente al fenómeno de la insurgencia y las organizaciones terroristas.

Los problemas complicados poseen más partes que los simples; se rigen también por el teorema de la causalidad, aunque a veces pueda estar separada en el tiempo y el espacio. En un problema complicado se sabe que hay parámetros desconocidos, pero también se sabe que este vacío de conocimiento se puede solucionar obteniendo los datos faltantes.

Los problemas complejos están compuestos por numerosas partes. En estos entornos o problemas se sabe que hay parámetros conocidos y desconocidos-conocidos, asimismo hay desconocidos-desconocidos. El vacío de conocimiento en este campo se puede solucionar en los desconocidos-conocidos, aunque no de manera sencilla o evidente; por definición, no se puede solucionar en los desconocidos-desconocidos. Generalmente existe multicausalidad, pero la causalidad solo es coherente y visible a posteriori.

En los entornos o problemas caóticos hay parámetros conocidos, desconocidos e incognoscibles. La causalidad no es detectable o no existe.

Por otro lado, los problemas también pueden dividirse en dos grandes grupos: los lineales y los no lineales. Un problema lineal es aquel que puede descomponerse en partes más sencillas y cada una de las partes puede resolverse por sí misma. El resultado final será equivalente a la suma de las partes constituyentes.

Los problemas no lineales pueden dividirse en partes componentes, pero no se les pueden aplicar las cuatro leyes que rigen la mecánica de sistemas lineales (la ley aditiva de elementos, la conmutativa, la asociativa y la distributiva). Es decir, no es posible solucionar el problema resolviendo de forma individual cada una de las partes constituyentes; no es factible realizar un reduccionismo metodológico. La resistencia de un material sometido a un estrés es un ejemplo de un sistema no lineal.

Por último están los problemas o entornos interactivos y no interactivos. Las partes constituyentes en un problema o entorno interactivo están relacionadas entre sí de tal forma que no es posible actuar sobre una sin influir o alterar a las demás. Un ecosistema o el cuerpo humano y sus órganos constituyentes son ejemplos de sistemas interactivos.

Desde René Descartes a Laplace se ha tenido plena confianza en el método científico basado en la relación causa-efecto, denostando cualquier otra aproximación al conocimiento científico. El método cartesiano fue un verdadero avance para desterrar especulaciones y creencias; sin embargo este método daba respuesta exclusivamente a problemas simples y complicados, que pertenecen al conjunto de aquellos en los que reina el principio de causalidad.

La astronomía, la física y la matemática asociada fueron las primeras disciplinas científicas que se enfrentaron a la resolución de problemas complejos, como el famoso problema de los tres cuerpos formulado por Isaac Newton en los Principia. Poincaré terminó con el determinismo laplaciano, cuando en 1890 escribió la versión corregida del problema de los tres cuerpos, donde exponía la creencia de que pequeños cambios en un sistema aparentemente estable pueden hacer que éste se desequilibre repentinamente. Era el nacimiento de la teoría del caos y la mecánica y dinámica de sistemas no lineales.

La comunidad científica tardaría más de tres cuartos de siglo en comprender los comportamientos caóticos, estocásticos, de un sistema dinámico como el descrito por Poincaré. Richard Feynman, Nobel de Física en 1965, apuntó que el indeterminismo no pertenece exclusivamente a la mecánica cuántica, sino que es una propiedad básica de muchos sistemas físicos.

De todos los tipos de problemas o entornos, los más difíciles de resolver son los caóticos y después los interactivamente complejos no lineales.

Hoy en día son muchas las ciencias que trabajan con sistemas indeterministas, sistemas interactivamente complejos o sistemas complejos no lineales como, por ejemplo: la medicina para el estudio del cerebro; la sociología en sus modelos predictivos de crecimiento de las ciudades y sociedades; la informática en la programación de inteligencias artificiales; la economía en la predicción de los mercados; la ingeniería en el control de procesos; la física y la astronomía, etc.

3. Transdisciplinariedad

Entrando un poco más en detalle, los problemas interactivamente complejos no lineales, como la insurgencia, el extremismo violento y el terrorismo, se caracterizan porque:

- Están compuestos por numerosas partes no homogéneas, siendo estas las que precisamente conforman, definen y dan carácter al problema o entorno.
- Sus partes constituyentes están interrelacionadas entre sí y no es posible actuar sobre una sin influir sobre otras (por ejemplo: el sistema de actores, el binomio seguridad-economía, política-religión, otros).
- La polemología del conflicto es multicausal (Fernández-Montesinos, 2013).
- Además, este tipo de problemas se caracterizan porque algunas de sus relaciones no obedecen al principio de causalidad. Muchas de las

decisiones de los seres humanos y grupos de estos, incluidos Estados, no son racionales. Así pues, muchas de las dinámicas del terrorismo, la insurgencia o el extremismo violento obedecen a otras relaciones diferentes a las causales, como emociones, sentimientos, estética, teoría del contagio u otras.

— El mismo estímulo puede causar reacciones muy diversas en un actor o sistema, cuantitativa y cualitativamente hablando.

Desde este punto de partida, como son muchas las causas y las partes componentes, son muchas las disciplinas que deben emplearse para analizarlas y tratarlas. Sin ánimo de ser exhaustivo, la política, el derecho, la psicología, la economía, la seguridad y defensa, obras públicas e infraestructuras, enseñanza, religión, son áreas o disciplinas que están directamente relacionadas con estos fenómenos. Así pues, para comprender bien estos tres problemas resulta necesario un análisis de inteligencia multidisciplinar y multinivel (macro, meso, micro, causas estructurales, causas superficiales, etc.).

Con el fin de la Guerra Fría y el paso a una realidad internacional multipolar, la OTAN empieza a tomar conciencia de la necesidad de emplear un enfoque integral en su aproximación a los conflictos; sin embargo, no será hasta el 2010 cuando la organización publica la primera directiva integral de planeamiento de operaciones, con un verdadero un enfoque multidisciplinar[2]. España incorporará en su doctrina nacional de operaciones e inteligencia el enfoque integral[3].

Los factores del PMESII-PT —acrónimo normalizado que hace referencia a *Political, Military, Economic, Social, Infrastructure and Informations-Physical Environment and Time*— son un buen punto de partida para analizar y comprender el conflicto o la crisis, pero hay que tener dos precauciones. Primero, estos factores no deben ser limitantes para el análisis del conflicto, es decir, como cada insurgencia, terrorismo o extremismo violento son únicos temporal y espacialmente, estos fenómenos deben analizarse empleando todas las disciplinas necesarias para alcanzar el enfoque integral y holístico, sin circunscribirse a un grupo cerrado. Segundo, no es posible que un único experto o analista produzca todo lo necesario para realizar un análisis completo del conflicto, área o actor, pues se necesitan varias disciplinas para abarcar con éxito la complejidad de estos problemas.

[2] Esta directiva se actualizó por la versión 2 en 2013, Allied Command Operations Comprehensive Operations Planning Directive. Recientemente se ha publicado la versión 3. Véase también OTAN (2019) AJP-03.

[3] El enfoque integral emana desde las doctrinas de más alto nivel, como las Publicaciones Doctrinales conjuntas PDC-01 *Empleo conjunto de las Fuerza Armadas*, de febrero de 2018; o la PDC-2 *Doctrina de Inteligencia para las Fuerzas Armadas*, de marzo de 2020; hasta las de más bajo nivel como las tácticas, técnicas y procedimientos.

Siendo cierto todo lo anterior, la aproximación multidisciplinar no es suficiente y este es un aspecto que todavía no se ha interiorizado ni operativizado totalmente ni en la OTAN ni en España. Lo trascendente de este asunto es que, en el análisis, toma de decisiones y desarrollo de operaciones en ambientes complejos, lo que aporte cada una de las disciplinas no puede tratarse de manera aislada a lo que aporte el resto de las otras, porque las partes constituyentes están interrelacionadas entre sí y cuando se actúa sobre una de ellas se afecta o se desestabiliza al resto de las partes.

Transdisciplinariedad es cuando varias disciplinas trabajan de forma coordinada y subsidiaria para dar una solución holística, lo cual es lo que verdaderamente hace falta para abordar problemas complejos como la insurgencia, el extremismo violento y el terrorismo. Así pues, las diferentes disciplinas deben aportar soluciones consensuadas, en los diferentes niveles (macro, meso, micro), para hacer frente de forma holística a las diferentes causas constituyentes (profundas, superficiales y detonantes) del entorno, sistema o problema.

4. Sistemas complejos adaptativos

Como se ha visto anteriormente, el terrorismo o el extremismo violento es un problema complejo compuesto por numerosas partes constituyentes heterogéneas y relacionadas entre sí, que no pueden resolverse de forma aislada. Desde este punto de vista, la aproximación más eficiente para hacer frente a este problema es la Teoría General de Sistemas[4], es decir, ver el problema como un sistema compuesto por diferentes subsistemas. Analicemos dentro de la Teoría General de Sistemas cual es la subdisciplina que mejor se adapta a estos fenómenos.

Así como los problemas simples y complicados pueden abordarse con lecciones aprendidas del pasado, planeamiento y procedimientos, los problemas interactivamente complejos no lineales requieren interactuar, detectar hacia donde evoluciona la situación y actuar en consecuencia. No es posible resolver un problema interactivamente complejo no lineal exclusivamente con buenas prácticas o lecciones aprendidas o con el método de planeamiento y toma de decisiones actual, ya que está basado en sistemas complicados lineales.

Lo que lo que funciona una vez y en un momento o lugar determinado, en un sistema de actores que se desenvuelve en un entorno complejo interactivo y no lineal, puede no funcionar con otro actor, o con el mismo actor en otro lugar o en otro momento, porque las relaciones que rigen en ese

[4] La Teoría General de Sistemas tuvo su origen en la biología, Bertalanffy (1950), aunque posteriormente se expandió al resto de disciplinas como la ingeniería, economía, sociología, etc.

dominio no son exclusivamente causales (linealidad). Así pues, en entornos y problemas interactivamente complejos no lineales no se producen siempre las mismas respuestas a los mismos estímulos. Aunque esta lección ha sido identificada por países y organizaciones en el plano teórico (OTAN AJP-3.4.4 2016: 2-11), no ha terminado de ser bien comprendida o aplicada adecuadamente, pues el fracaso de la campaña de Afganistán así lo demuestra.

Para complicarlo más, a lo anterior hay que sumarle que, para el problema del extremismo violento y terrorismo, tampoco funciona el teorema fundamental del bienestar económico, es decir, el sistema puede no alcanzar el equilibrio competitivo aunque las condiciones sean Pareto óptimas (Arrow, 1951; Debreu, 1959). Es decir, en esta relación competitiva es posible mejorar la situación de un actor, sin empeorar la situación del otro y viceversa.

En el caso del terrorismo y la radicalización violenta, el teorema del bienestar económico solo funciona en los subconjuntos de actores que tienen los mismos fines, por ejemplo: el conjunto de organizaciones violentas extremistas, insurgentes o terroristas, o bien el conjunto de aquellos que las combaten.

Cuando se estudia el conjunto general de actores, la dinámica que rige no es el principio de Pareto, sino el teorema de juegos, como los juegos competitivos de suma cero o los juegos diferenciales (Basar y Olsder, 1982), pues los intereses de los terroristas y de los que los combaten (ejecutivo, legislativo, judicial, Fuerzas y Cuerpos de Seguridad, defensa, etc.) tienen intereses encontrados e incompatibles.

Otro aspecto importante a la hora de decidir qué disciplina se adapta mejor al problema en cuestión, es ver cómo se comportan los elementos del sistema, porque a diferencia de otras disciplinas, como la astronomía, donde los problemas pueden ser complejos pero los elementos inanimados, en este sistema los elementos tienen voluntad y propósito; reaccionarán a los estímulos en su contra. De este modo se puede decir que un sistema, una estrategia o un actor es robusto y resiliente cuando es capaz de resistir al cambio, o bien cuando es capaz de reorganizarse eficientemente después del cambio (Holling, 1973; Levin, 1998; Levin y Lubchenco, 2008; Folke et *al*., 2010).

Saber para qué se va a emplear un sistema o disciplina ayuda también a escogerlo. En este sentido, los Estados y las organizaciones internacionales planean y establecen unas líneas de trabajo o esfuerzo, de forma que, partiendo de una situación indeseable se vayan realizando acciones que produzcan efectos que permitan lograr objetivos intermedios, y tras recorrer el camino planeado, se alcance la situación final deseada u objetivo final.

Las políticas o estrategias contraterrorismo o contra la radicalización violenta no pueden ceñirse, simplemente, a una fórmula magistral preplaneada o estudiada. Los elementos del sistema no son cuerpos exánimes. Las organizaciones violentas extremistas y terroristas tienen voluntad propia, se adaptan, reaccionan, evolucionan a las acciones de aquellos que las combaten (Jackson y Loidolt, 2013; Singh, 2017; Kettle y Mumford, 2017).

La lucha contra el terrorismo y la radicalización violenta requiere de una evaluación continua y particularizada para cada amenaza, pues cada actor se comporta de manera única temporal y espacialmente y no tiene por qué responder de idéntica manera a los mismos estímulos (Brock y Durlauf, 1999; Olsson et *al*., 2004). El objeto de esta evaluación continua es valorar si las acciones que realizan los poderes del Estado están alcanzando los efectos deseados, o si, por el contrario, son estériles, o incluso contraproducentes, y actuar en consecuencia[5].

Los sistemas complejos adaptativos son parte de la dinámica de sistemas no lineales y están específicamente diseñados para entornos interactivos. Estos sistemas dan cabida a todas las peculiaridades del problema del terrorismo, radicalización y extremismo violento. Los sistemas complejos adaptativos permiten la teoría de juegos, son capaces de trabajar con condiciones Pareto óptimas y sin ellas y, asimismo, admiten retrasos entre los subsistemas (causalidad o correlación de Granger). Además, estos sistemas permiten interactuar, detectar y valorar constantemente la situación para ofrecer la «mejor solución posible» en el momento y lugar oportuno.

Los sistemas complejos adaptativos llevan aplicándose numerosos años en el campo de la ingeniería, como, por ejemplo, la centralita de inyección de un vehículo, que varía la mezcla de aire y combustible en función de la temperatura, altitud y demanda. Sin embargo, estos sistemas no se han aplicado para el análisis, planeamiento, toma de decisiones o valoración de la situación en el campo de la lucha contra el terrorismo, radicalización o extremismo violento.

5. Complementariedad entre la transdisciplinariedad y los sistemas complejos adaptativos

Para hacer frente al extremismo violento o terrorismo la herramienta óptima son los sistemas adaptativos complejos complementados con un enfoque transdisciplinar y herramientas de medición adecuadas como, por ejemplo:

[5] Véase Jordán (2017), como ejemplo de ventaja, y Horowitz (2010), como ejemplo de acción-reacción por malas decisiones políticas o de gobernanza.

— El análisis de la evolución de sistemas dinámicos (Berglund y Gentz, 2003).

— El análisis de perturbación singular, que posibilita analizar la evolución de los sistemas dinámicos en marcos de avance lentos y rápidos (Wasow, 1965; Fenichel, 1979).

— Modelos basados en un agente o actor (Bonabeau, 2002; Couzin et al., 2005; Grimm y Railsback, 2005). Permiten modelizar las dinámicas de un actor individual en función de las acciones de otros actores. Esto facilita dos aspectos muy importantes en la lucha contra el terrorismo y extremismo violento. El primero, realizar el análisis de vulnerabilidades críticas del centro de gravedad de la organización violenta extremista o terrorista. El segundo, predecir y evaluar los efectos de segundo y tercer orden de las acciones de las políticas de la estrategia contraterrorista y de la estrategia del actor terrorista.

— Debe tenerse en cuenta que, debido a que el fenómeno del terrorismo y la radicalización violenta son problemas interactivamente complejo no lineales, los modelos basados en un agente no pueden interpretarse de forma aislada, deben estar enmarcados para poder interpretar las dinámicas heterogéneas del sistema de manera holística (Flierl et al., 1999; Couzin et al., 2011).

— Modelos de gestión del riesgo e incertidumbre (Biggs et al., 2009; Scheffer et al., 2009; Crépin et al., 2012). Relacionados con la robustez, la resiliencia y la precaución. La precaución es un principio que tiene aplicación directa en las políticas contra el terrorismo y extremismo violento, pero que mal empleado puede ser causante de conflicto prolongado.

6. Conclusiones

Se hace necesario revisar los métodos de análisis de inteligencia, planeamiento y toma de decisiones empleados para abordar problemas interactivamente complejos no lineales como la insurgencia, el extremismo violento o el terrorismo.

Emplear métodos antiguos, o no adecuados al tipo de problema, aumenta la probabilidad de fracaso en el análisis de inteligencia, o en la toma de decisiones, lo cual pone en riesgo alcanzar la situación final deseada de la campaña o de la línea de esfuerzo operacional o estratégica.

Los sistemas complejos adaptativos, dentro de la teoría general de sistemas, en combinación con un enfoque holístico transdisciplinar, ofrecen un sistema probado y adecuado en otras disciplinas como la medicina, inge-

niería o biología, para afrontar problemas interactivamente complejos no lineales como la insurgencia, el terrorismo o el extremismo violento.

Bibliografía

Arrow, K. J. (1951). An extension of the basic theorems of classical welfare economics. *Proceedings of the Second Berkeley Symposium*. Berkeley: University of California Press.

Basar, T. y G. J. Olsder. (1982). *Dynamic Non-Cooperative Game Theory*. New York: Academic Press.

Berglund, N. y Gentz, B. (2003). Geometric singular perturbation theory for stochastic differential equations. *Journal of differential equations*, 191 (1), pp. 1-54. [Consulta: 28 de enero 2022]. Disponible en: https://doi.org/10.1016/S0022-0396(03)00020-2

Biggs, R., Carpenter, S. R. y Brock, W. A. (2009). Turning back from the brink: detecting an impending regime shift in time to avert it. *Proceedings of the National academy of Sciences*, 106 (3), pp. 826-831. [Consulta: junio de 2022]. Disponible en: https://doi.org/10.1073/pnas.0811729106

Bonabeau, E. (2002). Adaptive agents, intelligence, and emergent human organization: capturing complexity through agent-based modeling: methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences USA* 99, pp. 7280-7287. [Consulta: junio de 2022]. Disponible en: https://doi.org/10.1073/pnas.082080899

Brock, W. A. y S. N. Durlauf. (1999). A formal model of theory choice in science. *Economic Theory* 14, pp. 113-130. [Consulta: el 27 de enero 2022]. Disponible en: https://doi.org/10.1007/s001990050284

Crépin, A. S. et *al.* (2012). Regime shifts and management. *Ecological Economics*, 84, pp. 15-22. [Consulta: en junio 2022]. Disponible en: https://doi.org/10.1016/j.ecolecon.2012.09.003

Couzin, I. D. et *al.* (2005). Effective leadership and decision-making in animal groups on the move. *Nature* 433, pp. 513-516. [Consulta: 27 de enero de 2022].Disponible en: https://doi.org/10.1038/nature03236

Couzin, I. D., Ioannou, C. C y Demirel, G. (2011). Uninformed individuals promote democratic consensus in animal groups. *Science* 332 (6062), pp. 1578-1580. [Consulta: 27 de enero 2022]. Disponible en: http://dx.doi.org/10.1126/science.1210280

Debreu, G. (1959). *Theory of Value*. New York: JohnWiley.

Fenichel, N. (1979). Geometric singular perturbation theory for ordinary differential equations. *Journal of Differential Equations* 31, pp. 53-98. [Consulta: 27 de enero 2022]. Disponible en: https://doi.org/10.1016/0022-0396(79)90152-9

Fernández-Montesinos, F. A. (2013). El terrorismo como narración. *Claves de razón práctica* (228), pp. 98-111. [Consulta: 27 de enero 2022]. Disponible en: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/F.Aznar_Articulo_TerrorismoNarracion_mayo2013.pdf

Flierl, G., Grünbaum, D. Levin, S. A. y Olson D. (1999). From individuals to aggregations: the interplay between behavior and physics. *Journal of Theoretical Biology* 196, pp. 397-454. [Consulta: 27 de enero 2022] Disponible en: https://doi.org/10.1006/jtbi.1998.0842

Folke, C. et *al.* (2010). Resilience thinking: integrating resilience, adaptability and transformability. *Ecology and Society* 15 (4), p. 20. [Consulta: 27 de enero 2022]. Disponible en: https://www.ecologyandsociety.org/vol15/iss4/art20/

Grimm, V. y Railsback, S. F. (2005). *Individual Based Modeling and Ecology*. Princeton, NJ: Princeton University Press.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, pp. 1-23. [Consulta: 27 de enero 2022]. Disponible en: https://doi.org/10.1146/annurev.es.04.110173.000245

Jackson, B. A. y Loidolt, B. (2013). Considering al-Qa'ida's Innovation Doctrine: From Strategic Texts «Innovation in Practice». *Terrorism and Political Violence*, 25 (2), pp. 284-310. Disponible en: https://doi.org/10.1080/09546553.2012.662557

Jackson, B. A. et *al.* (2005). *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups* (vol. 2). Rand Corporation.

Jordán, J. (2017). Un modelo explicativo de los procesos de cambio en las organizaciones militares: la respuesta de Estados Unidos después del 11-s como caso de estudio. *Revista de Ciencia Política* (Santiago), 37 (1), pp. 203-226. [Consulta: 27 de enero 2022] Disponible en: https://doi.org/10.4067/S0718-090X2017000100009

Kettle, L. y Mumford, A. (2017). Terrorist learning: A new analytical framework. *Studies in Conflict & Terrorism*, 40 (7), pp. 523-538. [Consulta: 27 de enero 2022]. Disponible en: https://doi.org/10.1080/1057610X.2016.1237224

Horowitz, M. (2010). Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism. *International Organization*, 64 (1),

pp. 33-64. [Consulta: 27 de enero 2022] Disponible en: https://doi.org/10.1017/S0020818309990233

Levin, S.A. (1998). Ecosystems and the biosphere as complex adaptive systems. *Ecosystems* 1, pp. 431-436. [Consulta: 27 de enero de 2022]. Disponible en: https://www.jstor.org/stable/3658676

Levin, S. A. y Lubchenco, J. (2008). Resilience, robustness, and marine ecosystem-based management. *Bioscience* 58 (1), pp. 27-32. [Consulta: 27 de enero 2022]. Disponible en: https://doi.org/10.1641/B580107

Ministerio de Defensa. (2018). *Empleo conjunto de las Fuerza Armadas*. Publicación Doctrinal Conjunta PDC-01. [Consulta: 30 de enero de 2022]. Disponible en:

https://publicaciones.defensa.gob.es/media/downloadable/files/links/p/d/pdc-01_a_doctrina_para_el_empleo_de_las_fas.pdf

Ministerio de Defensa. (2020). *Doctrina de Inteligencia para las Fuerzas Armadas*. Publicación Doctrinal Conjunta PDC-2.

Olsson, P., Folke, C. y Berkes F. (2004). Adaptive comanagement for building resilience in social-ecological systems. *Environmental Management* 34 (1), pp. 75-90. [Consulta: 22 de enero 2022]. Disponible en: http://dx.doi.org/10.1007/s00267-003-0101-7

Poincaré, H. (1890). Sur le problème des trois corps et les équations de la dynamique. *Acta mathematica*, 13 (1), pp. A3-A270. [Consulta: 8 de febrero 2022]. Disponible en: https://ia600708.us.archive.org/view_archive.php?archive=/22/items/crossref-pre-1909-scholarly-works/10.1007%252Fbf02360180.zip&file=10.1007%252Fbf02392506.pdf

OTAN. [Consulta: 19 de diciembre 2021] Disponible en: todas las publicaciones, previo registro, en: https://nso.nato.int/nso/home/main/home:

—. (2016). AJP-3.4.4 Ed A v.1 *Allied Joint Doctrine for Counter-Insurgency (COIN)*.

—. (2019). *AJP-3 Allied Joint Doctrine for the Conduct of Operations Edition C Version 1*.

Singh, R. (2017). A Preliminary Typology Mapping Pathways of Learning and Innovation by Modern Jihadist Groups. *Studies in Conflict & Terrorism*, 40: 7, pp. 624-644. [Consulta: 27 de enero 2022]. Disponible en: https://doi.org/10.1080/1057610X.2016.1237228

Scheffer, M. et *al.* (2009). Early-warning signals for critical transitions. *Nature*, 461 (7260), pp. 53-59. [Consulta: junio 2022]. Disponible en: https://doi.org/10.1038/nature08227

Von Bertalanffy, L. (1950). An Outline of General System Theory, British Journal for the Philosophy of Science 1, pp.139-164. [Consulta: 5 de febrero 2022. Disponible en: http://www.isnature.org/Events/2009/Summer/r/Bertalanffy1950-GST_Outline_SELECT.pdf

Wasow, W. (1965). *Asymptotic Expansions for Ordinary Differential Equations*. New York: Dover Phoenix Editions.

Contribución de la inteligencia sanitaria a la seguridad nacional e internacional

María del Carmen Ariñez Fernández

Resumen

La pandemia causada por el virus SARS-CoV-2 ha tenido un impacto importante en los sistemas sanitarios de los países, en la economía y en su geopolítica, de tal forma que ha sido una amenaza para la seguridad nacional e internacional. En el presente artículo se plantea la importancia de integrar la inteligencia sanitaria militar en la función conjunta de inteligencia, y así realizar el apoyo a la toma de decisiones ante la gestión de crisis sanitarias que pueden afectar a la seguridad nacional e internacional. El sistema sanitario español está desarrollando normativas en materia de salud pública que establezcan, entre sus líneas de acción, mejorar la inteligencia epidemiológica como un sistema de alerta precoz y predictivo de futuras epidemias y pandemias. Una inteligencia sanitaria militar reforzada y mejorada es una herramienta más imprescindible para el apoyo interno y a la población civil.

Palabras clave

Inteligencia sanitaria, seguridad, inteligencia epidemiológica, operaciones militares.

Contribution of health intelligence to national and international security

Abstract

The pandemic caused by the SARS-CoV-2 virus has had a significant impact on the health systems, economies and geopolitics of all countries, making it a threat to national and international security. This article discusses the importance of integrating military medical intelligence into the joint intelligence function to support the decision-making process in health crisis management that may affect national and international security. The Spanish national health system is developing public health regulations that include among its lines of action the improvement of epidemiological intelligence as an early warning and predictive system for future epidemics and pandemics. Strengthened and improved military medical intelligence is an important tool for internal and civilian support.

Keywords

Medical intelligence, security, epidemic intelligence, military operations.

1. Introducción

La pandemia por el virus SARS-CoV-2, que durante tres años afecta a la población a nivel mundial, ha dado un giro de 360 grados a las percepciones sobre la seguridad en España, en Europa y en todos los países, en general. La pandemia ha sido causada por un agente infeccioso por el que se ha restringido la libertad de los ciudadanos, su bienestar, y ha sido capaz de comprometer tanto la seguridad nacional como la internacional.

Esta situación de crisis confirma que, además de los conceptos tradicionales de seguridad y defensa, se ha de ampliar el concepto de seguridad con nuevas dimensiones como son la seguridad energética, la económica, la ciberseguridad y la seguridad sanitaria. La Directiva de Defensa Nacional 2020[1] incluye entre las amenazas para la seguridad y los desafíos a la seguridad de los Estados a las epidemias y pandemias, al mismo tiempo que asume que tienen un carácter complejo y transnacional, por lo que deben ser abordadas globalmente.

La experiencia acumulada durante la última década con la gestión de las situaciones de crisis sanitaria originadas por las epidemias de SARS, MERS, la Enfermedad por virus Ébola, los brotes de fiebre aftosa o, la más reciente, la causada por la covid-19, situaciones de emergencia que han afectado a todos los sectores de las sociedades (político, militar, económico, social, a las infraestructuras y a la información), ha puesto de manifiesto la necesidad de disponer de información temprana, fiable, predictiva, y de un sistema de inteligencia robusto, ágil, completo sobre todos los factores influyentes, como elemento clave para reducir la incertidumbre y facilitar la toma de decisiones sobre la gestión de la crisis y medidas de respuesta en escenarios complejos.

La inteligencia sanitaria es una herramienta que apoya la toma de decisiones de políticos, mandos militares, autoridades sanitarias, entre otros, y contribuye al planeamiento del apoyo sanitario de las operaciones. Puede considerarse una función de inteligencia más que una función de sanidad.

2. Entorno operativo

El entorno de paz y seguridad actual en el que vivimos se caracteriza por estar influido por numerosos riesgos y amenazas que alteran su estabilidad y generan un contexto caracterizado por la confusión e incertidumbre respecto a su evolución.

Factores sanitarios como son las enfermedades infecciosas, la contaminación ambiental y el fallo o la debilidad de los sistemas sanitarios constitu-

[1] «Todos los enlaces se encuentran activos a fecha de cierre del presente documento, 29 de enero de 2023».

yen una amenaza sobre la salud de los ciudadanos y los sistemas sanitarios, por tanto, son capaces de debilitar la seguridad colectiva de las sociedades (Kaufman 2001).

Por una parte, se ha incrementado la expansión de distintas amenazas sanitarias a nivel global, como son el virus SARS-CoV-2, MERS, el virus del Ébola, la detección de vectores de zoonosis en latitudes más altas, el aumento de casos infectados por el bacilo tuberculosis multirresistente, etc., reactivando el riesgo de que la salud de los ciudadanos se vea afectada, sin que pueda descartarse la aparición de nuevas epidemias a nivel local o incluso pandemias. De manera paralela, se ha producido un preocupante incremento de la actuación de grupos terroristas y de organizaciones con acceso a agentes biológicos y químicos con capacidad para su uso y diseminación, junto a una mejora en la investigación sobre la manipulación tecnológica de los agentes biológicos para facilitar su utilización (Interpol).

España está comprometida a contribuir a la preservación de la paz y seguridad internacionales, colaborando en la defensa de los intereses de seguridad compartidos con sus socios y aliados de la Unión Europea, de la Organización del Tratado del Atlántico Norte (OTAN), respaldando a las Naciones Unidas y con otros países mediante relaciones bilaterales y multilaterales.

La Ley de Seguridad Nacional (LSN 2015) incluye la seguridad sanitaria entre los ámbitos de especial interés de la seguridad nacional por resultar un factor básico para preservar los derechos y libertades, así como el bienestar de los ciudadanos.

La Directiva de Defensa Nacional 2020 (DDN 2020) indica que «las Fuerzas Armadas (FAS) son el instrumento especializado capaz de garantizar una defensa eficaz frente a cualquier reto de seguridad militar», tanto en Territorio Nacional (TN) como en las distintas Zonas de Operaciones (ZO) y establece que «las Fuerzas Armadas deben ser capaces y estar en disposición de afrontar una adaptación y transformación constantes, que les permita hacer frente a amenazas y desafíos múltiples y cambiantes».

Los compromisos de España con las distintas organizaciones que velan por la paz y seguridad de los ciudadanos implican la aportación de capacidades y fuerzas propias a sus estructuras, misiones y operaciones de paz, para hacer frente a cualquier reto de seguridad que se presente. Durante la operación Balmis para la gestión de la pandemia por covid-19, la actuación de las FAS se ha adaptado a un renovado contexto de globalización, condicionado por una mayor incertidumbre y un cambio acelerado.

La Estrategia de Seguridad Nacional 2021 (ESN 2021) contempla varios riesgos y amenazas a la Seguridad Nacional que están interrela-

cionados, que actúan de forma dinámica y que clasifica según su grado de probabilidad e impacto. Entre estos riesgos y amenazas se encuentran por un lado las epidemias y pandemias, las emergencias y catástrofes causadas por los riesgos nucleares, radiológicos y biológicos (NBQ) y, por otro, la amenaza real de proliferación de armas de destrucción masiva.

La magnitud de los riesgos y las amenazas actuales requiere la correcta adecuación de los recursos, medios, sistemas y organizaciones disponibles para hacerles frente. La pandemia ha puesto de relieve la importancia de los sistemas de alerta temprana, de la fusión y el análisis de la información y de los planes de respuesta para la gestión de crisis, medidas todas ellas que facilitan y agilizan la toma de decisiones. Para ello, es necesario disponer de un Sistema de Seguridad Nacional digitalizado, capaz de recoger datos y proporcionar información para la toma de decisiones en tiempo oportuno, ya que se la gestión de desafíos, como las pandemias, el terrorismo internacional, los ciberataques al sistema sanitario o las campañas de desinformación, incluidas las relacionadas con temas sanitarios, requieren respuestas colectivas e integración de capacidades civiles y militares.

En la actualidad, es necesario el fortalecimiento de las capacidades de los componentes fundamentales de la seguridad nacional (la defensa nacional, la acción exterior y la seguridad pública, con el apoyo de los servicios de inteligencia e información del Estado) junto al refuerzo de la sanidad pública, con la finalidad de reforzar la resiliencia y la capacidad de respuesta de todas las estructuras esenciales de la nación.

La prevención y la adaptación serán las claves para lograr contribuir a la actuación eficaz de las FAS en cualquier escenario.

Entre las conclusiones a las que llega la adaptación de la estrategia militar, (CEFAS 2021) al entorno estratégico actual se considera que se debe aumentar y prosperar la coordinación y el intercambio de información con otros ámbitos de la seguridad nacional para su contribución de las FAS a la estabilidad internacional.

3. La amenaza sanitaria

La Ley Orgánica 5/2005 de la Defensa Nacional especifica en el artículo 15 que las FAS «contribuyen militarmente a la seguridad y defensa de España y de sus aliados, en el marco de las organizaciones internacionales de las que España forma parte, así como al mantenimiento de la paz, la estabilidad y la ayuda humanitaria».

Con el fin de realizar su actuación para defender, preservar y asegurar los intereses de España, las FAS deben desplazarse fuera de TN para participar en distintas misiones internacionales y operaciones de paz en el marco multinacional de las Organizaciones Internacionales de Seguridad y Defensa (OISD) (CEFAS 2021).

El despliegue de una fuerza sana, en cualquier momento y a cualquier zona del mundo requiere disponer de medidas preventivas integrales y coordinadas para hacer frente a las distintas y variadas amenazas existentes en el Área de Operaciones (AO). Para ello es necesario conocer, previo al despliegue, cuáles son los factores existentes en el entorno operativo de despliegue que pueden afectar a la salud de la fuerza y, por ende, al cumplimiento de la misión (Borden Institut, vol. 1), es necesario conocer cuáles son los peligros y amenazas para la salud de la fuerza expedicionaria (Borden Institut, 2003).

Las operaciones militares se llevan a cabo en entornos que en la mayoría de las ocasiones son muy distintos a nuestro entorno habitual en España. Contextos donde bajo algunas situaciones determinadas, como guerras, terremotos, campamentos de refugiados, situaciones de hacinamiento e inadecuadas condiciones higiénicas, favorecen la expansión de agentes infecciosos y el desarrollo de la enfermedad.

La Publicación Doctrinal Conjunta de Inteligencia para las FAS (PDC-2) define amenaza a «toda circunstancia real que ponga en peligro la seguridad». Se entiende por amenaza sanitaria a cualquier factor, existente o potencial, acciones del enemigo, condiciones ambientales, que puede afectar a la salud de las personas, reduciendo su capacidad de combate, bien por causa de las heridas —no de combate— o por enfermedades.

Las poblaciones, los ejércitos, han visto diezmada su número de efectivos en diversas ocasiones a lo largo de la historia. La peste es un ejemplo claro, en Atenas, 430-426 a. C., causó la pérdida de un tercio de los ciudadanos, entre ellos la infantería ateniense y numerosos marinos; en el asedio de Siracusa por el ejército cartaginés, 396 a. C., o la peste en Roma en la época de gobierno de Marco Aurelio, que logró expandirse por toda Italia hasta las Galias (Ceberio, 2021), aniquilando a ciudadanos y ejércitos sin compasión.

Enfermedades transmitidas por vectores como son la fiebre amarilla y la malaria o paludismo (endémica en España hasta la década de los sesenta, s. XX), han sido el azote de los múltiples contingentes que se desplazan a zonas endémicas, en época y latitudes cálidas, hasta que se implementaron medidas preventivas como son la vacunación frente a la fiebre amarilla y la toma de quimioprofilaxis frente a la malaria.

En las campañas militares son múltiples los ejemplos en los que las unidades, los contingente,s han visto notablemente mermada su operatividad por las bajas causadas por enfermedades y lesiones no de combate, llegando incluso a originar el fracaso de la misión. En España se puede citar el brote epidémico de tifus registrado que ocurrió durante el asedio de Granada por los Reyes Católicos, 1489 (González, 2017). En las guerras con desplazamiento a otros continentes, como sucedió en la guerra de Cuba, el número de fallecidos por enfermedades transmisibles (fiebre amarilla, malaria, tifus, diarrea, etc.) fue muy superior a los fallecidos por combate (Díaz, 1998).

La amenaza sanitaria existe en las zonas de despliegue, por lo que es necesario identificar cuál es, estimar el riesgo de que pueda afectar al personal desplegado y establecer las medidas preventivas para reducir o eliminar ese riesgo. Se define riesgo en la PDC-2 como «la probabilidad de que una amenaza se materialice, produciendo un daño, así como el impacto que ello pueda tener, en este caso, en la salud de las personas».

Alrededor del 400 a. C., Hipócrates de Cos, gran médico griego y maestro reconocido de la época, enseñaba que para investigar en medicina se debe tener en cuenta los efectos de (FM N. 8-10-8):

Las estaciones.

— El viento, el calor y el frío.

— La cantidad de agua.

— El terreno de la ciudad.

Ya entonces reconocía estos factores críticos para el estudio antes de desplazarse a una ciudad donde se es un extraño. Consideraba que con el estudio de estas variables se podían identificar las enfermedades existentes, su forma de tratamiento y, lo más importante, cómo prevenirlas. Incluso de esta información se podían prever las epidemias que podrían aparecer.

Durante la preparación para los despliegues, es crítico que los mandos a nivel estratégico y operacional reciban asesoramiento sobre cuál es la amenaza sanitaria en el AO, ya que deben decidir qué medidas se deben implementar para proteger a los efectivos de las enfermedades no de combate. Un buen asesoramiento sanitario identificará las amenazas sanitarias que pueden disminuir la efectividad de la fuerza en sus misiones o en el combate y causar morbi-mortalidad que afectará a la consecución de la misión. La protección de la salud del combatiente es cada vez de mayor importancia dada su difícil reposición, lo que aumenta la importancia de la inteligencia sanitaria. Este asesoramiento será la base para implementar medidas que reduzcan o eliminen las amenazas.

4. Inteligencia sanitaria

Es a partir de 1992 cuando las FAS españolas, y con ellas la sanidad militar, aumentan su participación recurrente en misiones internacionales (Alsina, 2010). Este tipo de operaciones se llevan a cabo habitualmente en zonas geográficas donde están presentes enfermedades que no ocurren en España o su prevalencia es muy baja, por las condiciones climatológicas o las características del terreno hostiles a las operaciones militares, o por flora o fauna peligrosa.

En España, la doctrina relativa a la Inteligencia Sanitaria (MEDINTEL O MEDINT acrónimos aceptados en OTAN) está definida en la PDC-2 del Estado Mayor de la Defensa, publicación de referencia de la inteligencia militar en España. Se contempla la inteligencia sanitaria como uno de los campos de trabajo que satisface las necesidades de inteligencia especializada en materia sanitaria. Los analistas de inteligencia sanitaria proporcionan asesoramiento experto técnico y científico que será incluido en el asesoramiento general al mando.

En la Doctrina Sanitaria en Operaciones (PDC-4.10), se adopta la definición OTAN de inteligencia sanitaria. Se define como la inteligencia que resulta del análisis de información sanitaria, biocientífica, epidemiológica, medioambiental y cualquier otra relacionada con la salud humana o animal. Es un tipo de inteligencia de carácter técnico que requiere asesoramiento y análisis experto por personal sanitario durante todas las fases del ciclo de inteligencia.

MEDINTEL identifica las amenazas del área de despliegue y valora riesgos que podrían influir sobre la salud del contingente, de tal forma que proporciona al mando, a los decisores, la valoración sanitaria esencial para el conocimiento de la situación (SA, Situational Awareness), necesaria para el planeamiento y conducción de las operaciones, contribuyendo así a tener una comprensión integral del entorno operativo y apoya la adopción de decisiones eficientes para reducir el riesgo sobre la salud (AJMedP-3, 2020).

Para satisfacer las Necesidades de Información (NI) de este tipo de inteligencia especializada se recoge información que versará sobre el conocimiento del comportamiento y posible evolución de la amenaza, el número de personas afectadas, las necesidades de productos básicos, de apoyo sanitario o transporte, la ubicación de las infraestructuras que han sido dañadas o incluso las posibles amenazas a la seguridad ciudadana. Además, se recogerá información, entre otros, de los siguientes campos presentes en el AO (SRD-1 to AJMedP-3, 2020).

a) Factores ambientales del entorno, incluyendo compuestos industriales tóxicos, calidad medioambiental e industrias, radiaciones, agentes biológicos y químicos.

b) Características geográficas y climáticas, factores socioeconómicos y de salud pública que, de alguna forma, puedan afectar a la salud de las fuerzas o a la conducción del apoyo sanitario.
c) Información epidemiológica incluyendo la prevalencia e incidencia de las enfermedades transmisibles —en especial enfermedades transmitidas por agua y alimentos, vectores y enfermedades de transmisión sexual—. Riesgos derivados de la fauna y flora local.
d) Calidad y disponibilidad de los servicios sanitarios civiles y militares; infraestructuras locales existentes; la organización; especialidades de los hospitales y centros de tratamiento médico; los servicios de evacuación de bajas sanitarias y de emergencias; el equipamiento sanitario; bancos de sangre y laboratorios clínico; estándares y capacidades de salud pública, fiabilidad de su sanidad y posibilidades de empleo. Incluidas las capacidades militares sanitarias.
e) Gestión de recursos sanitarios, incluyendo los derivados de la sangre, instalaciones sanitarias, disponibilidad de personal cualificado en logística sanitaria.
f) Salud y aptitud psicofísica de las fuerzas adversarias y propias, al igual que el empleo de antídotos y vacunas.
g) Posible utilización de sistemas de armas NBQ desarrollados por otros países.
h) Capacidad de combate de fuerzas propias y adversarias.
i) Determinar los riesgos de carácter sanitario existentes y los que puedan surgir ante la ocurrencia de un conflicto, para las fuerzas propias, los beligerantes y la población civil.

Entre todas estas áreas de estudio, el asesoramiento proporcionado al mando incluye una estimación de las tasas de enfermedad y de las lesiones no de combate y proporciona información valiosa en el ámbito cívico-militar. Incluye información de un amplio espectro de características de la población local, de la estructura sanitaria local, normativa sanitaria y medioambiental local.

MEDINTEL forma parte de la función conjunta de inteligencia, cumplirá con sus principios, debiendo tener carácter predictivo, ser precisa, oportuna, objetiva y proporciona información clave que será la base para establecer un plan de prevención y protección sanitaria de la fuerza, que englobe las medidas sanitarias preventivas y de profilaxis adecuadas a la situación en el AO desde la preparación de la fuerza, durante la operación y hasta su repliegue a TN. De esta forma, la inteligencia sanitaria contribuye al mantenimiento de la operatividad de la fuerza y a la ejecución de las operaciones (Alsina, 2010).

El requerimiento esencial de la prevención sanitaria es disponer de información de interés sanitario en todas las fases de la operación. La información

debe ser actual, precisa y lo suficientemente dinámica para difundir rápidamente los cambios producidos ante una posible amenaza. Esta información, una vez compilada, integrada, analizada y evaluada, se transforma en inteligencia sanitaria, en la que es fundamental la prevención sanitaria. Después de la información inicial, la situación se evaluará de forma continua durante la operación y se valorará la efectividad de las medidas establecidas, se identificarán nuevas amenazas que puedan causar bajas. Este asesoramiento servirá de guía para la política sanitaria a seguir en la operación. MEDINTEL es, por tanto, un proceso dinámico.

El conocimiento de las características de la zona objeto de estudio tiene importancia incluso cuando no se prevea un conflicto, por cuanto puede facilitar el apoyo y despliegue sanitario en misiones humanitarias, de paz, de interposición, etc.

El apoyo sanitario a la fuerza en ejercicios, operaciones, en el cumplimiento de sus cometidos diarios, incluye actividades orientadas a la prevención de la enfermedad con el objetivo de alcanzar la capacidad operativa necesaria para el cumplimiento de la misión. En los siglos XVII-XVIII se inició el uso de la información estadística en el ámbito sanitario como herramienta para la toma de decisiones a nivel poblacional. Además, se utilizarán sistemas de información que recojan información sobre el estado de salud y sean capaces de detectar variaciones que puedan suponer una alerta. Por su carácter multidisciplinar, el equipo encargado de elaborar los productos de MEDINTEL debe incluir analistas de inteligencia de diferentes especialidades sanitarias fundamentales formados también en inteligencia.

Hoy en día, debido a la rapidez con las que se generan y evolucionan, las situaciones de crisis han reducido considerablemente el tiempo que tradicionalmente se ha dispuesto para llevar a cabo los planeamientos operativos. Por otro lado, la complejidad de los escenarios donde despliegan las tropas exige que desde un primer momento el mando o comandante de una fuerza disponga de una información completa e integral que le permita tomar sus decisiones con el mayor conocimiento posible de la situación, tanto en las fases de planeamiento como en la de conducción de las operaciones. Por ello, se necesita disponer de una inteligencia sanitaria capaz de procesar e integrar toda la información multidisciplinar de forma oportuna, facilitando la toma de decisiones rápidas y preventivas.

Por estos motivos, es necesario contar desde tiempo de paz con un sistema de información, de vigilancia sanitaria capaz de recoger información relacionada con la salud de los efectivos, en TN y desplegados en ZO, capaz de alertar cuanto antes de situaciones que puedan derivar en circunstancias de crisis, evite la sorpresa estratégica y permita decidir e implementar las medidas de control y prevención adecuadas.

Durante la pandemia por coronavirus, Migliore describe cómo el asesoramiento sanitario elaborado por equipos multidisciplinares ha contribuido a la gestión de la crisis sanitaria y a mejorar la protección sanitaria de la fuerza (Migliore, 2021).

5. Inteligencia sanitaria y seguridad nacional

El compromiso de las FAS con la seguridad nacional e internacional hace necesario contar con unos efectivos preparados en y desde TN, para cumplir con los cometidos que se les asignen. Ya se ha expuesto la importancia de contar con información precisa y oportuna, con informes de inteligencia sanitaria que asesore a los mandos, a los decisores, sobre los factores sanitarios que pueden afectar a la salud de las personas, disminuyendo, en general, su efectividad y operatividad, comprometiendo, por tanto, su actuación en defensa de la seguridad nacional.

El compromiso con la seguridad nacional es de todos los sectores del Estado. En el ámbito de la sanidad civil se ha desarrollado el concepto de «inteligencia epidemiológica» o «epidémica» por la Organización Mundial de la Salud (OMS) y el Centro Europeo para el Control de Enfermedades (ECDC) como herramienta para la alerta temprana y verificada en materia sanitaria, ya que es generalizada la preocupación por las amenazas sanitarias a la estabilidad y seguridad de las sociedades, en general.

La OMS considera la inteligencia epidémica como el ciclo de recolección sistemática y organizada, análisis e interpretación de información de todas las fuentes para detectar, verificar e investigar potenciales amenazas. Es un proceso dinámico y rutinario del que son responsables la propia OMS y un conjunto multidisciplinar de profesionales de los Estados miembros.

En España se define la inteligencia epidemiológica (Ministerio de Sanidad) como un «proceso dinámico e interactivo de detección, cribado/filtrado, verificación, análisis, evaluación e investigación de la información de aquellos eventos o situaciones que puedan representar una amenaza para la salud pública». Se ha constituido para ello una red de expertos y centros (investigadores, salud pública, laboratorios de referencia, instituciones académicas, etc.). El objetivo es asesorar de forma ágil fiable y verificada para la toma de decisiones en cuanto a la puesta en marcha de medidas de prevención y control.

La inteligencia epidemiológica se basa, por una parte, en unos indicadores determinados que recogen información de unos sistemas de información y vigilancia estructurados y, por otra, en una vigilancia de los eventos que pueden afectar a la salud pública, previendo diferentes escenarios futuros que tienen en cuenta no solo las consecuencias sanitarias directas de una

situación de crisis sanitaria, sino las indirectas, como son las consecuencias sociales y económicas.

Las fuentes que utiliza para recoger esta información son múltiples y variadas, oficiales y no oficiales, e interconectadas con organizaciones internacionales mediante sistemas de información con acceso restringido.

La inteligencia epidemiológica elaborada por el Ministerio de Sanidad proporciona conocimiento de la situación, predicciones sobre acontecimientos posibles, información relevante e inteligencia oportuna para la toma de decisiones tanto a nivel ministerial como por el Consejo de Seguridad Nacional, cuando sea necesario.

La vigilancia epidemiológica y la inteligencia sanitaria comparten objetivos y metodología y ambas contribuyen al mantenimiento de la Seguridad Nacional en materia sanitaria.

La posibilidad de que agentes biológicos o sus toxinas puedan ser utilizados como armas constituye una posible amenaza para la salud de los ciudadanos y la seguridad nacional. Por ello, se deben disponer mecanismos de intercambio de información e inteligencia entre los distintos centros involucrados y preparados en materia de defensa y seguridad, e incentivar la cooperación cívico-militar en esta materia.

En la actualidad, en el Ministerio de Defensa se realiza inteligencia sanitaria e informes sobre riesgos sanitarios en TN y en ZO por el Instituto de Medicina Preventiva de la Defensa (IMPDEF), centro dependiente de la Inspección General de Sanidad, respondiendo a las peticiones solicitadas por los Ejércitos y por el Centro de Inteligencia de las Fuerzas Armadas (CIFAS), «órgano responsable de facilitar al Ministro de Defensa, a través del JEMAD, y a las autoridades del Departamento, la inteligencia militar precisa para alertar sobre situaciones internacionales susceptibles de generar crisis que afecten a la Defensa Nacional, así como de prestar el apoyo necesario, en su ámbito, a las operaciones militares». El CIFAS incluye productos de inteligencia sanitaria que responden a las NI y a los elementos esenciales de inteligencia del plan de inteligencia militar, en las valoraciones de la amenaza y pone a disposición de los distintos analistas de inteligencia y del mando de operaciones el asesoramiento sobre las amenazas sanitarias en las distintas ZO.

Mediante la participación activa en el Panel OTAN de Inteligencia Sanitaria (MEDINTEL-P), el IMPDEF tiene contacto directo con los distintos países miembro de la Alianza y de los países socios. Se está trabajando en la configuración de un sistema de información interoperable mediante el que se pueda intercambiar información e inteligencia sanitaria entre los distintos países. Además, se revisa en ese panel la doctrina OTAN relativa a

MEDINTEL y se pone en común el enfoque que cada país da a la estructura y elaboración de productos de MEDINTEL.

El Ministerio de Defensa cuenta con un representante, un oficial médico destinado en el IMPDEF, en la Comisión de Salud Pública del Consejo Interterritorial del Sistema Nacional de Salud y en los grupos de trabajo de la Ponencia de Alertas y Planes de Preparación y Respuesta y de la Ponencia de Vigilancia Epidemiológica. Por tanto, Salud Pública del Ministerio de Defensa están en constante contacto con las autoridades sanitarias del Ministerio de Sanidad.

MEDINTEL, además, proporciona asesoramiento especializado en investigaciones y las operaciones de contraterrorismo y contrainteligencia, operaciones de inteligencia nacional enfocadas a asistir y asesorar a líderes políticos o militares para la comprensión de las amenazas nacionales o internacionales. Igualmente, se incluyen actividades de apoyo psicológico operativo a actividades de seguridad nacional e inteligencia militar, así como en la evaluación de amenazas internas para implementar identificación de ámbitos de alto riesgo en poblaciones o individuos que podrían constituir una amenaza interna.

6. Conclusiones

La ESN 2021 establece que la actuación frente a situaciones de crisis debe contar con un sistema de información que recoja y permita el análisis de indicadores de alerta temprana sobre riesgos y amenazas para la seguridad nacional y así facilitar la toma de decisiones.

Las FAS tienen un compromiso para mantener la seguridad nacional e internacional. Como indica Sánchez Gamboa (2016), «la inteligencia en beneficio de la seguridad del Estado ha de ser integral, multidisciplinar, oportuna, colaborativa…». La inteligencia sanitaria puede contribuir a esos compromisos atendiendo a la salud de la fuerza. Para ello, precisa disponer de un sistema de información que identifique las amenazas existentes en el AO, que registre la información relacionada con la vigilancia de los problemas de salud del personal militar, y que permita el análisis de esta información y la generación de conocimiento para la elaboración de informes de inteligencia para el Mando. Mediante la comprensión integral del entorno en el que actuarán los efectivos se podrán implementar las medidas pertinentes de protección sanitaria de la Fuerza, se contribuirá al mantenimiento de la operatividad del personal y a la consecución de la misión.

La ESN 2021 identifica que, entre las medidas de carácter sectorial, la lucha contra las epidemias y pandemias es necesario modernizar el sistema de vigilancia epidemiológica nacional, a partir de las lecciones aprendidas en la gestión de la pandemia de la covid-19. Por tanto, establece que es

necesario actualizar el sistema de vigilancia nacional de salud para permitir una respuesta ágil y acertada.

MEDINTEL necesita disponer de un sistema de alerta temprana moderno, versátil y digitalizado, capaz de procesar e integrar toda la información colaborativa oportunamente, permitiendo una respuesta ágil e interoperable con otros el sistema de sanidad civil y con otros países, mediante la renovación de la tecnología actual que utiliza y el sistema de información. La estrategia digital del Servicio Nacional de Salud se está actualizando para incluir medidas que mejoren la prevención, el diagnóstico, la vigilancia y la gestión de la salud. Sería conveniente actualizar el sistema de información de inteligencia sanitaria militar de manera armonizada con esta estrategia digital macional.

Con el fin de mantener las capacidades militares necesarias para contribuir a la soberanía, a los intereses nacionales e internacionales y actuar de forma autónoma si se dieran las circunstancias, según indica la Directiva de Política de Defensa 2020, es imperioso potenciar las capacidades y las fortalezas propias de la sanidad militar en materia de inteligencia sanitaria.

La preparación del Ministerio de Defensa para afrontar futuras crisis sanitarias incluye la mejora y el refuerzo de las capacidades actuales de sanidad militar y la potenciación de la sanidad operativa. La inteligencia sanitaria es una herramienta más imprescindible para mejorar y reforzar para el apoyo interno y a la población civil.

La mejora de la recogida de la información, utilización de fuentes de información, metodología de análisis, y elaboración de productos de inteligencia sanitaria precisa una formación continuada del personal sanitario y una colaboración estrecha con los analistas de inteligencia del Centro Militar de Inteligencia de las FAS.

Los despliegues actuales —en ejercicios, operaciones, destinos militares— son generalmente multinacionales, son complejos al requerir una estrecha coordinación con fuerzas de otros países. Por esta razón la doctrina en general, y en concreto la sanitaria, incluyendo la referida a la MEDINTEL, ha de ser necesariamente compatible con la doctrina OTAN que constituye el referente indispensable para todos los países, sean o no miembros de la Alianza Atlántica.

El asesoramiento en MEDINTEL es una parte integral del proceso de planeamiento de las operaciones y debe incluirse al inicio de todas las actividades, por lo que precisará tener desde tiempo de paz unas capacidades, medios, preparación, sistemas, herramientas e interoperabilidad necesaria para satisfacer las necesidades operativas y de información. Todos ello se deberá materializar en una arquitectura integral, única y colaborativa, con agilidad suficiente para responder a un entorno en constante evolución y

con capacidad de trabajar al servicio de los niveles estratégico, operacional y táctico, de forma fluida desde tiempo de paz hasta conflicto.

La respuesta nacional a las emergencias se fundamenta en un modelo multisectorial y multidimensional que permite dar una respuesta integral, sea cual sea su origen. La inteligencia sanitaria militar es una herramienta que puede contribuir a la respuesta nacional a la seguridad nacional e enternacional.

Bibliografía

Alsina, J. (2010). La Doctrina de Inteligencia Sanitaria. Concepto y organización. *Sanidad Militar*, 66 (2), pp. 106-111. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/s/rsm_66_2.pdf

Borden Institute. (2003). *Medical threat assessment. Chapter 11. Military preventive medicine: mobilization and deployment. Volume 1*. Uniformed Services University of the Health Sciences. Disponible en: https://medcoe.army.mil/borden-tb-mpm-vol1

Ceberio, M. R. (2021). Las pandemias precedentes a la COVID-19: de la peste de Atenas a la peste rosa. *Ciencias Psicológicas*, 15 (1), e–2555. Disponible en: http://www.scielo.edu.uy/pdf/cp/v15n1/1688-4221-cp-15-01-e2555.pdf

Díaz Martínez, Y. (1998). *La sanidad militar del ejército español en la guerra de 1895 en Cuba*. Instituto de Historia de Cuba - Palacio Aldama. La Habana (Cuba). Disponible en: https://asclepio.revistas.csic.es/index.php/asclepio/article/view/356/354

ECDC. (2021). ECDC activities on epidemic intelligence and outbreak response. *European Center for Disease Control*. Disponible en: https://www.ecdc.europa.eu/en/about-us/what-we-do/ecdc-activities-epidemic-intelligence-and-outbreak-response

González-Hernández, M. (2017). El tifus epidémico. Prevención y tratamiento a través de la historia. *Medicina Preventiva*, 22 (3), pp. 37-44.

Headquarters Department of the Army. (1989). Medical intelligence in a theater of operations. *Field Manual* No. 8-10-8. Washington, DC, 7 (July). Disponible en: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1087&context=dodmilintel

Interpol. Bioterrorismo. Disponible en: https://www.interpol.int/es/Delitos/Terrorismo/Bioterrorismo

Instituto Español de Estudios Estratégicos. (2022). *Documento de investigación 05/2022. Estrategias de Seguridad*. Centro Superior de

Estudios de la Defensa Nacional. Disponible en: https://www.ieee.es/Galerias/fichero/docs_investig/2022/DIEEEINV05_2022_EstrategiasdeSeguridad.pdf

Kaufman, DC. (2001). *Medical Intelligence: a theatre engagement tool. Strategy research Project.* USA. Defense Intelligence Agency.

Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional. Disponible en: https://www.boe.es/eli/es/lo/2005/11/17/5/con

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10389#:~:text=Esta%20ley%20tiene%20por%20objeto,c)%20La%20gesti%C3%B3n%20de%20crisis

Migliore, L., Hopkins, D., Jumpp, S., Brackett, C., Cromheecke, J.. (2021). Medical Intelligence Team Lessons Learned: Early Activation and Knowledge Product Development Mitigate COVID-19 Threats. *Military Medicine*, vol. 186, September/October Supplement.

Ministerio de Defensa. *Centro de Inteligencia de las Fuerzas Armadas (CIFAS)*. Disponible en: https://emad.defensa.gob.es/unidades/cifas/

Ministerio de Defensa. (2007). *Manual de Medicina Preventiva en operaciones*. Instituto de Medicina Preventiva de la Defensa «Capitán Médico Ramón y Cajal».

Ministerio de Defensa. (2020). Directiva de Política de Defensa 2020. *Boletín Oficial del Ministerio de Defensa*. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-politica-Defensa-2020.pdf

Ministerio de Defensa. (2020). *Publicación Doctrinal Conjunta. PDC-2 Doctrina de Inteligencia para las Fuerzas Armadas*. Estado Mayor de la Defensa.

Ministerio de Defensa. (2021). *Concepto de Empleo de las Fuerzas Armadas 2021*. Estado Mayor de la Defensa. Disponible en: https://emad.defensa.gob.es/Galerias/emad/files/CEFAS_2021.pdf

Ministerio de Defensa. (2021). *Publicación Doctrinal Conjunta PDC-4.10 Doctrina Sanitaria en Operaciones*. Estado Mayor de la Defensa. Ministerio de Defensa. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/PDC-4-10_Doctrina_Sanitaria_en_Operaciones.pdf

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. (2021). *Estrategia de Seguridad Nacional 2021*. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

Ministerio de Sanidad. ¿Qué es la inteligencia epidemiológica? Disponible en: https://www.sanidad.gob.es/profesionales/saludPublica/ccayes/inteligenciaepidemiologica/inteEpid.htm#:~:text=Se%20define%20como%20inteligencia%20epidemiol%C3%B3gica,amenaza%20para%20la%20salud%20p%C3%BAblica

NATO Standard AJMedP-3. (2020). *Allied Joint Medical Doctrine for Medical Intelligence Edition A, version 2*. Disponible en: https://www.coemed.org/files/stanags/02_AJMEDP/AJMedP-3_EDA_V2_E_(1)_2547.pdf

NATO Standards Related Document SRD-1 to AJMedP-3. (2020). *Guide To Medical Intelligence. Edition A, version 1*. Disponible en: https://www.coemed.org/files/stanags/02_AJMEDP/SRD-1_to_AJMedP-3_EDA_V1_E_(4)_2547.pdf

Organización Mundial de la Salud/ Organización Panamericana de la Salud. *Inteligencia Epidémica*. Disponible en: https://www.paho.org/es/temas/inteligencia-epidemica

Presidencia de Gobierno. (2020). *Directiva de Defensa Nacional 2020*. Gobierno de España. Disponible en: https://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2020.pdf

Sánchez Gamboa, J. (2016). Ideas fundamentales sobre inteligencia. Inteligencia. Un enfoque integral. *Monografías 148*. Escuela Superior de las Fuerzas Armadas.

El proceso IRM&CM en el Ejercicio JFX-22: las claves del éxito

Álvaro Álvarez Álvarez
Francisco Javier López Cuevas
Pablo Caneda López

Resumen

En el actual contexto impredecible, las organizaciones necesitan disponer de información oportuna y veraz que les permita avanzar hacia sus objetivos, siendo para ello indispensable una buena gestión de los medios encaminados a la obtención de información.

Las capacidades y el modo de empleo de estos medios están afectados por la irrupción de las nuevas tecnologías, y la adaptación a este tipo de herramientas y sistemas es también imprescindible para generar la inteligencia necesaria.

La estructura operativa de las Fuerzas Armadas no es ajena a estos desafíos, y periódicamente, se adiestra para adaptar sus procedimientos y sistemas al presente.

Durante la realización del ejercicio JFX 23, y ciñéndonos al ámbito de la inteligencia, se ha puesto en práctica procedimientos basados en herramientas informáticas que mejoran la eficiencia en la gestión de la obtención, dentro de una estructura de servidores descentralizados y sincronizados entre sí, que garantizan la conectividad permanente entre los distintos nodos con participación en el proceso IRM & CM, dando muestras de que la aplicación de nuevas tecnologías agiliza los procesos y mejora la eficiencia en la gestión de los medios ISR, habitualmente escasos y muy demandados.

Palabras clave

Gestión de la obtención, nuevas tecnologías, aplicaciones, herramientas informáticas, eficiencia.

The IRM&CM process in Exercise JFX-22: the keys to success

Abstract

In the current unpredictable context, it is necessary for organisations to have timely and truthful information that allows them to move towards their objectives, and for this to happen, good management of the means of obtaining information is indispensable. The possibilities and uses of

these media are affected by the emergence of new technologies, and it is also necessary to adapt to these types of tools and systems in order to generate the necessary information.

The operational structure of the armed forces is no stranger to these challenges, and is regularly trained to adapt its procedures and systems to the present.

During the JFX 23 exercise, and in the field of intelligence, procedures were implemented based on computer tools that improve the efficiency of procurement management, within a decentralised and synchronised server structure that ensures permanent connectivity between the different nodes involved in the MRI & CM process, demonstrating that the application of new technologies streamlines processes and improves efficiency in the management of ISR media, which are usually scarce and in demand.

Keywords

Procurement management, new technologies, applications, computer tools, efficiency.

> *«El mundo está cambiando rápidamente. Lo grande no golpeará más a lo pequeño. Será lo rápido lo que golpee a lo lento».*
>
> *Rupert Murdoch*

Así, citando al magnate australiano Rupert Murdoch, director ejecutivo de FOX News, podríamos definir un contexto geopolítico actual sujeto a cambios súbitos y difíciles de detectar, cambios que generan amenazas provenientes de distintos ámbitos, algunos ya conocidos y otros aun sin explorar.

La ya casi olvidada pandemia, la reciente invasión de Ucrania, la irrupción en el escenario mundial de nuevas potencias como China, la inestabilidad generalizada en el continente africano y los efectos del controvertido cambio climático, son algunos ejemplos claros que ilustran una realidad incierta generadora de amenazas en el futuro.

La actualidad demuestra que sin una aparente relación causa y efecto, un pequeño suceso singular puede desencadenar grandes consecuencias.

Las organizaciones supranacionales, los países, las empresas..., en definitiva, las organizaciones de cualquier índole y entidad, están hoy en día sujetas a cambios continuos y a un elevado nivel de incertidumbre.

La irrupción de las nuevas tecnologías, la hiperconectividad generada en entornos digitales, o el fenómeno de la sobreinformación, propician la aparición incluso de nuevos dominios más allá de los físicos en los que toda organización debe desenvolverse.

Estos nuevos factores afectan a todos procesos dentro de una organización, enfrentándola inexorablemente a un proceso de adaptación.

La estructura operativa de las Fuerzas Armadas no es ajena a estos desafíos, incluso, podemos afirmar que debe ser pionera en estrategias de adaptación, ya que difícilmente podrá hacer frente a nuevas e impredecibles amenazas basando su modo de funcionamiento en estructuras y procedimientos obsoletos o demasiado rígidos.

En el ámbito de la inteligencia, las nuevas tecnologías diversifican los medios de obtención y gestión de la información, constantemente aparecen nuevas plataformas más capaces, y herramientas que mejoran la conectividad, obligando a las organizaciones a familiarizarse con la gestión de esas nuevas tecnologías, y a hacer esfuerzos en su implantación.

Dentro de este contexto, durante los días 15 a 25 de noviembre de 2022, tuvo lugar el ejercicio JFX-22, donde la estructura operativa de las Fuerzas Armadas se ha adiestrado en el planeamiento y conducción de una operación de alta intensidad frente a una amenaza no compartida.

Contemplado dentro de la Directiva 13/21 del JEMAD, de 3 de junio, de Planeamiento de Ejercicios (DPE) para el año 2022, el JFX-22 es un Ejercicio Conjunto de Puestos de Mando (CPX) de nivel Operacional y Táctico.

Repartidos a lo largo de la geografía española, han participado el Mando de Operaciones (MOPS), los diversos mandos componentes (Terrestre, Marítimo, Aéreo, operaciones Especiales, Ciberespacio) y el Centro de Inteligencia de las Fuerzas Armadas (CIFAS).

Figura 1. Joint Operation Center del MOPS durante la realización del JFX 22

Dentro del ámbito de la inteligencia, y como parte de los objetivos de adiestramiento a alcanzar durante el ejercicio, era necesaria la definición y puesta en práctica de unos procedimientos agiles, para una correcta explotación de los medios de obtención mediante la ejecución de las funciones IRM&CM «Collection Management», gestión de RFI del nivel operacional.

No menos necesario era el establecimiento de una arquitectura que permitiera gestionar de forma eficiente la utilización de esos medios ISR a disposición de la operación.

Atendiendo a ambos objetivos de adiestramiento, el éxito alcanzado en la gestión de la obtención, obedece a la sinergia generada por dos factores: unos procedimientos flexibles, y un entorno facilitador del uso práctico de las herramientas de la suite SAPIIEM[1].

[1] SAPIIEM: Sistemas de Apoyo a la Interoperabilidad ISR Española Militar.

Con respecto a los procedimientos puestos en práctica, se ha establecido entre el MOPS y los mandos componentes a través de sus correspondientes secciones de inteligencia, una adecuada coordinación en los niveles operacional y táctico de esta gestión, que ha resultado clave para que el proceso IRM&CM[2] se haya desarrollado satisfactoriamente.

Esta dinámica de trabajo establecida entre el MOPS y los mandos componentes para la gestión de la obtención en el proceso JISR[3] tanto en la fase previa como durante la ejecución del JFX-22, ha facilitado el desarrollo de los procedimientos marcados para trabajar de forma eficiente. El uso coordinado de herramientas de trabajo colaborativo y un ritmo de batalla interno flexible, donde ha contemplado para el grupo de trabajo y para la preparación de la JCMB[4] varias vías de participación y aportación, ha permitido un nivel óptimo en el flujo del trabajo de las células encargadas del planeamiento y asignación de tareas dentro del proceso TCPED, planeamiento de tareas, obtención, tratamiento, explotación y difusión.

A nivel estructural, la piedra angular para toda la gestión IRM&CM ha sido, sin duda, el uso de las herramientas que conforman la suite SAPIIEM.

SAPIIEM, es un conjunto de herramientas de desarrollo nacional, dentro del marco del programa multinacional MAJIIC/MAJIIC2 (Multi-Intelligence All-Source Joint Intelligence Surveillance And Reconnaissance Interoperability Coalition), un entorno de trabajo colaborativo entre distintos países aliados, que pretende maximizar la utilidad militar de los nuevos recursos de

[2] Proceso IRM&CM (Intelligence Requirement Management and Collection Management Process). Este proceso asegura que las necesidades de Inteligencia (IR) son contestadas mediante el uso efectivo de todos los medios disponibles. Este proceso desarrolla dos funciones diferenciadas: IRM (gestión de las necesidades de Inteligencia) y CM (gestión de la obtención de información). Ambas funciones podrán fusionarse en una sola denominada IRM&CM que, en estos casos, se desarrollará igualmente como un proceso único. El proceso IRM&CM, implementado en todos los niveles, resulta vital para el correcto desarrollo del ciclo de Inteligencia.

[3] El Proceso JISR es el mecanismo por el cual el medio ISR más apropiado satisface en tiempo y forma una necesidad de obtención del ciclo de inteligencia o de los ciclos de operaciones y targeting.

[4] Junta Conjunta de Coordinación de la Obtención (Joint Collection Management Board, JCMB). La JCMB tiene como finalidad lograr una mayor optimización en el empleo de los medios ISR entre los diferentes niveles de mando y dar solución a aquellas necesidades de obtención (Collection Requirement, CR) que no hayan podido ser atendidas directamente con los medios disponibles, no haya sido posible la coordinación por otros medios, o porque existe conflicto en la gestión del empleo del medios ISR disponibles. En ella se coordina, prioriza, asigna y distribuye las responsabilidades de ejecución y se resuelven posibles conflictos, para lo cual, se precisará visibilidad de todas las CR generadas y validadas de los mandos subordinados. Para sus labores preparatorias y de gestión, la JCMB se apoyará en un equipo de trabajo (JCMWG). En ella participarán todos los elementos que se considere necesario para las actividades JISR (inteligencia, planes, operaciones, EW, IMINT, SIGINT, HUMINT, *targeting*, etc.).

inteligencia, vigilancia, adquisición de blancos y reconocimiento. La misión del citado programa MAJIIC es describir, desarrollar y demostrar procesos y herramientas interoperables, que agilicen y hagan eficiente la gestión y acceso a un amplio espectro de datos ISR procedentes de un amplio rango de sistemas.

Los desarrollos nacionales que conforman la mencionada suite SAPIIEM y que han estado a disposición de los participantes en el JFX22 son:

La herramienta ATENEA (IRM&CM Tool) que proporciona soporte a los *Collection Managers* en la planificación de la inteligencia, obtención y explotación; y a los *ISR Managers* en la ejecución de tareas de obtención/explotación para todos los niveles de conducción, en un entorno distribuido y colaborativo de acuerdo a principios de interoperabilidad, IRM para canalizar la información, y gestionar el ICP (Intelligence Collection Plan).

SEISMO (Multi-Int Exploitation Tool), que comparte datos procedentes de múltiples fuentes de información en diferentes formatos, y proporciona a los analistas de inteligencia herramientas para elaborar inteligencia útil y apropiada para todos los niveles de conducción.

SIERRA TOOLS es un conjunto de clientes web que permite una integración flexible en el ciclo JISR de aquellas unidades o personal que no tiene un acceso completo a estaciones IRM&CM y que son, por tanto, usuarios desventajados. En definitiva, permite un acceso Web remoto al CSD-Sierra.

CSD SIERRA (Coalition shared JISR data, interfaces and services), nodos que actúan como repositorios, que incluyen además interfaces que permiten el acceso a la información, su difusión, y otorgan la capacidad de interactuar durante los procesos del ciclo JISR.

Durante la realización del ejercicio JFX 22 se han utilizado en mayor o menor medida todas las herramientas citadas, siendo especialmente destacables los avances en la utilización de la herramienta de gestión IRM&CM ATENEA, y la creación de una estructura basada en los CSD (Coalition Share Database), desplegados de forma descentralizada, con varios servidores sincronizados entre sí.

Gracias a esta estructura, los gestores de la obtención han dejado atrás primitivas formas de trabajar, tanto en el planeamiento, como en la asignación de tareas ISR, que necesitaban completar el proceso con la difusión y alimentación del ICP con métodos más rudimentarios que implicaban un incremento en los tiempos de gestión ralentizando los procesos. La suite permite un control de la trazabilidad y accesibilidad, y un acceso al ICP que es alimentado con los productos fruto de las tareas ordenadas tras su sincronización.

Otro aspecto no menos importante y necesario para alcanzar el éxito ha sido contar con operadores formados durante las semanas previas a la fase de ejecución, en el uso de las herramientas y aplicaciones, estos operadores

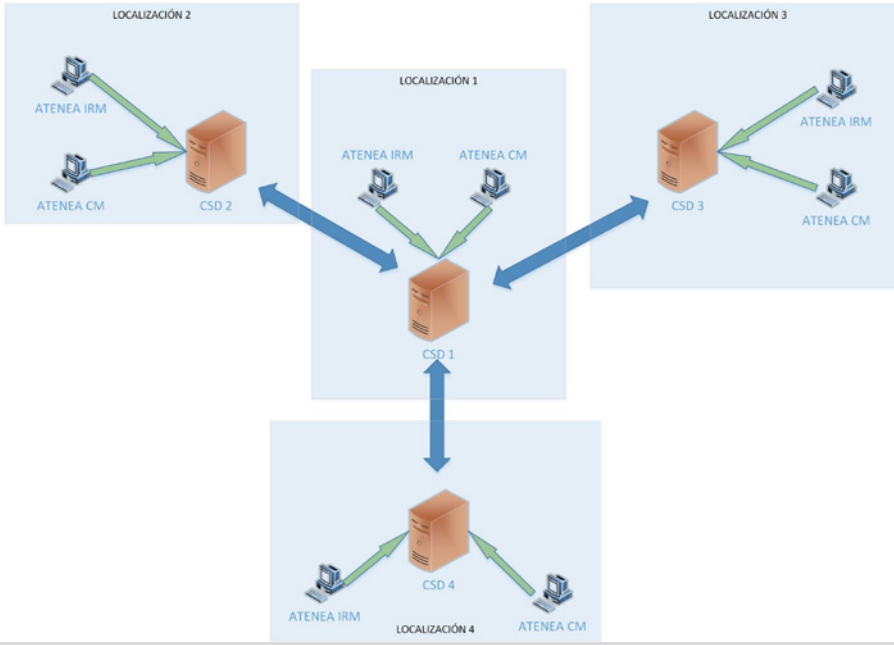


Figura 2. Esquema del despliegue descentralizado de los servidores CSD

han sido apoyados desde el MOPS, buscando siempre un enfoque eminentemente práctico y reiterativo en las tareas a realizar.

Es por ello que se decidiera convocar unas jornadas donde se estandarizaran unos criterios base de trabajo para fluir en la misma dirección, repercutiendo de forma directa en la reducción de tiempos en los procesos de IRM&CM al hacer más hincapié en los planeamientos *ad hoc* y dinámico dado que, si bien, la teoría estaba asentada, quedaba pendiente pulir la parte práctica con la herramienta, cuestión que se desarrolló de manera satisfactoria gracias, sobre todo, al bajo número de incidencias CIS.

Cabe destacar, que la utilización durante un ejercicio de estas características de herramientas en vías de implantación, donde aún cabe el refinamiento, supone a todas luces un valor añadido. Es en el adiestramiento donde la detección de posibles carencias o la identificación de mejoras en su uso cobran sentido.

Una vez finalizado el ejercicio, analizados los trabajos realizados durante la preparación, y extraídas las lecciones aprendidas durante la ejecución del ejercicio, se obtienen las siguientes conclusiones:

El establecimiento de una dinámica de trabajo flexible entre los niveles operacional y táctico, haciéndolo de una forma coordinada y colaborativa con un ajustado ritmo de batalla interno para IRM&CM, ha permitido optimizar tiempos en planeamiento y asignación de tareas en el ciclo JISR. Por un

lado, durante el planeamiento deliberado en la gestión del JCMWG previo a la JCMB diaria. Por otro, la gestión de cambios *ad hoc* y dinámicos que emergieron en el transcurso del ejercicio.

La utilización de la suite SAPIIEM para gestionar la interrelación del nivel operacional y el táctico dentro del proceso IRM&CM supone un paso de gigante que deja atrás métodos de control primitivos para actualizaciones del ICP y trazabilidad del proceso JISR.

El despliegue descentralizado de los CSD sincronizados entre sí garantiza la conectividad y la continuidad en los trabajos entre los distintos nodos.

Respecto a ATENEA, a pesar de tratarse de una herramienta aún sin implementar, la base del éxito ha sido el establecimiento de unas jornadas de formación y unificación de criterios buscando que el usuario automatizara las tareas con el fin de llegar al comienzo del ejercicio con altos niveles de rendimiento sobre la suite a pesar de las incidencias que pudieran surgir.

Poder instruir al personal en una fase previa a la ejecución del ejercicio en el empleo de las diversas herramientas a utilizar, agiliza al máximo todos los procesos que se desarrollan, obtener un mayor rendimiento en lo referente al adiestramiento, e identificar mejoras en los sistemas ya implantados o en vías de desarrollo.

Una estructura eficiente, un *software* de gestión actualizado, un personal familiarizado con el funcionamiento de la organización, y que cuente con el adiestramiento necesario en el empleo de las herramientas a su disposición, son las claves de una gestión eficiente de los medios de obtención, y un manejo oportuno de la información obtenida, las claves del éxito del proceso IRM&CM.

Inteligencia económica: un reto para España y sus empresas

Jesús Antonio Vicente Montaña

Resumen

Actualmente, debido a los rápidos cambios que se están produciendo en un mundo cada vez más interconectado, se está incrementando la conciencia sobre la importancia de la inteligencia como elemento mitigador de la incertidumbre que producen estos cambios tan súbitos.

Las empresas y la economía no escapan a esta incertidumbre y a la velocidad en la que se producen los cambios en los mercados. A pesar de ello, España aún no ha desarrollado una arquitectura de inteligencia económica que apoye a sus empresas a la hora de mitigar la incertidumbre en la toma de decisiones. Otros países de nuestro entorno, sí lo han hecho, quedando como asignatura pendiente para nuestro entramado empresarial.

Palabras clave

Libro Verde, Martre, Carayon, estrategia.

Economic intelligence: a challenge for Spain and its companies

Abstract

Today, with the rapid changes taking place in an increasingly interconnected world, there is a growing awareness of the importance of intelligence as an element in mitigating the uncertainty created by such sudden changes.

Businesses and the economy are not immune to this uncertainty and the speed at which markets change. Despite this, Spain has not yet developed an economic intelligence architecture to help its companies reduce uncertainty in decision-making. Other neighbouring countries have done so, but this remains an unresolved issue for our business fabric.

Keywords

Green Book, Martre, Carayon, strategy

1. Introducción

En diciembre de 1995, la Comisión Europea aprobó el Libro Verde sobre la innovación (Comisión Europea, 1995). Con esta iniciativa, la Comisión pretendía fomentar un amplio debate que sensibilizase a los agentes económicos acerca de la necesidad imperativa de innovar para consolidar la competitividad, contribuir al crecimiento y mejorar las perspectivas de empleo en Europa.

Posteriormente, en la sesión del 12 de febrero de 1996 del Parlamento Europeo, su presidente, Klaus Hänsch, anunció que había remitido el Libro Verde para su examen a la Comisión de Investigación, Desarrollo Tecnológico y Energía. La Comisión aprobó el Libro Verde y el proyecto de Resolución, en su reunión del 7 de mayo de 1996[1].

El planteamiento global de la innovación utilizado en el Libro Verde, aporta como corolario la inteligencia económica, «un útil estratégico de ayuda a la toma de decisiones en un contexto de mundialización de los intercambios y de aparición de la sociedad de la información».

La Comisión Europea define este concepto, inteligencia económica, como el «conjunto de las acciones coordinadas de investigación, tratamiento y distribución, con objeto de la explotación de la información útil a los protagonistas económicos». En ella se incluye también la protección de la información considerada sensible para la empresa.

Reconoce las carencias existentes: «el dinamismo en la recogida de información estratégica, su difusión (cooperación entre empresas, conjugación de recursos con los poderes públicos) y su protección no están todavía suficientemente generalizados en Europa». Y los problemas para su aplicación: «Las diferencias sociales y profesionales, el temor a la competencia y el secretismo hacen difícil la colaboración entre empresas y administraciones. Por ello, es importante que cambien las actitudes individuales y colectivas para que se desarrolle el recurso a la inteligencia económica».

La Comisión establecía las acciones a desarrollar. Entre ellas, algo muy parecido al espionaje industrial: «Reforzar la experiencia científica de algunas delegaciones de la Comisión en terceros países para que realicen una misión de alerta tecnológica y proporcionen a la Unión Europea análisis sobre la evolución de la investigación en el extranjero». Y una que no pasó de boceto: «podría lanzarse la licitación de un proyecto destinado a hacer inventario de lo ya existente y a definir las especificaciones de un sistema experto multilingüe de navegación en las vastas fuentes de información utilizando técnicas multimedia y determinar su viabilidad y costes». Dos años

[1] Parlamento Europeo. (1996). *Sobre el Libro Verde de la Innovación*. Disponible en: https://www.europarl.europa.eu/doceo/document/A-4-1996-0165_ES.html?redirect

después de la publicación del Libro Verde, en septiembre de 1998, se fundaba la compañía Google.

2. Exposición

2.1. *Los antecedentes del Libro Verde. Los informes Martre y Carayon*

Las instituciones comunitarias hacen suyo y definen por primera vez para un ámbito supranacional, un concepto que ya había sido ampliamente tratado por el grupo de trabajo presidido por Henri Martre (presidente de la Asociación Francesa de Normalización (AFNOR) y presidente de honor de la empresa estatal Aérospatiale). El que se conoce como Informe Martre (Martre, s. f.), lleva el título de Intelligence économique et stratégie des entreprises. Publicado en febrero de 1994, obedece al encargo realizado por el Commissariat général du Plan, un organismo asesor que informaba al gobierno de Francia.El informe destaca «la importancia de la inteligencia económica como herramienta para la comprensión de la reorganización de las economías de terceros países, que es esencial para la definición de estrategias industriales adaptadas, reactivas y eficaces».

Reconoce que la gestión estratégica de la información económica se ha convertido en uno de los motores esenciales del rendimiento global de las empresas y las naciones. Así, afirma que:

> El proceso de globalización de los mercados obliga a los agentes económicos a adaptarse a los nuevos equilibrios que se establecen entre competencia y cooperación. A partir de ahora, la conducción de las estrategias industriales se basará en gran medida en la capacidad de las empresas para acceder a la información estratégica para anticipar mejor los mercados futuros y las estrategias de los competidores (Martre, 1994).

Para un Estado con importantes empresas públicas[2], como era el francés, su defensa era un objetivo de primer orden (Comín *et al*., 2006).

A este primer informe le siguió la creación de escuelas de guerra económica. En 1997, el general Pichot-Duclos, exdirector de la Escuela de Inteligencia Conjunta (EIREL), crea con Christian Harbulot l'Ecole de Guerre Economique.

En julio de 2003, el Informe Carayon (Intelligence économique, compétitivité et cohésion social) (Carayon, 2003), elevaba 38 propuestas dirigidas al primer ministro, entre ellas la de crear una estructura que coordinara no solo los actores públicos, sino también los privados. A partir de este

[2] En 1990, la incidencia de las empresas de titularidad pública en relación PIB corriente era en Francia del 15,1%. El mayor de las principales economías europeas (Alemania 10%; Italia 11,5%; Reino Unido 4%).

informe, Francia ha sido el país que ha liderado la inteligencia económica en el ámbito europeo e internacional (Mora, 2016).

Francia es un ejemplo relevante de país donde el Estado apoya a las grandes empresas locales mediante sus servicios de inteligencia. Además, destaca por la transferencia de conocimiento desde la comunidad de inteligencia al ámbito privado a través de la creación de organizaciones y programas de formación que se han nutrido de la experiencia de antiguos miembros de los servicios de inteligencia. Dicho proceso ha permitido la generación de un pensamiento propio y original en materia de inteligencia económica[3].

2.2. La estrategia española de seguridad: un intento frustrado de inteligencia económica en España

En el resumen ejecutivo de la Estrategia de 2011, refiriéndose a la amenaza denominada Inseguridad Económica y Financiera se establece que:

> Las amenazas y riesgos relacionados con la actividad económica y financiera pueden tener su origen en factores como los desequilibrios macroeconómicos, públicos o privados, la volatilidad de los mercados, la actuación desestabilizadora, especuladora e incluso ilegal de diversos agentes, la deficiente actuación de los organismos supervisores y reguladores, la interdependencia económica, la competencia por los recursos o un modelo de crecimiento desequilibrado.

En lo referente a la inteligencia económica hay que destacar que su inclusión está muy condicionada por el momento en el que se elabora y revela una gran preocupación e inconcreción[4]. Hay que recordar que el documento fue elaborado en pleno impacto de la crisis económica que había comenzado en 2008.

A mayor abundamiento sobre cómo incidió la crisis en los contenidos del documento, recordar que, en la Estrategia Europea de Seguridad, publicada en 2009, con Javier Solana como secretario general del Consejo de la UE y alto representante de la Política Exterior y de Seguridad Común, es decir, con una participación muy destacada en su elaboración, no se menciona el término inteligencia económica[5].

---

[3] Rodríguez y Pérez. (2019). El Estado francés y la inteligencia económica. *Blog de Tarlogic*. Disponible en: https://www.tarlogic.com/es/blog/el-estado-frances-y-la-inteligencia-economica/

[4] Hispán, P. (2011). La primera Estrategia de Seguridad. *El País* (28 julio). Disponible en: https://elpais.com/diario/2011/07/28/opinion/1311804013_850215.html

[5] Hispán, P. (2011). La primera Estrategia de Seguridad. *El País* (28 julio). Disponible en: https://elpais.com/diario/2011/07/28/opinion/1311804013_850215.html

La enumeración de los variados factores da a entender que se pretende hacer una enmienda a la totalidad del sistema financiero, los organismos reguladores y los instrumentos de apoyo y análisis de los que disponía el Gobierno de España. Todos ellos fueron incapaces de anticipar lo sucedido. Cabe preguntarse si un organismo más, un sistema de inteligencia económica, hubiese tenido mayor capacidad de análisis y prevención que el Banco de España, los servicios de estudios de las entidades financieras o la propia Oficina Económica de la Presidencia del Gobierno y los servicios del Ministerio de Economía. Sin mencionar la supuesta capacidad de análisis en la materia de los servicios de inteligencia.

Las propuestas de actuación son tan amplias como imprecisas:

> La prevención como la mitigación de sus efectos requiere luchar contra las actividades delictivas, asegurar una correcta supervisión y regulación de los mercados, avanzar en la gobernanza económica europea y global, potenciar la presencia internacional de España, garantizar el funcionamiento de los servicios e infraestructuras críticos económicos y financieros, y promover un desarrollo económico sostenible que minimice los desequilibrios y garantice el crecimiento económico y la cohesión social (ESN, 2011).

Para tan ambiciosos objetivos y con el fin de analizar la información relevante y facilitar la acción del Estado, se creará un Sistema de Inteligencia Económica (SIE).

Con razón, afirma el general de División D. Valentín Martínez Valero, primer director del Centro de Inteligencia de las Fuerzas Armadas (CIFAS), que no hay ningún lugar del documento donde se proporcione una clara definición de lo que se entiende por inteligencia económica (Martínez, 2017).

Esa concatenación de conceptos que superaban ampliamente el ámbito de una Estrategia de Seguridad de un Estado: «la volatilidad de los mercados, los desequilibrios macroeconómicos» etc. Así como la inconcreción de su objetivos y mecanismos de actuación, la convirtieron en un propósito fallido[6] y en el nonato Sistema de Inteligencia Económica». (ESN, 2011).

[6] «Se establecerá un Sistema de Inteligencia Económica (SIE) con la misión de analizar y facilitar información económica, financiera y empresarial estratégica relevante, oportuna y útil para apoyar la acción del Estado y una mejor toma de decisiones. Este sistema permitirá compartir conocimiento, crear sinergias, evitar duplicidades y facilitar la adopción de posiciones comunes en las administraciones públicas. En estrecha relación también con los diferentes actores económicos, contribuirá a las labores de seguridad del Estado, facilitando la detección y prevención de actuaciones contrarias a los intereses económicos, financieros, tecnológicos y comerciales de España en sectores estratégicos» (ESN, 2011: 58).

Así, en la actualización de la Estrategia de Seguridad Nacional correspondiente al año 2013, al SIE se le considera una herramienta de apoyo: «Fomento de los mecanismos de coordinación adecuados que permitan el desarrollo de la seguridad económica y de sus herramientas de apoyo como, por ejemplo, el Sistema de Inteligencia Económica (SIE)». Por el contrario, lo que se pretende es fortalecer los mecanismos existentes. «Refuerzo de los actuales mecanismos de regulación y supervisión, para conseguir que su labor sea efectiva y se eviten crisis sistémicas» (ESN, 2013).

Por último, en la Estrategia de 2021 no hay mención alguna ni al sistema ni al concepto.

3. Conclusiones: una demanda reiterada

Este hipotético como necesario SIE español debería disponer, asimismo, según algunos autores, de un comité conformado por los principales grupos de interés afectados, entre los que se contarían todos los departamentos ministeriales, cuyas competencias tengan que ver con seguridad, economía o empresa, así como aquellas asociaciones e instituciones de apoyo a las empresas, los sindicatos, las asociaciones de españoles en el extranjero, las universidades y los centros de investigación. En 2019, el presidente de honor del Club de Exportadores e Inversores Españoles y el subdirector de la Escuela de Inteligencia Económica firmaban un artículo en el que exponían la composición del órgano del SIE español.

Sus funciones serían analizar las prioridades de las solicitudes recibidas, en función de su peso en la seguridad económica, y proceder a formular las correspondientes respuestas. Con este modelo, cualquier empresa española que tuviese una necesidad de inteligencia, pero no pudiera afrontarla con sus recursos, podría recurrir al SIE para canalizar su preocupación y obtener de este un análisis válido para su sector en concreto, y también para la reputación del país y sus intereses estratégicos.

De este modo tendría una capacidad operativa: «En relación con la operativa y el tratamiento de la información, su realización bajo los procedimientos del CNI, dada su experiencia en la obtención, análisis y difusión de la información confidencial, supondría una notable garantía de éxito, lo mismo que contar con un personal multidisciplinar conformado por analistas de inteligencia y economistas con décadas de experiencia empresarial. De este modo se combinaría la gestión de la información con el conocimiento de la ciencia económica y empresarial»[7].

[7] Prieto, B. e Izquierdo H. (2009). *España necesita un sistema de inteligencia económica.* Disponible en: https://clubexportadores.org/espana-necesita-un-sistema-de-inteligencia-economica-por-balbino-prieto-y-hector-izquierdo-el-economista/

Leyendo esto, se puede comprender por qué se decidió suprimir de la ESN en 2021. La inoperancia del organismo hubiera sido estudiada en las escuelas de negocio. En la actualidad, la Inteligencia Económica en España es básicamente una disciplina circunscrita al ámbito académico, en el que proliferan los estudios y las academias o cursos específicos.

Bibliografía

Carayon, B. (2003). Intelligence économique, compétitivité et cohésion sociale: rapport au Premier ministre. *La Documentation francaise*, Paris.

Comín, F., Clifton, J. y Díaz D. (2006). La privatización de empresas públicas en la UE: ¿la vía británica o la senda europea? *Revista de Economía Mundial*, 15, pp. 121-153.

Comisión Europea. (1995). Libro Verde sobre la Innovación. *Boletín de la Unión Europea*. Suplemento 5/95.

Gobierno de España. (2011). *Estrategia Española de Seguridad*. Gobierno de España.

Gobierno de España. (2013). *Estrategia de Seguridad Nacional*. Gobierno de España.

Martínez, V. (2017). *Inteligencia económica, tecnológica y logística. Una visión transversal de la seguridad. Documentos de Seguridad y Defensa 74*. Madrid. Instituto Español de Estudios Estratégicos. P. 12. Disponible en: https://www.ieee.es/publicaciones-new/documentos-de-trabajo/2017/Doc_SegyDef_74.html

Martre, H. (1994). *Informe Martre*.

Mora, J. A. (2016). *Inteligencia económica y Fuerzas Armadas: ¿una simbiosis necesaria?* Instituto Español de Estudios Estratégicos. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5992461

Valero, V. (2017). La inteligencia económica en la Estrategia de Seguridad Nacional. *Blog Inteligencia Empresarial*.

La función de inteligencia en emergencias

Juan Soriano Paradinas

Resumen

Una de las misiones que asigna la Ley Orgánica 05/2005, de la Defensa Nacional, a las Fuerzas Armadas es el deber de preservar la seguridad y bienestar de los ciudadanos en los supuestos de grave riesgo, catástrofe, calamidad u otras necesidades públicas.

A través del Real Decreto 372/2020, de 18 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, la Unidad Militar de Emergencias (UME) tiene la misión de intervenir en cualquier lugar del territorio nacional y en el exterior, para contribuir a la misión indicada en el párrafo anterior, además de poder participar en las operaciones militares que se determinen, según recoge la normativa actualmente en vigor.

La existencia de la inteligencia en emergencias no solo obedece a razones de metodología en el planeamiento de las intervenciones, sino a que, para poder proporcionar rapidez de respuesta, es necesario: analizar los riesgos que van a provocar las catástrofes, a las que no es posible anticiparse en la mayoría de las ocasiones y donde el factor tiempo es de vital importancia; monitorizar la situación de manera permanente y disponer de unos indicadores de alerta que permitan determinar la probabilidad de intervención de la UME.

Palabras clave

UME, riesgo, información, catástrofe, Fuerzas Armadas.

The intelligence function in emergencies

Abstract

One of the missions assigned to the Armed Forces by Organic Law 05/2005 on National Defence is to ensure the safety and well-being of citizens in cases of serious risk, disaster, calamity or other public need. By Royal Decree 372/2020, of 18 February, which establishes the basic organisational structure of the Ministry of Defence, the Military Emergency Unit (UME) has the mission to intervene anywhere in the national territory and abroad to contribute to the mission referred to in the previous paragraph, in addition to being able to participate in military operations to be determined, as stated in the regulations currently in force.

The existence of intelligence in emergencies is not only due to methodological reasons in the planning of interventions, but also to the fact that, in order to be able to react quickly, it is necessary to analyse the risks that will cause disasters, which in most cases cannot be foreseen and where the time factor is crucial, to monitor the situation constantly and to have warning indicators that allow us to determine the probability of intervention by the EMU.

Keywords

UME, risk, information, catastrophe, armed forces.

1. Introducción

El artículo 15.3 de Ley Orgánica 05/2005 de la Defensa Nacional establece como una de las misiones de las Fuerzas Armadas (FAS) el deber de «preservar la seguridad y bienestar de los ciudadanos en los supuestos de grave riesgo, catástrofe, calamidad u otras necesidades públicas, conforme a lo establecido en la legislación vigente».

Por otra parte, el artículo 3.6 del Real Decreto 372/2020, de 18 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, afirma que la Unidad Militar de Emergencias (UME) tiene como misión la intervención de forma rápida en cualquier lugar del territorio nacional y en el exterior, para contribuir a la misión indicada en el párrafo anterior.

Una UME, constituida de manera permanente, que es parte integrante de las FAS y que, como tal, supone la principal colaboración de estas en operaciones de emergencias, además de poder participar en el cumplimiento de las operaciones militares que se determinen como Mando Componente de Emergencias del Mando de Operaciones (MOPS).

La UME es una fuerza conjunta que tiene una organización, una forma de adiestrarse, de planear y de operar similar a la de los Ejércitos y Armada.

Esto último es especialmente importante porque significa que se va a seguir la misma metodología en el planeamiento de las operaciones de emergencias que la empleada para el planeamiento de las operaciones militares. Una metodología que empieza con un conocimiento inicial y continuo de la situación y una valoración sobre la posible evolución de la misma, que hace necesario contar con una estructura de inteligencia capaz de dirigir, obtener, elaborar y difundir, de manera oportuna, objetiva y fiable, toda la información existente sobre el escenario de la emergencia en la que se va a intervenir.

2. Sistema de inteligencia de la UME

Para hacer posible una función de inteligencia orientada al ámbito de las emergencias que satisfaga las necesidades de información del mando, según se ha indicado en el apartado anterior, será necesario disponer de una organización funcional formada por un personal y unos medios, que contemple, además, una doctrina, unos procedimientos y unas relaciones funcionales que hagan posible llevar a cabo todas las actividades propias de esta función, formando todo ello un sistema de inteligencia, apoyado por una arquitectura CIS para facilitar el control y los flujos de información entre los diferentes órganos y niveles del mismo y que, en la UME, se denomina SINTUME.

El SINTUME tiene los siguientes objetivos:

a) Llevar a cabo una monitorización permanente de la situación a nivel nacional e internacional, que permita prever una emergencia con la mayor antelación posible y, por tanto, la posibilidad de que la Unidad sea activada.
b) Obtener y mantener un conocimiento de la situación adecuado en las intervenciones para las que haya sido activada la Unidad, que permita apoyar el planeamiento y la conducción de las operaciones que se lleven a cabo.
c) Establecer la forma en que se debe realizar la función de inteligencia en la UME, homogénea con el resto de las FAS, que esté en sintonía con la doctrina y procedimientos de carácter nacional y OTAN, de manera que se pueda integrar —sin fricciones— en una operación militar conjunta o conjunto-combinada.

Además, el SINTUME no se entiende como un sistema aislado, sino que debe estar integrado y relacionarse funcionalmente con otros sistemas de inteligencia, tanto de su nivel como de un nivel superior, y por partida doble. Por una parte, dentro del ámbito civil de las emergencias y de protección civil, en el nivel estatal y autonómico. Por otra parte, la UME como unidad militar y como parte integrante de las FAS, debe estar integrada en el Sistema de Inteligencia de las FAS (SIFAS). Esta doble integración confiere al SINTUME un carácter único, característico y diferenciador de los demás sistemas de inteligencia militares.

La eficacia del funcionamiento del SINTUME y de su capacidad para generar inteligencia en tiempo y forma oportuna, residirá en la implementación de estándares interoperables con otros sistemas de inteligencia, en aspectos como la doctrina, los medios CIS, en la disciplina y rigurosidad a la hora de seguir los procedimientos establecidos, así como en la cooperación de todos los actores implicados, tanto internos como ajenos a la UME.

2.1. *Estructura del SINTUME*

Con carácter general y en una situación de normalidad en la que la Unidad no se encuentre interviniendo en una emergencia, el SINTUME se estructurará en dos niveles: un nivel superior y un nivel básico.

El nivel superior estará ubicado en el Cuartel General de la UME (CGUME), en la Sección de Inteligencia y Seguridad (J2) del Estado Mayor de la UME, y lo constituyen dos órganos: uno de dirección y otro de ejecución.

El órgano de dirección tiene los siguientes cometidos:

a) Dirigir el SINTUME, controlando y coordinando el funcionamiento del sistema, así como todas las actividades y procesos que comprenden el ciclo de inteligencia en sus diferentes fases.
b) Planear y dirigir a través del programa de obtención (PROB) la adquisición de la información que satisfaga las necesidades del mando para apoyar los procesos de planeamiento y conducción de las operaciones.
c) Proporcionar a las unidades de la UME la inteligencia necesaria que oriente sus actividades de preparación y el desarrollo de las actuaciones que se les encomiende en una emergencia en la que esté interviniendo la UME.
d) Integrarse en el SIFAS o en aquellas estructuras funcionales de inteligencia de carácter conjunto o conjunto-combinado, que se formen con motivo de una operación militar.
e) Relacionarse y colaborar con otros organismos civiles, nacionales, autonómicos e incluso internacionales, llegado el caso, en asuntos que le competan en este ámbito.
f) Colaborar en la elaboración y actualización de la doctrina para la acción conjunta en el ámbito de la inteligencia.
g) Constituir la célula de inteligencia del Puesto de Mando Fijo (PMF) cuando se activa la Unidad con motivo de una emergencia y del Mando Operativo Integrado (MOPI), si la emergencia es declarada de interés nacional o con motivo de los ejercicios que se determinen.

El órgano de ejecución lo constituye el Centro de Integración y Difusión de Inteligencia (CIDI) de la Sección de Inteligencia y Seguridad. Este órgano será el responsable de elaborar la inteligencia que se genera en la UME de nivel operacional para el planeamiento y conducción de las operaciones en las que intervenga la UME, así como la que se elabore de nivel táctico, en apoyo a las necesidades de inteligencia de las unidades.

Por su parte, el nivel básico estará formado por las unidades de la UME, las cuales actuarán como órganos de ejecución y serán responsables de:

a) La gestión de la inteligencia a su nivel.
b) Contribuir con sus medios a la obtención de la información en su área funcional o de responsabilidad (AOR) en el tiempo requerido, de manera que satisfagan las necesidades de inteligencia que le asigna el PROB y aquellas otras que le lleguen por medio de órdenes de obtención.
c) Cuando la Unidad se encuentre interviniendo en una emergencia de situación operativa 2[1], la estructura del SINTUME será la misma que

[1] El Plan Estatal General de Emergencias de Protección Civil (PLEGEM) establece que una emergencia de situación operativa 2 se declarará por el Ministerio del Interior cuando la o las emergencias no puedan controlarse, o haya un riesgo cierto de que no puedan controlarse con los medios ordinarios propios de la o las comunidades o ciudades autónomas afectadas y sea, o pueda ser, necesaria la aportación de recursos y medios extraordinarios

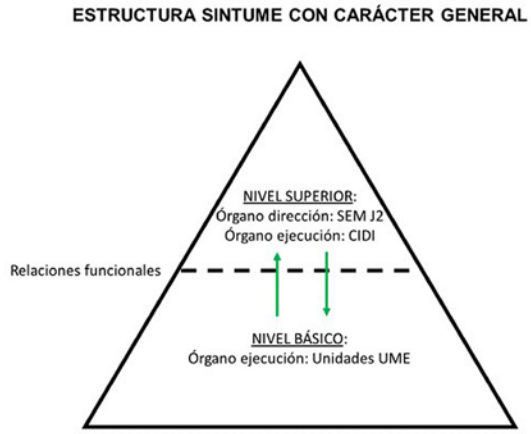


Figura 1. Estructura SINTUME carácter general. Fuente: UME

la anterior, con dos niveles, con la salvedad de que el nivel superior lo ejercerá la célula de inteligencia del PMF y el nivel básico será el batallón que se encuentre activado en la emergencia y actuando como Coordinador Militar de la Emergencia (CME). Las funciones de ambos niveles serán las mismas, si bien en este caso, particularizadas a la emergencia en la que se esté interviniendo.

En el caso de una emergencia de situación operativa 3 o de interés nacional[2], habrá un tercer nivel en la estructura del SINTUME, que será intermedio entre los dos anteriores y que estará ubicado en el MOPI, el cual estará formado, a su vez, por dos órganos: uno, de dirección y otro de ejecución.

El órgano de dirección será responsable de:

a) Planear y dirigir a su nivel la obtención de la información que le asigne el PROB del nivel superior y aquella que satisfaga las necesidades de información/inteligencia del director del MOPI (DIRMOPI) para apoyar la conducción de las operaciones.

---

de la Administración General del Estado, o movilizables por ésta, o de otras comunidades cutónomas o de las ciudades de Ceuta y Melilla, así como cuando se prevea que alguna de las emergencias declaradas puedan derivar en una situación de interés nacional.

[2] Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil establece que son emergencias de interés nacional:

1. Las que requieran para la protección de personas y bienes la aplicación de la Ley Orgánica 4/1981, de 1 de junio, reguladora de los estados de alarma, excepción y sitio.
2. Aquellas en las que sea necesario prever la coordinación de Administraciones diversas porque afecten a varias comunidades autónomas y exijan una aportación de recursos a nivel supraautonómico.
3. Las que por sus dimensiones efectivas o previsibles requieran una dirección de carácter nacional.

Figura 2. Estructura SINTUME emergencia nivel 2. Fuente: UME

b) Proporcionar a los puestos de mando avanzado (PMA) subordinados la inteligencia necesaria que oriente en el desarrollo de sus actuaciones en una emergencia de interés nacional.
c) El órgano de ejecución será la célula de análisis de MOPI/J2 y será responsable de proporcionar la inteligencia necesaria para cubrir las necesidades del DIRMOPI en la conducción de las operaciones de emergencia que se lleven a cabo en su área de responsabilidad. Este órgano no tendrá el mismo dimensionamiento ni posibilidades de elaboración de inteligencia que el CIDI, por lo que deberá mantener un contacto estrecho y frecuente con el nivel superior con el fin de obtener la inteligencia que se le requiera.

Figura 3. Estructura SINTUME emergencia nivel 3. Fuente: UME

Cada nivel de la estructura del SINTUME que se ha definido podrá mantener una relación de carácter funcional con su nivel inmediatamente superior e inferior a través de una arquitectura CIS, que haga posible la conexión de todos los elementos del sistema y el intercambio de información e inteligencia.

2.2. *Integración del SINTUME en el SIFAS*

Como se ha señalado anteriormente, el SINTUME no se entiende como un sistema aislado puesto que la función de inteligencia tiene un carácter conjunto y colaborativo, por lo que, al ser la UME parte integrante de las FAS, tiene sentido que el SINTUME se integre en el SIFAS.

El nivel superior del SINTUME estará encuadrado en el escalón intermedio u operacional del SIFAS, al ejercer la dirección del subsistema específico de Inteligencia de Emergencias de la UME.

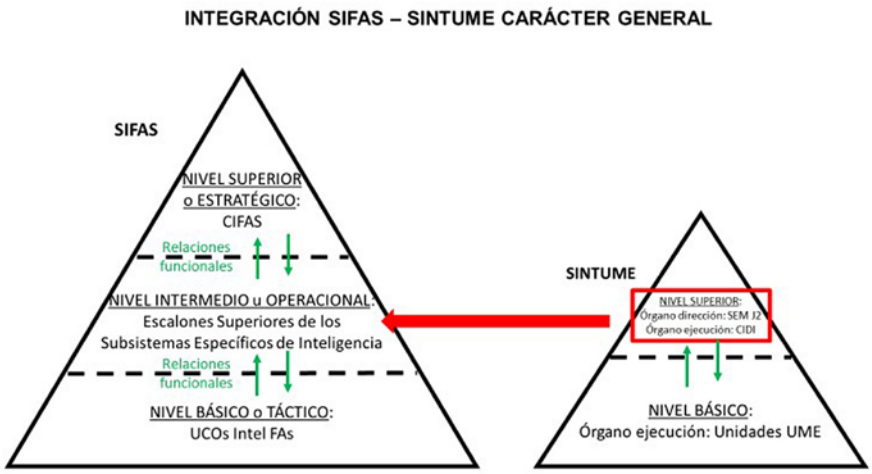


Figura 4. Integración SIFAS-SINTUME carácter general. Fuente: UME

Por último, la célula de inteligencia que se forme en el Mando Componente de Emergencias, como mando subordinado al MOPS, con motivo de una operación militar derivada del cometido asignado a las FAS en el artículo 15.2 de la Ley Orgánica de Defensa Nacional, estará integrada en el escalón básico o táctico del SIFAS.

La integración del SINTUME en el SIFAS y las relaciones funcionales entre ambos sistemas se hará efectiva, a través del nivel Superior del SINTUME, mediante la asistencia regular a las reuniones sectoriales de interés que se convoquen y a través de los sistemas CIS específicos de inteligencia que

Figura 5. Integración SIFAS-SINTUME operaciones militares. Fuente: UME

aseguren la conexión y el intercambio de información entre ambos sistemas, así como la tramitación de peticiones de información (RFI) y de imágenes.

3. Centro de integración y difusión de inteligencia

La UME dispone de un CIDI donde se compila la información procedente de las diferentes fuentes y se elabora la inteligencia de nivel operacional para el planeamiento y conducción de las operaciones en las que intervenga la UME, así como la que se elabore de nivel táctico, en apoyo a las necesidades de inteligencia de las unidades.

En este órgano se encuentra el personal analista orgánico del CGUME y donde, en caso necesario, se integraría el personal de aumento perteneciente a otras unidades de inteligencia de las FAS; el personal militar reservista, especialista en diferentes riesgos y materias de interés del ámbito de las emergencias; y el personal civil de aumento y de enlace perteneciente a organismos externos públicos (estatales y autonómicos) y a empresas privadas, expertos en diferentes riesgos, que puedan estar involucrados en una emergencia.

Sin duda, la formación del personal analista es un aspecto crítico para la inteligencia en emergencias, al igual que en el resto de los ámbitos de la inteligencia militar, donde la experiencia adquirida con el tiempo y la formación propia en emergencias son fundamentales para que los productos de inteligencia sean de calidad y satisfagan plenamente las necesidades de información requeridas por el mando. Por todo ello, los analistas de la UME invierten una parte muy importante de su tiempo en formación, a través de cursos del ámbito de las emergencias propios de la UME, de los Ejér-

citos y Armada, de la Dirección General de Protección Civil y Emergencias (DGPCE) o los impartidos por empresas privadas.

Por otra parte, en cuanto a las disciplinas de inteligencia más empleadas en la UME para la obtención de información, se pueden distinguir las siguientes:

a) Inteligencia humana (HUMINT), a partir del personal de enlace (OFEN) que se encuentra en los diferentes centros de coordinación de operaciones (CECOD y CECOP/CECOPI) y puestos de mando avanzados que se encuentran en la zona de la emergencia, así como a través de los representantes de los organismos externos con los que la UME tiene relación habitualmente.
b) Inteligencia de Imágenes (IMINT), a partir de los productos proporcionados por los satélites de la NASA, el sistema Copernicus de la UE, y los productos satelitales que puedan proporcionar el CIFAS o empresas civiles.
c) Inteligencia Geoespacial (GEOINT), con la integración de toda la inteligencia básica y productos georreferenciados en el Sistema de Información Geográfica de la UME (SIG-UME).
d) Inteligencia de fuentes abiertas (OSINT), que supone la principal fuente de obtención para la Unidad, especialmente por la información que se obtiene en redes sociales (Inteligencia de Redes Sociales -SOCMINT) y por la posibilidad de acceder a la información disponible en los portales web y visores de organismos oficiales como la Agencia Estatal de Meteorología (AEMET), Dirección General de Protección Civil y Emergencias (DGPCE), Instituto Geográfico Nacional (IGN), Instituto Geológico y Minero (IGME), Dirección General del Agua (DGA), Ministerio para la Transición Ecológica y el Reto Demográfico (MITECO), confederaciones hidrográficas, etc.
e) Inteligencia sanitaria (MEDINT). El apoyo técnico proporcionado por el ámbito sanitario se considera fundamental en emergencias sanitarias, como se ha demostrado durante la emergencia sanitaria provocada por la covid-19 y en caso de intervención fuera de territorio nacional.

3.1. Apoyo geoespacial

El apoyo geoespacial lleva a cabo el conjunto de actividades que aseguran que la información geoespacial esté disponible y pueda ser explotada cuando y donde sea preciso.

En el apoyo geoespacial a emergencias, los sistemas de información geográfica (GIS) cobran una especial importancia al permitir analizar la ubicación espacial de los datos que integran el entorno operativo de una

emergencia, organizados por capas de información. De esta manera pueden revelar relaciones, situaciones y patrones, apoyando la elaboración de los mapas de riesgo y de probabilidad de intervención de la UME, así como la realización de simulaciones dirigidas a obtener una prospectiva sobre la evolución de la misma.

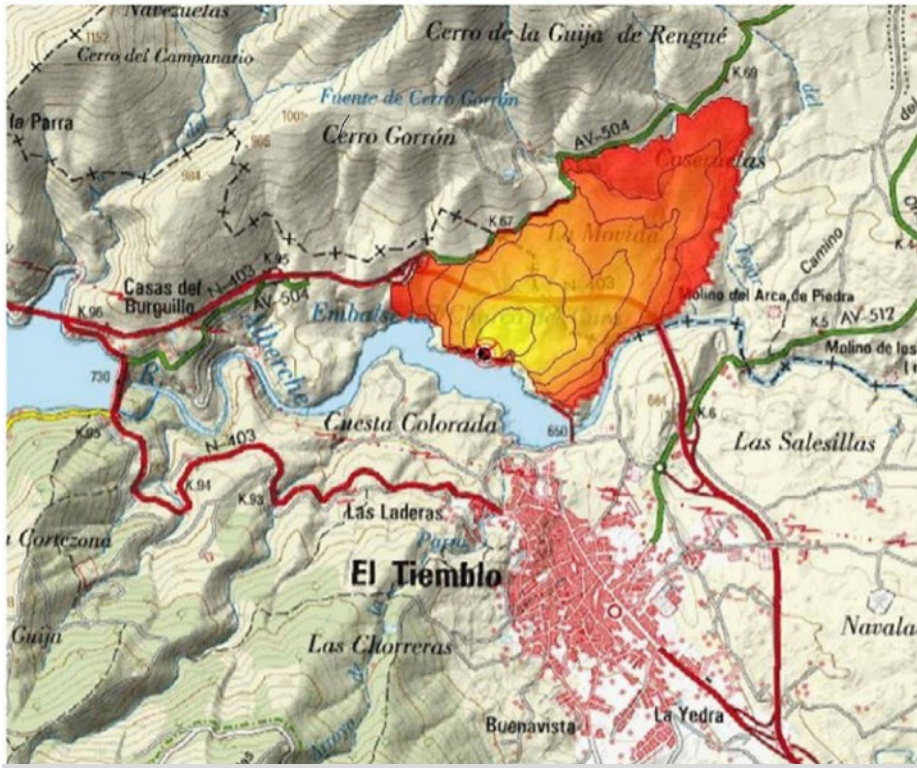


Figura 6. Simulación de evolución de incendio forestal en el GIS de la UME sobre una base del Mapa Topográfico Nacional del IGN. Fuente: UME

El SIG-UME es la herramienta GIS empleada en la UME, la cual comprende la información geoespacial necesaria para el análisis de distintos riesgos entre los que destacan los siguientes:

a) Riesgos tecnológicos (RRTT), con la localización de las infraestructuras consideradas de interés (como pueden ser centrales nucleares, industrias SEVESO[3], etc.).

[3] Según el RD 840/2015 define como incidente SEVESO: «Cualquier suceso, como una emisión en forma de fuga o vertido, un incendio o una explosión importantes, que resulte de un proceso no controlado durante el funcionamiento de cualquier establecimiento al que sea de aplicación este real decreto, que suponga un riesgo grave, inmediato o diferido, para la salud humana, los bienes, o el medio ambiente, dentro o fuera del establecimiento y en el que intervengan una o varias sustancias peligrosas».

b) Riesgo medioambiental, con la delimitación de las áreas afectadas.
c) Riesgo volcánico, mediante la actualización de la evolución de las coladas de lava, formación de posibles fajanas, modelos 3D de la zona afectada, etc.
d) Riesgo sísmico, con la delimitación de las áreas de mayor peligrosidad sísmica, localización de enjambres sísmicos y de las infraestructuras consideradas de interés (presas, túneles) que se puedan ver afectadas.
e) Riesgo de inundaciones, mediante la delimitación de las zonas inundables con riesgo para la población.
f) Riesgo de incendios forestales, actualizando las capas de vegetación, áreas geográficas con mayor estrés hídrico, mapas con la valoración del riesgo de propagación de un incendio forestal debido a factores meteorológicos (FWI), la localización geográfica de los incendios, la integración de los parques nacionales, parques naturales, elementos de la Red Natura 2000, entre otros.

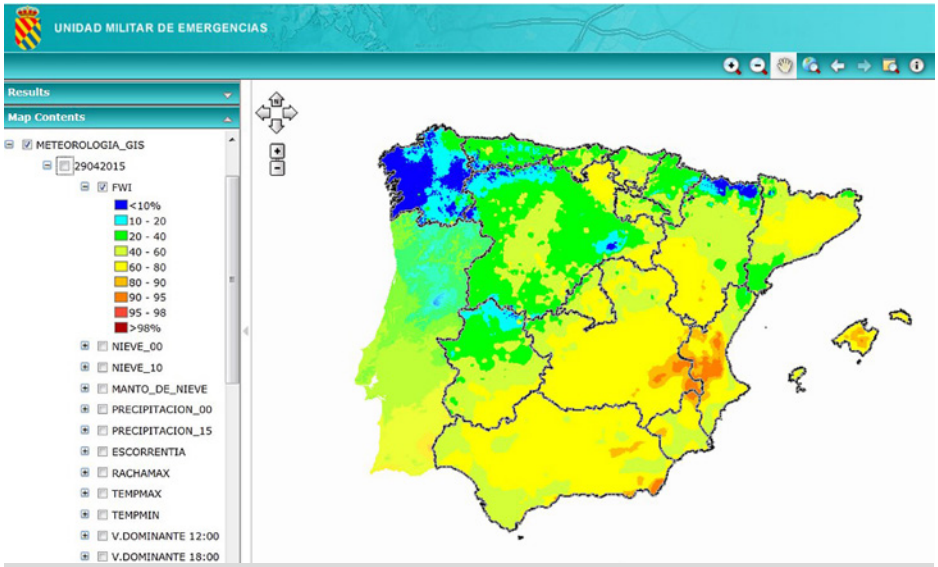


Figura 7. Mapa FWI en SIG-UME. Fuente: UME

g) Otros, como la localización y afectación a Bienes de Interés Cultural (BIC) o el posicionamiento de unidades UME en tiempo real.

También será relevante disponer de un catálogo histórico de imágenes georreferenciadas de la zona afectada, de forma que puedan compararse las imágenes obtenidas antes y después de un incidente, que permitan realizar un análisis y una valoración sobre la magnitud y la posible evolución de la emergencia.

4. Análisis de riesgos

Como se ha dicho anteriormente, para la conducción de las operaciones de emergencias es fundamental disponer de un conocimiento de la situación adecuado de la misma, lo que hace necesario contar con una estructura especializada que sea capaz de dirigir, obtener, elaborar y difundir, en tiempo oportuno, toda la información existente sobre la amenaza, sus causas, sus efectos y su posible evolución y consecuencias, vinculándolo todo ello con el entorno donde se produce y la población que puede verse afectada, con el fin de asesorar y apoyar al mando en el planeamiento de las operaciones y en el ciclo de toma de decisiones.

Desde el punto de vista de inteligencia, las principales características de las operaciones de emergencias son:

a) El adversario es la catástrofe, calamidad o cualquier amenaza que suponga un riesgo para la seguridad de las personas y sus bienes, principalmente.
b) 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 que ocurra.
c) En muchas ocasiones no se podrá llevar a cabo el ciclo de inteligencia de forma completa, principalmente porque lo que prima en los primeros momentos de la emergencia es recopilar la información existente para iniciar el planeamiento de la intervención, ya que toda demora que se produzca aumenta los daños y los efectos de la 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.

Por lo tanto, este será el primer cometido que tendrá la función de inteligencia en emergencias: analizar y determinar las zonas de mayor riesgo de que se produzca 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 (CRI) y Tormentas Invernales Severas (TIS)), y los planes de contingencia (COP) que se elaboren.

A continuación, la inteligencia 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.

En esos procedimientos la inteligencia básica y de objetivos van a ser un elemento fundamental e imprescindible para obtener la información inicial necesaria para empezar a dar las primeras respuestas a las necesidades de información que se planteen. Se entiende por inteligencia básica a 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 que va a proporcionar ese ahorro de tiempo del que carecemos.

Por otro lado, la inteligencia de objetivos describe una instalación sensible o crítica, como puede ser una presa, una industria SEVESO 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, a continuación será importante señalar la elaboración de inteligencia actual, es decir, la inteligencia relativa a una catástrofe, una vez que se ha producido: 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. Por ello, los analistas del CIDI deben tener unos conocimientos avanzados en esta materia que les permitan alertar con el mayor tiempo posible sobre situaciones que puedan desembocar en una intervención.

5. Riesgos

Como se ha indicado en el apartado anterior, en las operaciones de emergencias el adversario es la catástrofe, la calamidad o cualquier amenaza que suponga un riesgo para la seguridad de las personas y sus bienes, principalmente.

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».

Tradicionalmente los riesgos se clasifican como:

a) Riesgos naturales: procesos o fenómenos naturales potencialmente peligrosos como inundaciones, terremotos, tsunamis, incendios forestales, TIS y volcanes.
b) Riesgos antrópicos: derivados de la acción del ser humano, entre los que se encuentran los riesgos tecnológicos[4] y medioambientales.

Como se puede ver, por tanto, en el ámbito de las emergencias no hay un solo adversario (riesgo) al que nos enfrentemos, sino varios, que se pueden distinguir también según se produzcan 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.

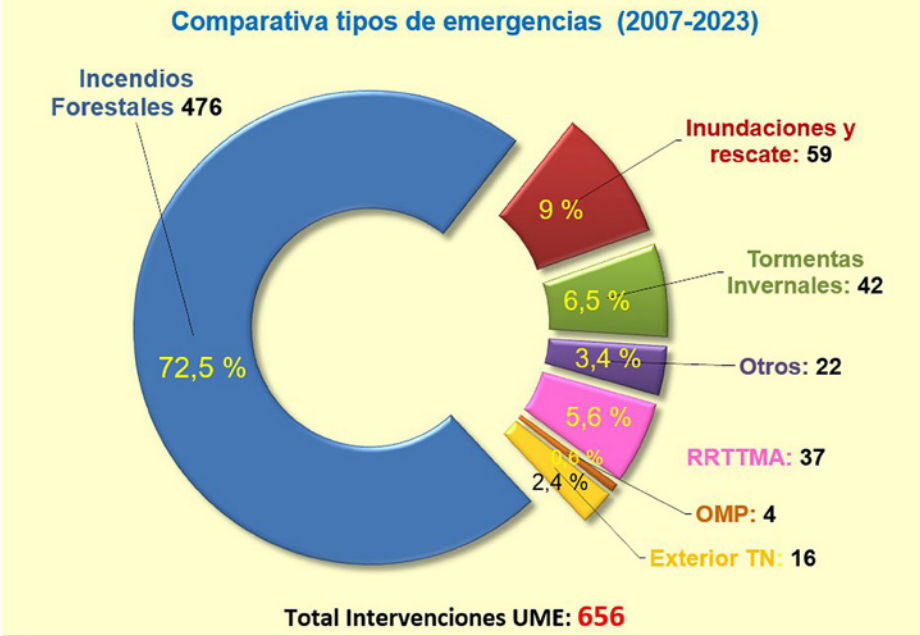


Figura 8. Intervenciones de la UME por riesgos. Fuente: UME

[4] Un riesgo tecnológico viene definido por los daños o pérdidas que pueden presentarse debido a eventos asociados con el almacenamiento, producción, transformación 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.

5.1. Incendios forestales

Los incendios forestales son, con diferencia, la primera causa de intervención de la UME tanto en territorio nacional como en el extranjero.

La meteorología junto con el estado del combustible son los factores más determinantes en los incendios forestales y dentro de estos factores, las variables más importantes a analizar son las temperaturas, la humedad relativa y la dirección e intensidad del viento, elementos que influirán en el comportamiento del fuego y que forman parte del FWI, índice de riesgo meteorológico de incendio forestal.

También influyen circunstancias geográficas, políticas, sociales, económicas o culturales que favorecen o reducen la intencionalidad, accidentalidad o negligencia, haciendo que su distribución territorial y ocurrencia sea muy variable.

El mes de agosto representa el máximo absoluto en número de siniestros, seguido de un máximo relativo en el mes de marzo, así como de julio y septiembre, por este orden.

La elevada ocurrencia durante el verano está fuertemente asociada al mayor riesgo de incendio forestal en la mayor parte de España, mientras que las cifras del mes de marzo se deben principalmente al uso accidental, negligente o intencional del fuego con objeto de transformar el territorio, concentrándose fundamentalmente en el noroeste. Aunque el número de

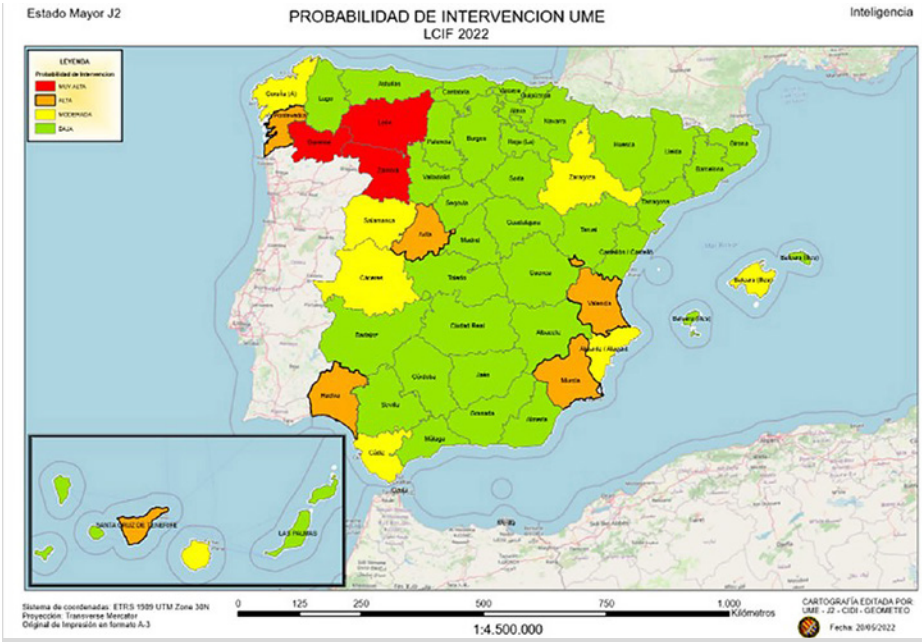


Figura 9. Mapa de probabilidad de intervención de la UME en LCIF. Fuente: UME

siniestros de marzo es equiparable al de agosto e incluso superior a los sucedidos en julio y septiembre, casi la mitad de ellos son conatos, caso que no sucede en los meses de verano.

El 80,77% del total de los siniestros tienen origen antrópico, ya sea debido a negligencias y accidentes o intencionados. Destaca que los incendios intencionados son los más numerosos, representando más de la mitad del total

(52,70%).

Con base en el estudio de los factores anteriores se elaboran las líneas de acción de la amenaza de incendios más probables y más peligrosos, así como el mapa de probabilidad de intervención de la UME en incendios forestales.

5.2. *Inundaciones*

Las inundaciones pueden ser el resultado de precipitaciones fuertes y/o continuas que exceden la capacidad de absorción del suelo, así como de los ríos y zonas de drenaje naturales, ocasionando que el curso de agua rebose su cauce natural hacia las tierras adyacentes originándose la inundación. Pero también puede ser el resultado de subidas bruscas de temperatura que generen una rápida fusión de la nieve acumulada en las montañas, y con ello, un caudal que supere la capacidad de desagüe de la cuenca. Esto se da sobre todo en primavera, cuando el deshielo es mayor, o tras fuertes nevadas en cotas inusuales, que tras la ola de frío se funden provocando riadas.

Otro tipo de inundaciones son las producidas por maremotos, tsunamis o rissagas, que son fenómenos de crecida de las olas que llegan a la costa, ya sean estas debidas a episodios sísmicos en el lecho marino o episodios de fuerte viento asociados a mareas. Finalmente, hay que contemplar las inundaciones que tienen un antecedente antrópico: por roturas de presas, balsas, etc., y que en este caso suelen tener asociados graves consecuencias.

En España el régimen pluviométrico es muy variable, pasando de estados de sequía a fuertes precipitaciones que en pocas horas alcanzan valores superiores al promedio. Estas precipitaciones extraordinarias provocan caudales extremos, habitualmente denominados crecidas, avenidas o riadas, que al desbordar su cauce habitual provocan la inundación de terrenos, afectando a personas y bienes.

Las inundaciones revisten una especial gravedad en España, siendo el fenómeno natural que mayor incidencia tiene en nuestra sociedad, y el que con mayor frecuencia deriva en situaciones de grave riesgo, catástrofe o

calamidad pública, lo que provoca mayores pérdidas económicas y supone la segunda causa de activación de la UME.

El riesgo de inundaciones afecta prácticamente a toda la geografía española, aunque el territorio más afectado se centra en las costas mediterráneas y cantábricas y en los espacios fluviales de los grandes ríos peninsulares.

La principal causa de las inundaciones en España lo constituyen las fuertes precipitaciones, sobre todo, las derivadas de las depresiones aisladas en niveles altos (DANA), también conocidas como «gota fría». Las regiones mediterráneas son las más afectadas.

Los episodios de inundaciones más recurrentes en nuestro país se registran en las cuencas hidrográficas del Ebro, Júcar y Segura, seguidas por las cuencas del Guadalquivir y Duero.

En base a lo anterior, las líneas de acción más probables que se establecen en cada campaña anual suelen incluir: inundaciones causadas por DANA; inundaciones por rápida fusión de gran cantidad de nieve acumulada en sistemas montañosos como los Pirineos, los Picos de Europa o el Sistema Central; e inundaciones fluviales con crecidas de los grandes ríos en cuencas como la del Ebro.

En cuanto a las líneas de acción más peligrosas, estas suelen incluir posibles inundaciones en zonas costeras producidas por tsunamis, a su vez causados por sismos.

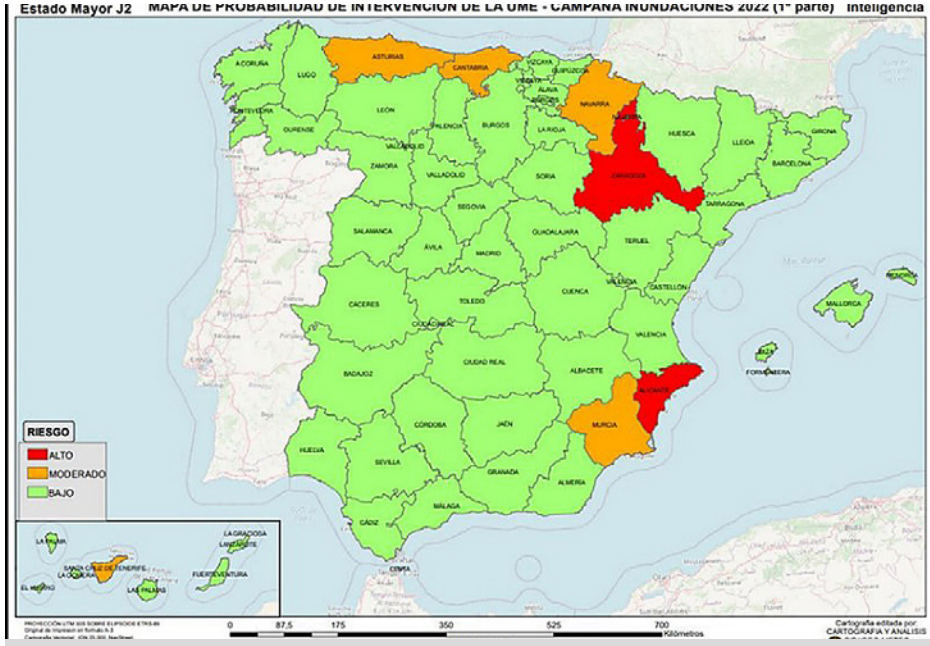


Figura 10. Mapa de probabilidad de intervención UME por inundaciones. Fuente: UME

5.3. *Tormentas invernales severas*

Las emergencias derivadas de grandes nevadas originan situaciones como aludes, incomunicaciones y aislamientos de poblaciones y personas, y restricciones de movimiento, suponiendo la tercera causa de intervención de la UME.

Sin duda el caso más reciente y conocido de este riesgo fue el episodio de fuertes nevadas que provocó la tormenta Filomena en 2021, como consecuencia de la coincidencia de una vaguada polar con un frente atlántico o tropical.

En este caso, la monitorización de la situación varios días antes de que se produjera, permitió una preparación adecuada de la Unidad y el despliegue adelantado de unidades en puntos concretos para poder actuar desde ahí si se activaba la Unidad, como así ocurrió en las provincias de Albacete, Madrid, Teruel y Zaragoza.

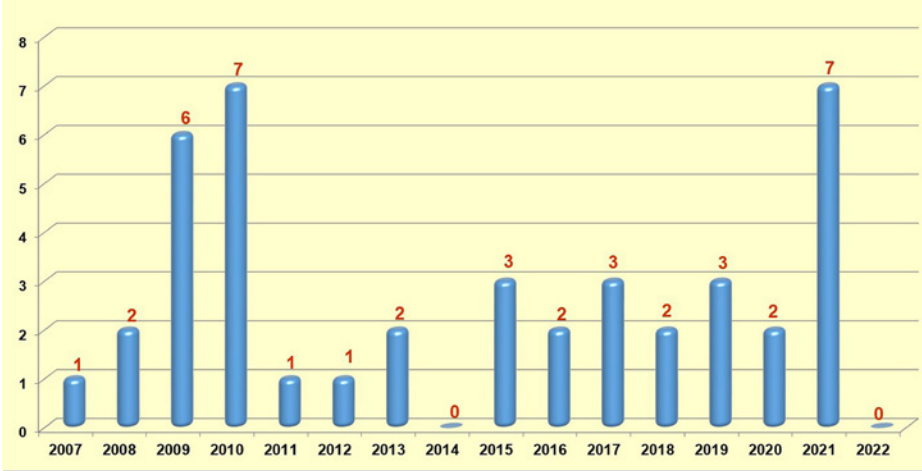


Figura 11. Intervenciones UME en Tormentas Invernales 2007-2022. Fuente: UME

La línea de acción más probable por nevadas intensas suele ser relativa a nevadas fuertes que afectan a las vías de comunicación que atraviesan la cordillera Cantábrica, principalmente las que cruzan por el norte de León y Burgos; las que atraviesan las estribaciones orientales del Sistema Ibérico, afectando a las provincias de Teruel y Castellón; y las que atraviesan el Sistema Central en la Comunidad Autónoma de Madrid.

Entre las líneas de acción más peligrosas, por orden de menor a mayor peligrosidad, se considerarían nevadas fuertes que provoquen aludes en zonas altas de montaña y nevadas fuertes en el entorno de Madrid y las que afecten completamente a sectores estratégicos de infraestructuras y servicios esenciales (ISEM) como los suministros de agua, energía, transporte y telecomunicaciones.

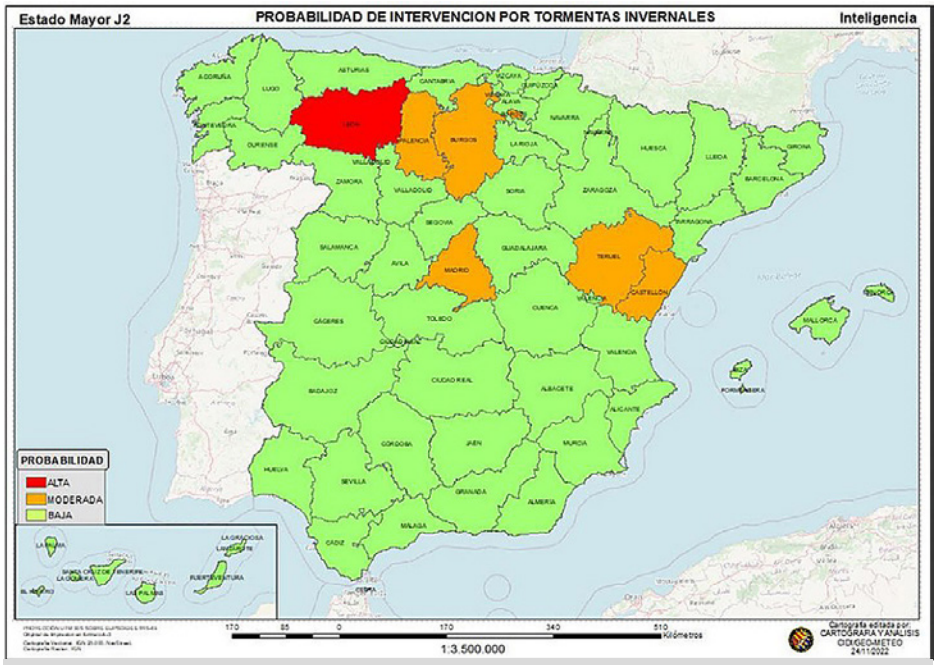


Figura 12. Mapa de probabilidad de intervención UME. Fuente: UME

5.4. Seísmos

El riesgo de terremotos en España no suele ser una causa habitual de activación de la Unidad, cuya intervención más importante en territorio nacional fue debido al terremoto de Lorca (Murcia), entre los meses de mayo y octubre de 2011. En cuanto a intervenciones fuera de nuestras fronteras, la UME ha intervenido en los terremotos que tuvieron lugar en Ecuador, en abril de 2016; México, entre los meses de septiembre y octubre de 2017; y en el momento en el que se está escribiendo este trabajo la UME está interviniendo en el terremoto ocurrido en Turquía el 6 de febrero del presente año, 2023.

Afortunadamente, España no representa un área de ocurrencia de grandes terremotos. Sin embargo, sí tiene una actividad sísmica relevante con sismos de magnitudes inferiores a 7,0, capaces de generar daños muy graves.

En ocasiones, las costas atlánticas peninsulares, especialmente las comprendidas entre Lisboa y Gibraltar, han sido alcanzadas por tsunamis, producidos por epicentros submarinos situados en la región sísmica de Azores-Gibraltar. El tsunami mejor documentado de la historia de España, acaeció el 1 de noviembre de 1755 en la zona del Cabo de San Vicente, donde 1.500 personas murieron ahogadas en España.

La zona occidental de la Península (Galicia y Portugal) tiene una cierta actividad sísmica debido a una línea de sismos que conecta con la dorsal Atlántica (falla transformante Azores-Gibraltar).

La sismicidad en Canarias parece estar asociada en gran medida al vulcanismo, aunque no puede descartarse una actividad sísmica intraplaca, independiente del fenómeno volcánico.

Los daños causados por un terremoto pueden afectar a dominios tan diversos como:

a) Forestal: afectando masas forestales que puedan producir incendios que agraven la ya delicada situación de emergencia.
b) Subsuelo: afectando más o menos gravemente las redes subterráneas de abastecimiento de agua, de conducción de energía y de telecomunicaciones.
c) Núcleos urbanos y Bienes de Interés Cultural: afectando directamente a los habitantes de los núcleos urbanos y produciendo daños directos a viviendas, edificios y BIC.
d) Infraestructuras: afectando a infraestructuras ISEM tan diversas como la hospitalaria, la relacionada con la producción y distribución de energía eléctrica y gas, las telecomunicaciones y las diferentes redes de transporte, pudiendo ser indirectamente el origen de otras emergencias como medioambientales, riesgos tecnológicos, inundaciones por rotura de presas, etc., que agraven la situación. Infraestructuras críticas como complejos petroquímicos o centrales nucleares, deberán ser especialmente reconocidas después de un terremoto de alta intensidad, dado el peligro potencial que entrañan.

A pesar de lo difícil que es predecir la ocurrencia de este riesgo, las líneas de acción más probables irían orientadas a la ocurrencia de un terremoto en Andalucía oriental (especialmente la zona de Granada) y la Región de Murcia y, con menor probabilidad, en la zona pirenaica de Aragón y Cataluña. Por otra parte, se contemplan las islas Canarias más occidentales, por su actividad volcánica, muy relacionada con el riesgo sísmico, como ya se ha mencionado.

Por su parte, las líneas de acción más peligrosas se referirían a la ocurrencia de eventos de intensidades entre IX-X con epicentro en el sur o sureste peninsular, que afectasen principalmente a la provincia de Granada, Almería y Murcia, y eventos de las mismas intensidades con epicentro en el Océano Atlántico, que afectase principalmente a Portugal y a zonas de España cercanas al país vecino. La diferencia esencial entre ambas líneas de acción estaría en la intensidad del evento, que tendría una afectación más o menos grave en los dominios indicados anteriormente.

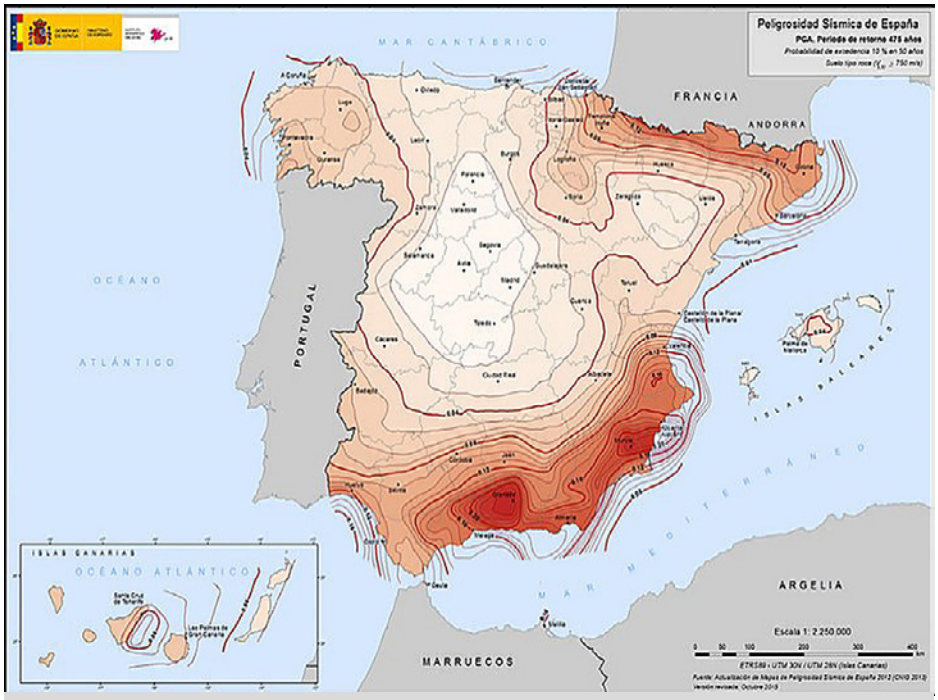


Figura 13. Mapa de peligrosidad sísmica en España. Periodo de retorno: 475 años. Fuente: IGN 2015

5.5. *Volcanes*

En España podemos diferenciar, por una parte, el vulcanismo que se localiza en el ámbito peninsular y en algunas de sus islas próximas y, por otra, el que se encuentra en Canarias. El origen del primero está relacionado con la colisión entre las placas africana y euroasiática, mientras que el segundo es debido a la formación de un punto caliente en el interior de una placa oceánica, situada en el contacto con el continente africano.

Existen, por tanto, varias áreas volcánicas en España: las islas Canarias, la comarca de La Garroxta (Gerona), Cabo de Gata (Almería), Cofrentes (Valencia), las islas Columbretes (Castellón) y Campos de Calatrava (Ciudad Real). Entre ellas, solamente en La Garrotxa y en Canarias han tenido lugar erupciones en los últimos 10.000 años.

En el archipiélago canario no todas las islas tienen el mismo nivel de actividad eruptiva reciente ni las mismas probabilidades de que se produzcan en ellas erupciones volcánicas en un futuro cercano. El riesgo volcánico se ha manifestado con mayor intensidad en las islas occidentales de La Palma, Tenerife y El Hierro, registrándose en esta última una erupción volcánica submarina en el año 2011 y varias crisis sismovolcánicas en los años 2012 y

2013. Sin embargo, el evento eruptivo reciente más importante tuvo lugar en la isla de La Palma entre el 19 de septiembre y el 13 de diciembre de 2021.

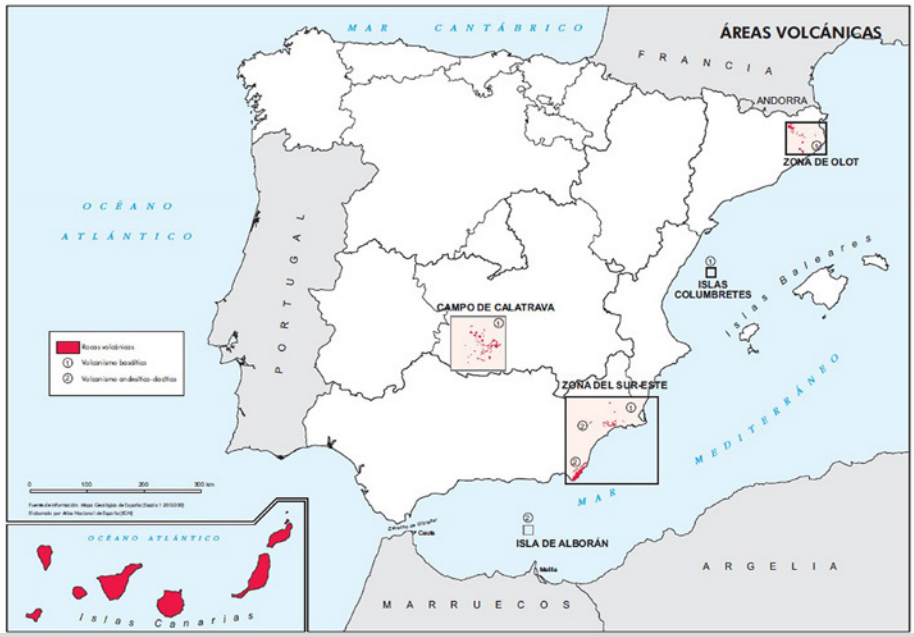


Figura 14. Mapa de zonas volcánicas en España. Fuente: IGN

Al igual que ocurre en otros riesgos, los daños causados por un volcán pueden afectar a dominios muy diversos:

a) Urbano: afectando directamente a los habitantes de los núcleos urbanos y produciendo daños directos a las viviendas y al resto de edificios (escuelas, comercios, etc.), e indirectamente, por ser el origen de otras emergencias (incendios, inundaciones por lahares, contaminación por escapes químicos, etc.) que agravan la situación.
b) Forestal: la emisión de partículas incandescentes sobre combustibles en condiciones de arder puede provocar incendios forestales.
c) Subsuelo: debido a la contaminación de acuíferos por dióxido de azufre (SO_2) o sulfuro de hidrógeno (H_2S).
d) Infraestructuras: pueden verse más o menos gravemente afectadas por daños directos o indirectos a infraestructuras ISEM como la hospitalaria, la red de distribución de agua, la producción o la distribución de energía eléctrica o gas, las telecomunicaciones y las diferentes redes de transporte, incluido el tráfico aéreo.

Como línea de acción más probable se contempla una serie de erupciones que podrían ser de carácter submarino, principalmente al sur de la isla

del Hierro, afectando de forma inicial a sus costas, pero que, dependiendo de la intensidad y duración, comprometerían seriamente a toda la isla.

Como línea de acción más peligrosa se contempla una erupción muy explosiva que evolucionara de manera muy rápida en el tiempo en alguna de las islas más occidentales del archipiélago canario, especialmente en las islas de El Hierro, La Palma o Tenerife, que son las que presentan un mayor riesgo.

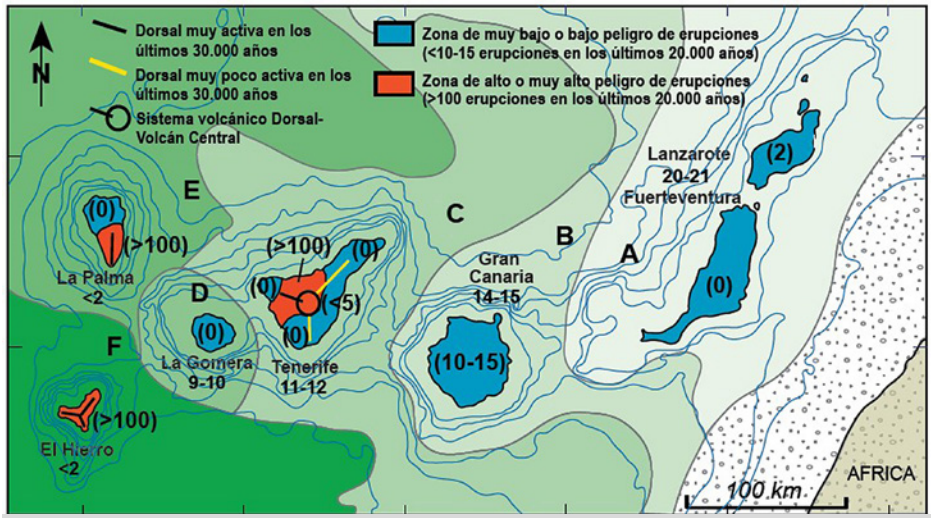


Figura 15. Mapa de riesgo volcánico en Canarias. Fuente: IDEE Canarias

5.6. *Riesgos sanitarios*

Dentro de este tipo de riesgos, tenemos sin duda la reciente y aún existente emergencia sanitaria[5] provocada por el coronavirus SARS-CoV-2.

En este caso, el análisis de inteligencia contribuyó a mantener un conocimiento de la situación —actualizado en todo momento— y a establecer los diferentes umbrales para definir una valoración de la amenaza de contagio del coronavirus en las diferentes áreas de responsabilidad (AOR) de los batallones de intervención de la UME (BIEM), con el doble objetivo de:

a) Asegurar la máxima operatividad de la Unidad, mediante la adopción de las medidas de profilaxis y sanitarias adecuadas a la situación dentro de la Unidad.
b) Prever la probabilidad de activación de la Unidad ante el grado de afectación de la COVID-19 en el conjunto del territorio nacional.

[5] Actualmente, la OMS continúa manteniendo en vigor el estado de emergencia sanitaria mundial por la covid-19.

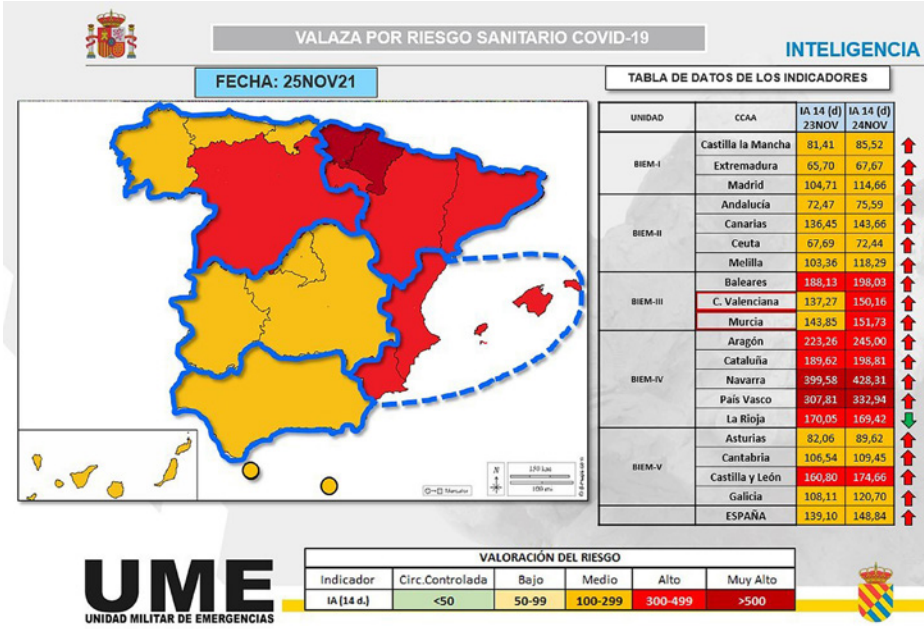


Figura 16. Valoración de la amenaza por riesgo sanitario COVID-19. Fuente: UME

5.7. *Riesgos tecnológicos y medioambientales*

Un riesgo tecnológico viene definido por los daños o pérdidas que pueden presentarse debido a eventos asociados con el almacenamiento, producción, transformación 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.

Por otro lado, hablamos de riesgo medioambiental cuando hay posibilidad de que la amenaza afecte al medioambiente natural debido a la actividad humana.

Se puede afirmar que el riesgo que puede acontecer con mayor probabilidad es el químico, aun cuando el que mayor peligro conlleva es el derivado de un accidente nuclear; mientras que el biológico será el que genere un mayor impacto social, económico y sobre la salud pública.

6. Sistema de alerta y seguimiento de la situación

Como ya se ha indicado a lo largo de este trabajo, uno de los cometidos que tiene la inteligencia que se lleva a cabo en la UME es la monitorización permanente de la situación a nivel nacional e internacional, que permita

prever una emergencia con la mayor antelación posible, cualquiera que sea su naturaleza, determinar la probabilidad de que la Unidad sea activada y conseguir con ello una mayor rapidez en la respuesta.

Para ello, se ha establecido un procedimiento que contiene un catálogo de indicadores, según el riesgo del que se trate, para una mejor monitorización por parte de los diferentes centros de situación de la UME, tanto los Centros de Operaciones de los Batallones (COB) como el Centro de Seguimiento y de Operaciones Conjuntas (CESIJOC) del CGUME.

Dicho procedimiento contempla también las directrices que activan los mecanismos de prealerta de manera escalonada, según se avanza de un nivel a otro superior.

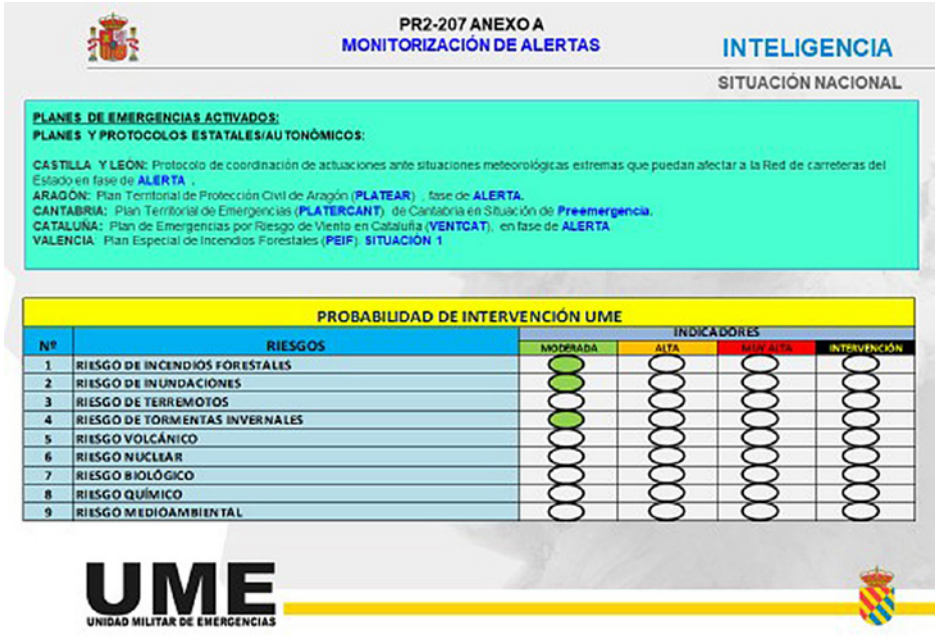


Figura 17. Probabilidad de intervención de la UME. Fuente: UME

7. Conclusiones

La experiencia reciente en operaciones y ejercicios ha puesto de manifiesto que la UME, como parte de las FAS, es la principal contribución de estas para cumplir la misión asignada de preservar la seguridad y bienestar de los ciudadanos en los supuestos de grave riesgo, catástrofe, calamidad u otras necesidades públicas, pero sin olvidar que puede participar en operaciones militares conjuntas, con lo que debe desarrollar una función de inteligencia en emergencias que esté en sintonía con la doctrina nacional.

Con carácter general, los conceptos y procesos que se llevan a cabo en la inteligencia militar son aplicables a la inteligencia en emergencias, donde los adversarios son las catástrofes, de carácter imprevisible en la mayoría de los casos, y donde el factor tiempo es de vital importancia para los intervinientes y la población afectada.

La clave del éxito para poder proporcionar una respuesta rápida y eficaz reside en la monitorización de la situación de manera permanente y disponer de unos indicadores de alerta que permitan determinar la probabilidad de intervención de la UME, apoyado por un análisis previo de los mapas de riesgos y de las líneas de acción más probables y peligrosas que se puedan presentar.

El empleo de herramientas de análisis que combinen, la información obtenida en fuentes abiertas —en especial las redes sociales— y la inteligencia geoespacial pueden aportar un gran valor añadido a lo indicado en el párrafo anterior.

Por último, la inteligencia militar y la inteligencia en emergencias comparten una problemática común como es la de disponer de un personal analista con la combinación adecuada de formación, experiencia y conocimiento experto.

Referencias

Estado Mayor de la Defensa. (2022). Apoyo Geoespacial. Publicación Doctrinal Conjunta PDC-3.17.

Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.

Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

Real Decreto 372/2020, de 18 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa.

UME Unidad Militar de Emergencias. (2019). Centro de integración y difusión de inteligencia en la Unidad Militar de Emergencias. Norma General NG2-213.

UME Unidad Militar de Emergencias. (2020). Inteligencia y seguridad de la Unidad Militar de Emergencias. Publicación Doctrinal de Emergencias PDE3-002.

UME Unidad Militar de Emergencias. (2020). Indicadores para seguimiento y monitorización de emergencias por los centros de operaciones y seguimiento de la UME. Procedimiento UME PR-207.

UME Unidad Militar de Emergencias. (2020). Órdenes Operaciones (OPORD) campañas estacionales 2022.

Glosario de términos y abreviaturas

BIC. Bienes de interés cultural.

CECOD. Comité Estatal de Coordinación y Dirección.

CECOP. Centro de Coordinación Operativa.

CECOPI. Centro de Coordinación Operativa Integrado.

CESIJOC. Centro de Seguimiento y de Operaciones Conjuntas.

CIDI. Centro de Integración y Difusión de Inteligencia.

CIFAS. Centro de Inteligencia de las Fuerzas Armadas.

CME. Coordinador Militar de la Emergencia.

COB. Centro de Operaciones de Batallón.

COP. Contingency Plans – Planes de Contingencia.

CRI. Campaña de Rescate e Inundaciones.

DIRMOPI. Director del MOPI.

FAS. Fuerzas Armadas.

FWI. Fire Weather Index – Índice de propagación de un incendio debido a factores meteorológicos.

GIS. Geographical Information System – Sistema de Información Geográfica.

ISEM. Infraestructuras y Servicios Esenciales.

LCIF. Lucha Contra Incendios Forestales.

MCE. Mando Componente de Emergencias.

MOPI. Mando Operativo Integrado.

MOPS. Mando de Operaciones.

OFEN. Oficial de Enlace.

PLEGEM. Plan Estatal General de Emergencias de Protección Civil.

PROB. Programa de obtención.

PMF. Puesto de Mando Fijo.

RFI. Request for Information – Petición de información.

SIFAS. Sistema de Inteligencia de las FAS.

SIG-UME. Sistema de Información Geográfica de la UME.

SINTUME. Sistema de Inteligencia de la UME.

SNPC. Sistema Nacional de Protección Civil.

TIS. Tormentas Invernales Severas.

UE. Unión Europea.

UME. Unidad Militar de Emergencias.

La inteligencia en la guerra de Ucrania Observaciones preliminares

Ángel Segundo Gómez González

«We are witnessing the ways wars will be fought, and won, for years to come»[1]
Gen. Mark A. Milley, chairman of the US Joint Chiefs of Staff

«The power of advanced algorithmic warfare systems is now so great that it equates to having tactical nuclear weapons against an adversary with only conventional ones»[2]
Alex Karp, chief executive of Palantir

Resumen

La invasión de Ucrania por parte de Rusia se presenta como un «escaparate» de tendencias en todos los niveles de conducción de la guerra y en todas sus áreas funcionales y dominios de las operaciones. La inteligencia se está mostrando como una función clave en la que además observamos tendencias e incluso posibles cambios importantes. Su observación y análisis reviste el máximo interés. Es prematuro realizar un análisis profundo acerca de esta materia, pero ya pueden hacerse algunas observaciones que merecerán un análisis más profundo en el futuro. Este es el propósito de este modesto artículo.

Palabras clave

ISR atípico, inteligencia colectiva, X-cueing (activación dirigida de sensores), multidominio, configuración del entorno, disuasión, influencia, disuasión.

Intelligence in the Ukrainian War

Preliminary observations

Abstract

Russia's invasion of Ukraine can be seen as a 'showcase' for trends at all levels of warfare, in all its functional and operational domains. Intelligence is proving to be a key function in which we can observe trends and possibly even major changes. Its monitoring and analysis is of paramount interest. It is still too early to make an in-depth analysis of the subject, but

[1] Ignatus, D. (2022). How the algorithm tipped the balance in Ukraine. *Washington Post.*
[2] *Idem.*

some observations can already be made that will certainly merit further analysis in the future. This is the purpose of this modest article.

Keywords

Non-traditional ISR, crowdsourcing intelligence, X-cueing, multidomain, environment shaping, deterrance, influence, declassification.

1. Introducción

Nadie duda de la importancia de la inteligencia y la contrainteligencia para tener éxito en los ámbitos de la seguridad y la defensa y en particular en la guerra, en sus campañas y en sus batallas. También es conocido que la historia está llena de sonados fracasos político-diplomáticos, estratégicos, operacionales y tácticos que pueden atribuirse a una inteligencia escasa, de mala calidad, mal comunicada y/o mal trasladada a las decisiones de la acción ofensiva o defensiva.

Cuando esto ocurre, cuando puede atribuirse a la inteligencia a cualquier nivel una parte de la «culpa» en el fracaso, el análisis crítico de sus organizaciones, de sus procesos y actividades, de la calidad de sus productos y de cómo y a quién se difunden, es imprescindible para mejorar. Por eso, las organizaciones de inteligencia deben dotarse de mecanismos de control de calidad y valoración del desempeño de sus distintos elementos y componentes, pero también de procesos que permitan medir su efectividad, el grado en que contribuyen a alcanzar el éxito, a reducir el impacto de las situaciones desfavorables o a neutralizar las amenazas. Frecuentemente, hacen lo primero basado en los MOP[3]. Lo segundo (basado en los MOE[4]) es en gran medida una asignatura pendiente. En ambos casos, además de herramientas metodológicas, se requiere una sólida cultura de la autocrítica que no siempre está presente.

En el ámbito académico y profesional anglosajón se usa el término *post mortem* para referirse a los estudios retrospectivos, muy frecuentes y útiles en el ámbito de la inteligencia. Estos estudios se desarrollan cuando teóricamente ya están todas las *cartas sobre la mesa*, una vez pasada la crisis o finalizado el conflicto. Ofrecen grandes posibilidades para el análisis y la identificación de errores y también, en algunos casos, de buenas prácticas que interesa replicar en el futuro. En España tenemos poca tradición de estudios académicos sobre inteligencia. Menos aún de *post mortems*, en el ámbito de las ccomunidades de inteligencia, acerca de nuestras propias crisis u operaciones y, aún menos, sobre aquellas relativamente recientes. Es cierto que estos estudios se ven limitados por el difícil acceso a documentos, a menudo clasificados e incluso no disponibles por haber sido destruidos, pero también —por qué no reconocerlo—, por la falta de espíritu autocrítico. No tan efectivo, pero mucho más fácil, es tratar de aprender de los errores y aciertos ajenos y en esos casos la falta de autocrítica no suele

[3] *MOP: Measures of performance*. Indicadores medibles de la calidad de los procesos y de la de los resultados de los mismos, incluida, especialmente en el caso de la inteligencia, la propia calidad de los productos.

[4] *MOE: Measures of effectiveness*. Indicadores del grado de contribución de nuestros procesos a la consecución de los objetivos de la organización.

ser un factor limitante. La guerra de Ucrania ofrece una magnífica ocasión para ello.

Por definición, un estudio de inteligencia *post mortem* debe realizarse cuando la operación o crisis haya finalizado, cuando el *muerto* ya esté frío, cuando los *futuros* a los que se referían las previsiones y los análisis de inteligencia ya formen parte del pasado.

La guerra en curso en Ucrania puede considerarse un campo de pruebas[5], un *escaparate* de tendencias en muchos aspectos y singularmente en relación con la inteligencia. Su análisis es, por lo tanto, de máximo interés. Los aciertos y errores de los beligerantes y de los que les apoyamos; en general todo lo que observamos en el conflicto y en torno a él, puede enseñar mucho y mostrar elementos de un camino por el que previsiblemente transitaremos en el futuro.

Por desgracia la guerra continúa y es, por tanto, muy prematuro acometer cualquier estudio profundo al respecto. Al intentar un modesto análisis, como el que propone este artículo, debemos asumir que será parcial y muy condicionado por la niebla cognitiva que envuelve, no solo a los beligerantes, sino también a los observadores externos de la guerra. Una *niebla* agravada por el *ruido de fondo* infodémico que limita nuestra capacidad para verlo todo, para identificar qué es lo importante de aquello que vemos y de lo que no vemos y, más aún, para alcanzar una buena conciencia y comprensión de todo ello y de lo que significa.

Sin embargo, y a pesar de las limitaciones citadas, el análisis del papel y de la actuación de la inteligencia en y en torno a la Guerra de Ucrania y en el proceso que llevó a la invasión del 24 de febrero, son del máximo interés. Con todos los reparos que imponen las consideraciones anteriores y con plena conciencia del carácter limitado de este estudio, pueden, no obstante, hacerse ciertas observaciones que ya merecen una reflexión inicial y ese es el propósito de este breve trabajo.

2. Uso atípico de la inteligencia (audiencias, finalidades)

> «We've been transparent with the world. We've shared declassified evidence about Russia's plans and cyberattacks and false pretexts so that there can be no confusion or cover-up about what Putin was doing. Putin is the aggressor. Putin chose this war. And now he and his country will bear the consequences»[6] president Joe Biden.

[5] Brennan, D. (2022). Russia-Ukraine Cyber War Is 'Test Ground' for NATO. *Newsweek* 90. Disponible en: https://www.newsweek.com/russia-ukraine-war-cyberattack-test-ground-nato-eu-hackers-1745309

[6] *The White House*. (2022). Remarks by President Biden on Russia's Unprovoked and Unjustified Attack on Ukraine. East Room. Disponible en: https://www.whitehouse.

«Over-classification undermines critical democratic objectives, such as increasing transparency to promote an informed citizenry and greater accountability»[7] Avril Haines, directora nacional de Inteligencia EEUU

La inteligencia, como es bien sabido, está primordialmente orientada a la generación y difusión de comprensión acerca del entorno y valoraciones sobre las amenazas que comporta y sobre su posible evolución futura. El destinatario, el consumidor, de dicho conocimiento es normalmente la propia organización o Estado en beneficio de su acción (política, diplomática, militar) en los distintos niveles del diseño, planeamiento y conducción de la acción.

Sin embargo, este modelo no es único. Más aun, como veremos más adelante, en el camino que llevó a la invasión del 24 de febrero y en la subsiguiente guerra de Ucrania, se han podido observar, con gran frecuencia e intensidad, otros patrones que merecen una reflexión. Algunos analistas sugieren incluso que se está produciendo un cambio de paradigma en el uso que hacen los decisores de la inteligencia y en la relación de la inteligencia con el entorno.

La difusión de inteligencia a audiencias distintas de la genérica mencionada en el primer párrafo de este apartado no es nueva[8] [9] [10] [11], pero en torno a la guerra de Ucrania este fenómeno ha alcanzado cotas nunca antes vistas[12]. La difusión citada no tiene como finalidad, en esos casos, que las pro-

---

gov/briefing-room/speeches-remarks/2022/02/24/remarks-by-president-biden-on-russias-unprovoked-and-unjustified-attack-on-ukraine/

[7] *Nextgov*. (2023). The National Intelligence Director: Over-Classification Undermines Democracy. Disponible en: https://www.nextgov.com/cxo-briefing/2023/01/national-intelligence-director-over-classification-undermines-democracy/382367/

[8] *FOIA*. (2016). *The role of intelligence during the Cuban missile crisis*. General CIA Records. Disponible en : https://www.cia.gov/readingroom/document/cia-rdp-85g00105r000100040005-5

[9] SNIE. (1962). *The military build up in Cuba*. Disponible en: https://www.cia.gov/readingroom/docs/DOC_0000242425.pdf

[10] *Timegoggles*. (2019). Photos from history: Presence of Soviet missiles in Cuba triggers crisis. Disponible en: https://timegoggles.com/news/archives/photos-from-history-presence-of-soviet-missiles-in-cuba-triggers-crisis/collection_0fa1acc4-ef67-11e9-8a8f-570537186298.html#10

[11] Dilanian, K. et *al*. (2022). In a break with the past, U.S. is using intel to fight an info war with Russia, even when the intel isn't rock solid. *NBC news*. Disponible en: https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014

[12] [1]2 *CNAS* (2022). War in Ukraine: Declassifying Intel. «The declassification of intelligence before and after the Russian invasion of Ukraine was unprecedented in its speed, and lauded for its accuracy. Releasing the intel has been credited with stopping the spread of Russia's false justification for launching an invasion, but in the end did not deter Russia from starting a war with its neighbor. A panel of intel experts gather to

pias decisiones sean más correctas para mejorar las opciones de éxito en la acción. Busca, por el contrario, influir en el entorno, configurarlo en nuestro beneficio y en último término, contribuir así también indirectamente al éxito.

Podemos identificar distintas modalidades de esta difusión configuradora del entorno y todas ellas han sido visibles en los últimos meses en torno a la escalada previa, a la propia guerra de Ucrania y al contexto geopolítico en que se desarrolla.

En primer lugar, la difusión puede hacerse para influir en actores amigos o aliados. Esta difusión normalmente busca el acercamiento de las posiciones de otros actores a las propias para recabar apoyos o dar solidez a una posición política o a un planteamiento estratégico común. Así lo hizo la inteligencia norteamericana en 2003 para buscar apoyo a su posición sobre Irak[13] y contribuir a la formación de una gran coalición internacional. Un patrón análogo se ha observado en torno a Ucrania en los últimos meses.

Con la difusión se puede también intentar influir análogamente en actores neutrales externos, buscando su apoyo o el mantenimiento de su neutralidad.

En el marco de la batalla por los *corazones y las mentes*, la difusión también puede dirigirse a la población para conformar el campo de batalla cognitivo y alcanzar no solo la *information superiority* (función clásica de la inteligencia) sino también la *narrative superiority* mediante el reforzamiento de la credibilidad de nuestros mensajes.

Queda por citar en último lugar uno de los casos más interesantes: la difusión dirigida al enemigo, a sus dirigentes, para modelar sus decisiones. En este caso, se trata de configurar la conciencia situacional y las valoraciones del liderazgo adversario con fines disuasorios o bien para intentar que incurra en errores a nuestra conveniencia. El caso más habitual es la difusión disuasoria basada en el simple y poderoso mensaje subyacente de *no hagas lo que estás pensando hacer porque ya sé que estas a punto de hacerlo*[14]. También puede intentar promoverse, mediante un mecanismo análogo, la actuación enemiga en una dirección que pueda llevarle al fracaso o a una sobreactuación de la que se deriven beneficios políticos o militares para el difusor de dicha inteligencia.

---

discuss the process of declassification, and the impact it has played in the Russian war». Disponible en: https://conference.cnas.org/session/declassifying-intel/

[13] *History* (2023). Secretary of State Colin Powell speaks at UN, justifies US invasion of Iraq. Disponible en: https://www.history.com/this-day-in-history/secretary-of-state-colin-powell-speaks-at-un-invasion-of-iraq

[14] Nowroozi, K. (2022). Intelligence Sharing as A Deterrent and A Method of Warfare. *Security and Politics*. Disponible en: https://kavon.substack.com/p/intelligence-sharing-as-a-deterrent

No hay duda de que en las semanas anteriores al inicio de la invasión y también después de la misma, las distintas inteligencias nacionales — la norteamericana, británica, rusa y ucraniana—, han hecho un amplio uso de estas metodologías. Lo han hecho para, según los casos, buscar el apoyo de aliados, recabar apoyo de la propia población rusa a la invasión, fortalecer el espíritu de resistencia de la población ucraniana, fomentar el apoyo militar y otros tipos de ayuda a Ucrania, disuadir a Rusia de actuar militarmente contra Ucrania (antes de la invasión) y a China y a otros estados de dar una apoyo abierto e incondicional a Rusia —sobre todo después de la invasión y hasta la fecha—, contribuir a la cohesión de la posición europea y de su convergencia con la anglo-norteamericana, etc.

Es cierto que la difusión de inteligencia de acuerdo con estos modelos no es nueva. Resulta fácil identificar ejemplos de ello en el pasado. Sin embargo, no es menos cierto que nunca antes en la historia se había producido un volumen de desclasificación de inteligencia para su difusión comparable al de la guerra de Ucrania[15].

Se puede decir que en torno a la guerra de Ucrania se está observando un uso muy abundante de la inteligencia con fines que se podrían llamar «atípicos» y quizás se esté consolidando una tendencia de cambio de paradigma en la difusión de la inteligencia. Una tendencia que acerca la inteligencia al ámbito de la comunicación estratégica, que sustituye, en ciertos casos, las paredes blindadas de los archivos de inteligencia por *escaparates transparentes*. Una tendencia que vincula la búsqueda de la superioridad en el conocimiento de la situación a la superioridad en la confrontación de narrativas.

Estos *usos atípicos* de la difusión de inteligencia e incluso de su producción *ad hoc* en beneficio de la influencia orientada a la decepción, a la disuasión, al fortalecimiento de la cohesión o a cualquier otra finalidad, no deben desdeñarse. Probablemente han llegado para quedarse. Sin embargo, este asunto requiere reflexión, desarrollo conceptual y procedimental. Cuando se acometa esta tarea deberán considerarse, entre otros aspectos, los riesgos colaterales de la sobredifusión que también se recogen de forma superficial más adelante en este documento y que se deben aprender a valorar adecuadamente[16] [17].

---

[15] Harrington, J. (2022). Intelligence disclosures in the Ukraine crisis and beyond. *War on the rocks*. Disponible en: https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/

[16] CIA. Conferencia de Marzo de 1954 sobre «Dissemination of intelligence» (Approved for release CIA-RDP78-033662A0007000330001-8). Disponible en: https://www.cia.gov/readingroom/docs/CIA-RDP78-03362A000700030001-8.pdf

[17] *Firstpost*. (2022). Explained: The risks countries are facing for sharing intelligence inputs over the Ukraine war. Disponible en: https://www.firstpost.com/explainers/explained-the-risks-countries-are-facing-for-sharing-intelligence-inputs-over-the-ukraine-war-11341881.html

Una variante a esta difusión atípica de inteligencia producida con rigor sobre la base de las informaciones obtenidas y evaluadas con los procesos y los estándares de calidad requeridos, es la *fabricación* de *inteligencia* completamente desvinculada de la realidad, de la verdad. Esta *fabricación* puede hacerse con algunos de los fines mencionados anteriormente: influir en aliados, disuadir a enemigos, configurar el entorno cognitivo para alcanzar la superioridad en la narrativa,... Es cierto que en sentido estricto esa *inteligencia* no merece siquiera tal denominación, pero no deja de tener relación con el tema de este artículo. Además, esta práctica más allá de si encaja taxonómicamente o no en esta categoría, o si más bien debemos considerarla solo como desinformación, ha sido ampliamente empleada por Rusia, y probablemente no solo por Rusia en este conflicto[18] [19]. Lo cierto es que esta *fake intelligence* contamina e interactúa —distorsionándolo— con el ciclo de inteligencia del adversario y, en todo caso, añade *niebla* a la *niebla de la guerra*.

3. Los vectores de la difusión

Cuando hablamos del uso habitual, canónico, de la inteligencia, no tiene mucho sentido utilizar el término vectores que aparece en el título de este párrafo. Los sistemas nacionales de inteligencia y de seguridad nacional, así como las organizaciones de inteligencia internamente, disponen de canales para ordenar sus flujos de trabajo y de difusión de inteligencia.

Cuando hablamos del resto de los casos, sí que se observa una variedad de canales e incluso vectores indirectos de difusión que merecen un comentario.

El proceso parte siempre de una decisión de difundir algo con una finalidad y para ello, se deben desclasificar o reclasificar productos de inteligencia o de la información que contienen. A partir de ahí, por supuesto, existen canales formales, y en muchos casos permanentemente operativos, para el intercambio bilateral o multilateral de inteligencia entre países y también existen herramientas para los intercambios discretos. En el caso de los países aliados que comparten pertenencia a organizaciones internacionales de seguridad y defensa, este intercambio es rutinario y se apoya en mecanismos muy sólidos y permanentes.

En otros casos, los productos de inteligencia y más frecuentemente la información que contienen, o parte de ella, es transferida a los canales de

[18] *Felgenhauer*, P. (2017). Russian Military Spreads Fake Intelligence. The Jamestown Foundation. Disponible en: *https://jamestown.org/program/russian-military-spreads-fake-intelligence/*

[19] *Ukrinform*. (2022). Russian intelligence creates fake website to discredit Zelensky. Disponible en: https://www.ukrinform.net/rubric-polytics/3566988-russian-intelligence-creates-fake-website-to-discredit-zelensky.html

la comunicación pública a través de las notas o declaraciones oficiales de los departamentos de comunicación u oficinas de prensa de los organismos gubernamentales.

El paradigma que describe el párrafo anterior lleva la difusión al ámbito resbaladizo en el que las acciones de influencia encuentran sus *municiones* cognitivas en la inteligencia. Ese es también es el caso que observamos cuando se utilizan vectores de difusión no convencionales ni formales al servicio del propósito de esas acciones difusoras *atípicas*. Un caso paradigmático, y sin duda el más frecuente en este ámbito, es el del periodista que publica sus crónicas o valoraciones empezándolas con la clásica frase: «según fuentes de la inteligencia de...»[20]. A veces esta transferencia, aunque sea intencional, se disfraza de fuga de información o de indiscreción. Puede ocurrir que esos periodistas sean conscientes de ser una pieza de un mecanismo atípico de difusión de inteligencia para la influencia. Sin embargo, en muchos otros casos. quizás sean completamente inconscientes de ello y se sientan afortunados de la ocasión de *brillo* profesional que les brindan *sus fuentes*. El resto del *trabajo* lo harán los medios de comunicación y su habitual tendencia a la redifusión con efecto de eco multiplicador en esa caja de resonancia mediática que es el entorno de la información.

4. Los riesgos de la sobredifusión

El citado uso atípico de la inteligencia tiene mucha capacidad para la configuración del entono del conflicto, pero, sin duda, comporta también riesgos que pueden llegar a desaconsejarlo y que, en todo caso, deben ser valorados convenientemente.

En primer lugar, hay un riesgo evidente: la transferencia de productos de inteligencia de los canales reservados al acceso público, los pone en conocimiento de nuestros oponentes que pueden adaptar en consecuencia sus *modus operandi*, sus técnicas, tácticas y procedimientos. El impacto de este fenómeno es especialmente importante en relación con las acciones de nuestros enemigos o competidores para protegerse de nuestras actividades de obtención. En algún caso, puede llegar a resultar en la neutralización de fuentes de obtención de información o en la reducción de la eficacia operativa de determinadas técnicas, tácticas y/o procedimientos de obtención.

La difusión de lo que sabemos acerca de los planes del enemigo realizada con intención disuasoria pudiera también, en algún caso, generar paradójicamente el efecto contrario. Producir una aceleración de su acción al verse apremiado por el aparente buen progreso de nuestra conciencia situacional

[20] Marinho, J. (2016). Journalists and Intelligence Services. *Marinho Media Analysis*. Disponible en: http://www.marinho-mediaanalysis.org/articles/Sep-02-2016/journalists-and-intelligence-services

acerca de sus intenciones. Esta dinámica de respuesta en nuestro adversario, que responde a la lógica «cuanto más esperemos, peor será», puede en ciertos casos desencadenar inmediatamente aquello que se estaba tratando de impedir mediante la difusión disuasoria de inteligencia.

Otro riesgo tiene que ver con la lógica de que cuando ya se han mostrado las cartas no hay margen para elegir cómo continuar la partida. Hacer público el propio conocimiento sobre ciertos aspectos de nuestro oponente y de sus planes o sus acciones reprochables, condiciona a nuestro enemigo, pero también puede limitar nuestras propias opciones de negociación, de desescalada, de disuasión ulterior, de decepción... En ciertos casos podemos llegar a ser esclavos de nuestra propia difusión.

Por último, hay un riesgo relacionado con el conocido fenómeno de la *self negating prophecy*, versión en negativo del aún más famoso *self fulfilling prophecy*[21].

En ocasiones la difusión disuasoria («no lo hagas, ya sé lo que estas preparando») puede alcanzar el efecto que busca, que, sin duda, puede considerarse un éxito operativo. Sin embargo, a los efectos de la valoración *post mortem* de la efectividad de la inteligencia y su impacto en su prestigio y credibilidad, los vaticinios incumplidos podrían simplemente ser vistos como predicciones excesivamente desfavorables («veis como no ha pasado nada»), un caso más del *típico* exceso de dramatismo de la comunidad de inteligencia en sus estimaciones sobre la amenaza y las líneas de acción del enemigo.

Tristemente, serán pocos los que piensen que esa difusión en concreto pueda haber sido la que haya evitado que ocurriera aquello de lo que se alertaba. La mayoría tenderá a creer que se ha tratado de un simple vaticinio que no se ha cumplido, con la erosión que esto tiene siempre sobre el prestigio y credibilidad de las organizaciones de inteligencia. Se trata de un dilema en el que deberán valorarse beneficios y perjuicios para buscar soluciones de compromiso y, en algún caso, aceptar posiciones extremas si el balance ventajas-inconvenientes resulta favorable.

5. El prestigio y la credibilidad

> «Mistrust in intelligence has serious consequences for the effectiveness of intelligence agencies[22]».

[21] Cole, N. L. (2019). Definición de profecía autocumplida en sociología». *Greelane*. Disponible en: https://www.greelane.com/es/ciencia-tecnolog%C3%ADa-matem%C3%A1ticas/ciencias-sociales/self-fulfilling-prophecy-3026577/

[22] Matei, F. C. y Halladay, C. (2019) The conduct of intelligence in democracies: Processes, practices and cultures. ISBN 978-1-62637-769-1. Disponible en: https://www.tandfonline.com/doi/full/10.1080/23800992.2019.1695719

Uno de los procesos más importantes y conocidos del ciclo de inteligencia es el de valoración de la credibilidad de las informaciones obtenidas y de la fiabilidad de las fuentes de información.

Hay otro asunto que normalmente no se considera de manera sistemática, ni lo recogen nuestros procedimientos ni hay métodos para su cuantificación, pero que también merece ser considerado. El prestigio y credibilidad de los analistas, de los oficiales responsables de inteligencia, y hasta el de cada organización de inteligencia en su conjunto, es asimismo objeto de valoración, aunque sea de manera espontánea e informal. Esta valoración se basa en la calidad del desempeño, pero, sobre todo, en lo que mejor puede observarse, su historial de éxitos o fracasos.

La credibilidad que se dé —en su propia organización— a los asesoramientos, a las valoraciones, juicios y recomendaciones de la inteligencia procede, sin duda, de lo que contengan los productos de inteligencia y del rigor en la aplicación de las metodologías de valoración de credibilidad y fiabilidad. Sin embargo, también depende, en gran medida, de algo tan subjetivo como es el prestigio y la credibilidad del propio analista y del oficial responsable de inteligencia. Este prestigio, y el crédito asociado al mismo, pueden atribuirse asimismo a las organizaciones o estados y de él depende, en gran medida, que las valoraciones y los consejos que explícita o implícitamente contengan dichos productos sean considerados y trasladados a la acción.

Es por ello que el prestigio de las organizaciones de inteligencia y el de sus componentes individuales debe cuidarse como un valioso bien a proteger. La guerra de Ucrania y las fases anteriores al inicio de la invasión ha dado ejemplos de lo difícil que resulta *limpiar* las manchas del pasado en el *expediente*, en el *historial* de los estados y de sus organizaciones de inteligencia y como estas afectan a su credibilidad en el presente. La dificultad encontrada por la inteligencia norteamericana y británica para que sus valoraciones fueran compartidas por algunos aliados en las semanas anteriores a la invasión, a pesar del gran flujo de difusión de productos que las apuntalaban, puede haberse debido a la erosión de su prestigio por graves fallos con trascendencia global cometidos en el pasado.

6. Contar tanques es fácil, predecir intenciones es difícil

En inteligencia normalmente diferenciamos las necesidades de la conducción de las que tiene el diseño y planeamiento de las operaciones. Efectivamente, la conducción es ávida consumidora de conciencia situacional y el planeamiento requiere estimaciones sobre el futuro. En ambos casos se deben hacer valoraciones sobre lo que significa lo que *vemos*, en un proceso para el que en lengua inglesa se emplea la atractiva secuencia de verbos: *sense-make sense*.

De ambos procesos lo verdaderamente difícil es el *make sense*. Observar disposiciones de unidades militares y geolocalizarlas es relativamente fácil si se dispone de medios de vigilancia y reconocimiento. No es difícil, y cada vez lo será menos, detectar y *contar* buques, aviones, vehículos de combate y situar esos objetos (Battle Space Objects, BSO) en el mapa de situación con el valor añadido de un cierto análisis y etiquetado.

Por el contrario, anticipar intenciones para configurar la propia acción ofensiva o defensiva en base a estimaciones de calidad sobre las intenciones y los conceptos de operaciones del enemigo es mucho más difícil. Valorar la magnitud de la potencia de combate de las unidades que se observan y, por tanto, sus opciones de éxito en los enfrentamientos militares es extremadamente difícil, como se ha señalado con insistencia. Este problema afecta a la inteligencia militar en todos los niveles de la conducción de la guerra y de las operaciones.

La derivada de todo esto —para el asunto que interesa aquí—, es la dificultad, pero también la importancia, de la evaluación de esos elementos no físicos y también de su detección, lo que representa un reto mayúsculo para la inteligencia de los *corazones y las mentes*, la inteligencia del ámbito cognitivo.

Análogamente podríamos añadir que los aspectos culturales de las organizaciones militares pudieran ser susceptibles de evaluación como catalizadores o como inhibidores de su éxito en el diseño, planeamiento y ejecución de las actividades militares. Aun a falta de un estudio sistemático, resulta, no obstante, evidente que las FAS rusas padecen el efecto de su propia y fuertemente arraigada cultura de freno sistemático a la iniciativa y de su modelo de liderazgo rígido y autoritario[23]. Esta cultura, que es conocida y cuyo impacto en los fracasos tácticos ha sido ya suficientemente señalada[24], puede estar también detrás de una de las posibles causas del grave error estratégico que cometió el presidente de la Federación Rusa cuando invadió Ucrania. Sus asesores, como quedo de manifiesto en una famosa grabación de su jefe de inteligencia, más que aumentar la comprensión y conciencia

[23] Watling, J. (2022). Russia's underperforming military capability may be key to its downfall . *The Guardian*. «Fear of punishment has created a military in which soldiers will doggedly implement orders even when they no longer make sense. For example, Russian artillery units routinely prosecute targets in the order that they receive fire missions, with no contextual prioritisation. Even when new intelligence indicates a target has moved, Russian units will often engage the previous location and then the new one, giving the target time to move once more». Disponible en: https://www.theguardian.com/world/2022/sep/18/russia-military-underperforming-ukraine

[24] Frías, C. J. (2022). Ucrania y el Ejército ruso: primeras impresiones (II). Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO71_2022_CARFRI_Ucrania.pdf

situacional de Vladimir Putin, parecían ser una caja de resonancia de sus ideas sesgadas y preconcebidas evitando desagradar al *Jefe*[25].

Análogamente al razonamiento de la potencia de combate y la capacidad de combate de párrafos precedentes, nadie duda que la cultura de las organizaciones puede ser *lubricante* o puede ser *arena* en sus engranajes. Entre otros *pecados* de su acervo organizacional, la cultura ruso-soviética de la jerarquía rígida contraria la iniciativa parece que ha sido y está siendo una rémora. A pesar de la enorme dificultad para el manejo de elementos intangibles en los juicios y valoraciones predictivas en inteligencia, debemos mejorar nuestra manera de medirlos, evaluarlos e integrarlos en nuestros estudios y *wargamings* para evitar sonados fracasos como los cometidos por casi todas las inteligencias estatales, multinacionales y por muchos *think tanks* en Occidente en la evaluación de la potencia de combate, de la verdadera magnitud de la capacidad militar rusa.

Un análisis cargado de la inteligencia actual y sustentado en la inteligencia básica es importante y es una de las bases de la conciencia situacional y sobre ella se construyen las estimaciones de evolución de la situación. Sin embargo, aún más importante que tener la *fotografía* de la disposición física de los elementos, incluso de la fotografía anotada y etiquetada, es poder valorar adecuadamente esos elementos subjetivos en los que radica la verdadera naturaleza de la amenaza y el efecto de esos BSO en nuestra potencial actuación y opciones de éxito. Conocer, anticipar, entender las intenciones, voluntades de resistencia, previsibles reacciones de los comandantes ante la presión y otros elementos abstractos e intangibles es mucho más importante y supone un gran reto para la inteligencia. Un reto difícil de superar con éxito. Algo que ya sabíamos y que Ucrania nos ha recordado.

Casi todo el mundo reconoce los graves errores cometidos en relación con las estimaciones sobre la posible invasión rusa de Ucrania y, una vez producida, acerca de la evolución posterior de la misma. Por los motivos mencionados, ha habido errores en la evaluación de las capacidades de las Fuerzas Armadas rusas y también en la de las ucranianas.

Sin duda, lo que falló en ese cálculo, no se debió a un *recuento* incorrecto de los medios militares de los beligerantes, sino que tuvo que ver con los citados aspectos intangibles, y por tanto, difícilmente cuantificables. La voluntad de resistir, la conciencia de estar *haciendo lo correcto*, la confianza en el mando o la disciplina en todas sus dimensiones son clave en esta ecuación. En esa categoría de elementos, mencionada de forma repetitiva en las líneas precedentes, radica la explicación a la inesperada resiliencia del

[25] *La Vanguardia*. (2002) Putin humilla a su jefe de inteligencia en una reunión de alto nivel sobre Ucrania: «¡Habla claro!». Disponible en: https://www.youtube.com/watch?v=z0ZWg-FFkVRQ

pueblo ucraniano y también en ellos hay que buscar algunas de las debilidades incomprensibles de la maquinaria militar rusa. Podríamos decir que «el mejor *hardware* no sirve de nada sin un buen *software* cultural y moral».

Los sistemas de indicadores de alerta estratégicos pueden establecer multitud de parámetros a monitorizar, medir y trasladar a sistemas complejos de integración para su análisis. No obstante, la emisión, o no, de alertas derivadas de ese estudio de indicadores tiene mucho de valorativo, de subjetivo. No siempre la concentración de tanques anticipa la voluntad de usarlos en una acción ofensiva. No hay duda de que debemos aprender a parametrizar e integrar mejor los intangibles culturales y morales mencionados, en nuestros sistemas de la inteligencia de alertas en beneficio de la anticipación estratégica u operacional.

Una prueba de las limitaciones de estos sistemas fue el mantenimiento de la posición de la *Direction du Renseignement Militaire* (DRM) francesa y de algunas otras organizaciones, que consideraron poco probable la invasión hasta las vísperas mismas de su inicio. Como es sabido, esta situación provoco el cese, pocos días después, del Director de la DRM, General Eric Vidaud[26].

Es cierto que nada de lo dicho en los párrafos precedentes es una novedad, pero también lo es que la guerra de Ucrania ha sido un recordatorio de hasta qué punto toda la tecnología, todos los sensores, todo el *hardware* y *software*, toda la analítica avanzada acaban chocando con nuestra incapacidad para obtener y descifrar nuestras más deseadas y necesarias necesidades de inteligencia: lo que piensan, lo que pretenden y lo que asusta a los comandantes adversarios.

7. La tecnología y la democratización de la inteligencia

La ciencia y la tecnología han sido históricamente una constante configuradora de la actividad militar. Las tecnologías han ido desarrollándose como soluciones ofensivas o defensivas contra otras tecnologías defensivas u ofensivas existentes. Su aparición ha sido casi siempre un catalizador de cambios en las doctrinas, los procedimientos y en las organizaciones. A veces, no siempre, estas novedades hacen su aparición como *huracanes* disruptivos que cambian las *reglas del juego* y provocan grandes modificaciones en el modo de hacer la guerra o de evitarla.

La guerra de Ucrania ha sido el escenario de muchas novedades tecnológicas ya intuidas o anticipadas en nuestras previsiones, pero que en pocas ocasiones habíamos visto materializarse hasta ahora en un contexto real

[26] *Midi Libre* (2022). Pourquoi le directeur du renseignement militaire français va-t-il quitter son poste ? Disponible en: https://www.midilibre.fr/2022/03/31/pourquoi-le-directeur-du-renseignement-militaire-francais-va-t-il-quitter-son-poste-10205898.php

de acción militar. Algunas de estas novedades, también en el ámbito de la inteligencia, han tenido un impacto muy significativo en el desarrollo de los acontecimientos.

La inteligencia de fuentes abiertas y de redes sociales (RR.SS.) no es nueva para las comunidades de inteligencia, pero ambas, y especialmente esta última, han tenido una importancia nunca antes vista en anteriores conflictos bélicos. Las herramientas analíticas y de rastreo disponibles han convertido a las RR.SS. en una valiosa fuente de información[27]. Su contribución a la inteligencia militar, y a través de ella, a la acción operativa ha sido muy importante en la guerra de Ucrania y se ha materializado en innumerables facetas entre las que se pueden mencionar las siguientes:

- Identificación de personas fallecidas.
- Identificación positiva de individuos de alto valor susceptibles de ser objetivos.
- Geolocalización de personas y/o unidades.
- Identificación de materiales significativos.
- Captura de imágenes o videos para su uso en el ámbito de las acciones de influencia.

En el campo de la identificación biométrica de personas o la identificación de objetos a partir de sus elementos físicos reflejados en imágenes o video, los avances de los últimos años han puesto en manos de los beligerantes (especialmente de Ucrania) herramientas de *software* que han sido usadas con gran éxito. Han sido empleadas en el análisis, valoración y preparación de la acción (letal o no letal) sobre objetivos, lo que conocemos como *targeting*. También han contribuido a la generación y mejora del llamado orden de batalla (identificación y disposición) de las fuerzas adversarias, así como a las acciones de guerra psicológica, algunas marcadamente agresivas, en el contexto del cruento enfrentamiento que ha venido librándose en el ámbito cognitivo[28].

En el campo de la inteligencia de imágenes, esta guerra ha puesto de manifiesto el papel de los proveedores comerciales de imágenes e incluso de aquellos que, quizás con fines muy lejanos a la inteligencia militar, las proporcionan con carácter libre y gratuito[29].

---

[27] *The Economist* (2022). The invasion of Ukraine is not the first social media war, but it is the most viral. Disponible en: https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456

[28] Weiss, Michael. (2022). Inside Ukraine's Psyops on Russian and Belarusian Soldiers. *New Lines Magazine*. Disponible en: https://newlinesmag.com/reportage/inside-ukraines-psyops-on-russian-and-belarusian-soldiers/

[29] Ignatus, D. (2022). How the algorithm tipped the balance in Ukraine. *Washinton Post*. «In our Kherson example, Palantir assesses that roughly 40 commercial satellites will pass over the area in a 24-hour period». Disponible en: https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

No hay duda de que uno de los protagonistas de esta guerra han sido las aeronaves tripuladas remotamente. La guerra de Nagorno-Karabaj[30] fue, probablemente, la primera guerra en la que este tipo de medios tuvieron un papel importante, en algún caso decisivo, pero Ucrania está siendo la consolidación del *reinado* de los RPAS en las actividades de ataque y desde luego también de ISR[31]. Un reinado previsible y previsto, que no sorprende a nadie y que estamos observando con nitidez.

En definitiva, la tecnología al servicio de la obtención y el análisis de inteligencia no solo ha avanzado, sino que se ha hecho accesible, se ha *democratizado* hasta el punto, como se analizará en el próximo apartado, de estar disponible en manos incluso privadas.

8. Multidominio, ISR atípico[32], *crowdsourcing intelligence*[33]

La noción de entorno operativo multidominio y operaciones militares que integran acciones en los dominios físicos y no físicos no es estrictamente nueva, se lleva hablando de ella casi una década[34]. Sin embargo, la guerra de Ucrania la está mostrando en su máxima expresión. Los proyectiles físicos y la destrucción que provocan, conviven con la batalla en el ciberespacio y también con las bombas cognitivas portadoras de *submuniciones* generadoras de confusión y desmoralización. Hace algunos años que las Fuerzas Armadas occidentales, incluidas las españolas, hemos empezado a aproximarnos al ámbito cognitivo, considerándolo ya sin paliativos un espacio de confrontación, quizás ni siquiera secundario[35].

---

[30] Dyxon, R. (2022). *The Washington Post*. Disponible en : https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441b-cbd2-193d-11eb-8bda-814ca56e138b_story.html

[31] JISR: Joint intelligence, surveillance and reconnaissance, actividades conjuntas de Inteligencia, Vigilancia y Reconocimiento. En general el concepto de ISR o Joint ISR-JISR nace para poner el énfasis en la agilidad del apoyo a las operaciones y al ciclo de targeting (análisis, valoración, ataque a objetivos, con acciones físicas o no físicas, letales o no letales).

[32] Conocido como *non-traditional ISR*.

[33] McCabe, M. (2019). What is Crowdsourcing Intelligence? *Intelligence Fusion*. Disponible en: https://www.intelligencefusion.co.uk/insights/resources/article/what-is-crowdsourcing-intelligence/

[34] McCoy, K. (2017). The road to multi-domain battle: an origin story. *Modern War Institute*. Disponible en: https://mwi.usma.edu/road-multi-domain-battle-origin-story/#:~:text=The%20origins%20of%20Multi-Domain%20Battle%20can%20be%20traced,will%20create%20and%20the%20solutions%20it%20will%20require.

[35] Goldstein, Simon (2020). A British Perspective On Information Manoeuvre. *Defstrat*. Disponible en: https://www.defstrat.com/magazine_articles/a-british-perspective-on-information-manoeuvre/

Las operaciones multidominio requirieren, como resulta evidente, inteligencia (y por ende ISR) multidominio[36]. La máxima expresión de la inteligencia multidominio son los episodios, cada vez más frecuentes, de lo que podríamos llamar *cross domain cueing* [37] y del apoyo a las acciones letales mediante la obtención y el procesamiento de inteligencia en los ámbitos no físicos del entorno operativo.

Ucrania ha mostrado casos de éxito en los procesos mencionados, en la inteligencia de redes sociales, en el análisis de sus flujos, de sus mensajes y en el procesamiento de sus materiales gráficos con fines de inteligencia. Una inteligencia con efecto en la conciencia situacional acerca de los ámbitos no físicos, pero también en la comprensión holística del entorno en sus múltiples dimensiones. Una inteligencia que cataliza acciones en el mundo físico desde la inteligencia en los ámbitos no físicos.

Otro aspecto significativo, otra tendencia en curso, es el llamado ISR atípico o *non-traditional ISR* (NTISR)[38]. Este concepto nació en referencia a los sensores no específicos de inteligencia de plataformas y sistema de armas, pero puede ahora aplicarse a sensores de toda índole, como las cámaras de los teléfonos móviles[39], de los sistemas seguridad de edificios o de los sistemas de control de tráfico que son valiosos contribuyentes potenciales a la obtención ISR.

Por otra parte, en la guerra Ucrania, y en torno a ella, está brillando como nunca antes la creciente facilidad para que ciudadanos normales puedan realizar el seguimiento y análisis de la guerra desde el salón de su casa. Se puede decir que la guerra de Ucrania está ofreciendo a los analistas *freelance* un festín de fuentes abiertas[40] e incluso de información del entorno que pueden consumir en tiempo real o casi real. Esta facilidad de acceso a la información en fuentes abiertas, favorecida por el cambio de paradigma en la difusión citado

[36] Atkins, S. A. (2018). Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace. *OTH Over The Horizon*. Disponible en: https://overthehorizonmdos.wpcomstaging.com/2018/09/12/multidomain-observing-and-orienting-isr-to-meet-the-emerging-battlespace/

[37] Pang, C. et *al*. (2017). Multi-Sensor Cross Cueing Technology and Its Application in Target Tracking. *ResearchGate*. Disponible en: https://www.researchgate.net/publication/317750654_Multi-Sensor_Cross_Cueing_Technology_and_Its_Application_in_Target_Tracking

[38] Deway, D. (2022). Here are 4 ways Non-traditional ISR can accelerate time to insight. *C4ISRnet*. Disponible en: https://www.c4isrnet.com/cyber/2022/10/31/here-are-4-ways-non-traditional-isr-can-accelerate-time-to-insight/

[39] Brodsky, S. (2022). How mobile phones are changing war in Ukraine. *Digitaltrends*. Disponible en: https://www.digitaltrends.com/mobile/ukraine-phones-warfare/

[40] *The Conversation* (2022). Open-source intelligence: how digital sleuths are making their mark on the Ukraine war. *The conversation*. Disponible en: https://theconversation.com/open-source-intelligence-how-digital-sleuths-are-making-their-mark-on-the-ukraine-war-179135

en párrafos precedentes, unida a la disponibilidad de *software* de explotación y análisis —en algunos casos incluso gratuito— proporciona capacidades nunca antes vistas fuera de las agencias oficiales o grandes *think tanks*. Cualquier persona con interés y una mínima formación puede ahora hacer aportaciones significativas al seguimiento y análisis de la guerra que hacen las agencias oficiales o los grandes operadores privados de inteligencia.

Como resulta evidente, lo mencionado en los párrafos anteriores subraya la magnitud de las capacidades privadas, tanto en obtención como en elaboración, que pueden ponerse al servicio del esfuerzo colectivo de inteligencia. La *crowd intelligence/crowdsourcing intelligence* (inteligencia colectiva) que aparece en el título del párrafo es, sin duda, una tendencia y una dimensión novedosa del concepto clásico del *pueblo en armas*, aplicado específicamente al campo de la inteligencia.

9. Obtención en entornos degradados

En la guerra de Ucrania hemos observado como las acciones de ISR han sido frecuentemente precedidas por acciones degradadoras del entorno para favorecer el efecto de determinadas disciplinas de obtención. Un caso paradigmático ha sido el recurso frecuente y fatal de los jefes militares rusos a las comunicaciones no seguras e incluso a la telefonía GSM ante la degradación de sus redes tácticas de sus comunicaciones militares[41] [42]. En muchos casos sus vulnerabilidades materiales y/o procedimentales preexistentes se han visto intensificadas por la acción de la guerra electrónica ucraniana preparando así el terreno a una efectiva obtención en inteligencia de comunicaciones (COMINT). Estos éxitos en COMINT han llevado, como ha sido ampliamente comentado, a éxitos importantes en la destrucción o neutralización de elementos de mando y control e incluso a la efectiva acción letal contra los propios jefes militares usuarios de medios de comunicación no seguros. Estos casos de uso han sido ejemplos paradigmáticos de la interacción sinérgica entre la guerra electrónica, la inteligencia de comunicaciones y las acciones de destrucción física de objetivos.

10. Debilidades de Rusia, oportunidades para Ucrania

La superioridad en conciencia situacional, en comprensión del entorno, la llamada *information superiority* es un pilar clave del éxito militar. Rusia

[41] Frías, C. J. (2022). Ucrania: la guerra de los teléfonos móviles. Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO112_2022_CARFRI_Ucrania.pdf

[42] Frías, C. J. (2022). Ucrania y el Ejército ruso: primeras impresiones (II). Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO71_2022_CARFRI_Ucrania.pdf

parece haber tenido y estar teniendo dificultades en ese ámbito, tanto por sus limitadas capacidades de obtención como en relación con el procesamiento-fusión, y probablemente, también en la alimentación de sus decisiones relativas al diseño y la conducción de la guerra. Precisamente en este campo, con un gran apoyo[43] exterior, recibido antes y durante la guerra, Ucrania ha sustentado, sin duda, una gran parte de sus éxitos.

En relación con la inteligencia militar de las fuerzas rusas en los niveles operacional y táctico, parecen observarse deficiencias en su ciclo de obtención en apoyo al análisis y valoración objetivos y en la acción sobre ellos (el llamado ciclo de *targeting*). Es cierto que su Fuerza Aérea ha mostrado limitada capacidad, pero sigue siendo sorprendente como ejemplo en este sentido, como señala el general de brigada Carlos Frias[44], el poco éxito a pesar de su capacidad artillera, en la destrucción de los RPAS BAYKTAR cuyas pistas normalmente se encontraban sobradamente dentro del alcance de la artillería rusa y en zonas que, teóricamente, no debieran haber presentado dificultades graves a la obtención ISR rusa [45].

De forma análoga, hay ciertos éxitos ucranianos en el este del país (Jerson, Jarkov) que difícilmente podrían entenderse sin la aparente sorpresa operacional y táctica que alcanzaron frente a las Fuerzas rusas lo que indica, una vez más, la debilidad de su ISR táctico y operacional y de su sistema de indicadores de alerta a esos niveles.

Otro aspecto en el que las deficiencias rusas han propiciado oportunidades a Ucrania han sido los problemas con el sistema de C2 y la debilidad de los escalones Brigada y División[46] [47]. Es en esas deficiencias, unidas quizás a aspectos relativos a la cultura militar rusa, donde hay que buscar la razón de la frecuente presencia de comandantes de los niveles tácticos superiores en los primeros escalones. En su intento de alcanzar conciencia situacional de primera mano y tratar de *conducir* fases principales de la maniobra táctica desde la proximidad de grupos tácticos de 1.º escalón, han ofrecido, en ocasiones, grandes oportunidades para la obtención ISR y el *targeting* ucraniano.

---

[43] Grady, J. (2022). Intel Sharing Between U.S. and Ukraine 'Revolutionary' Says DIA Director. *USNI News*. Disponible en: https://news.usni.org/2022/03/18/intel-sharing-between-u-s-and-ukraine-revolutionary-says-dia-director

[44] Frías, C. J. (2022). Ucrania y el ejército ruso: primeras impresiones. Instituto Español de Estudios Estratégicos (*ieee.es*). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO33_2022_CARFRI_Ucrania.pdf

[45] *Idem.*

[46] *Idem.*

[47] Ripley, T. (2022). Ukraine conflict: Russian military adapts command-and-control for Ukraine operations. *Janes*. Disponible en : https://www.janes.com/defence-news/news-detail/ukraine-conflict-russian-military-adapts-command-and-control-for-ukraine-operations

La debilidad de las comunicaciones tácticas rusas explotada adecuadamente por las Fuerzas ucranianas, unida a una conciencia y disciplina inadecuada en el uso de los teléfonos móviles, ha expuesto a las fuerzas rusas a una vulnerabilidad que ha sido, de nuevo, una oportunidad de oro para la Inteligencia/ISR ucraniana[48].

11. Epílogo

Como quedó advertido en las primeras líneas de este texto, resulta evidente que aquí no se ha hecho un análisis exhaustivo y sistemático del asunto. Sí se apuntan ciertas observaciones preliminares que, sin duda, merecerían un estudio más profundo y riguroso.

Entretanto propongo algunos aspectos acerca de los que la observación inicial de lo ocurrido sugiere una reflexión:

- La inteligencia como modelador del entorno y no solo como herramienta para su comprensión, así como la relación de la inteligencia desclasificada con la influencia, y en particular, con la acción disuasoria.
- La necesidad de mejorar los sistemas de indicadores de alerta estratégicos y de wargaming.
- La creciente dificultad para sustraerse a la obtención ISR enemiga en lo relativo a la disposición de elementos físicos en el entorno operativo y la necesidad de un nuevo modo de alcanzar la sorpresa.
- Los métodos de parametrización y medida de los elementos intangibles que configuran la potencia de combate y la eficiencia de organizaciones y procesos.
- Los mecanismos para mejorar la contribución del ISR atípico y de los contribuyentes externos (privados o corporativos) al esfuerzo de inteligencia (crowdsourcing intelligence).
- La mejora de los mecanismos de ISR multidominio y en particular del X-domain cueing.

[48] Frías, C. J. (2022). Ucrania y el Ejército ruso: primeras impresiones (II). Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO71_2022_CARFRI_Ucrania.pdf

Operaciones de explotación. Inteligencia, vigilancia y reconocimiento en el ciberespacio, una capacidad al servicio de todos los ámbitos

Enrique Castañeda de Benito

1. Introducción

Durante las últimas décadas, el campo de batalla moderno ha experimentado numerosas transformaciones. Uno de los cambios más profundos es la incorporación del ámbito ciberespacial a los conflictos actuales con entidad propia o como apoyo a las operaciones en los dominios tradicionales de tierra, mar y aire. Esta incorporación sitúa al ciberespacio en el centro de la pugna por el bien más preciado de las sociedades contemporáneas: la información.

En la actualidad, multitud de conflictos se desarrollan en zona gris, ya que la intención de los actores es mantener la confrontación por debajo del umbral del conflicto armado. Para ello, los contendientes emplean métodos híbridos para evitar enfrentamientos directos, dificultar la atribución de los ataques, facilitar la denegación plausible de las acciones y, con ello, llevar al adversario a la inacción impidiendo la toma de decisiones y la respuesta frente a las acciones del adversario.

Ilustración 1. Espectro del conflicto. Fuente: Cuadernos de la Guardia Civil, n.º 64. 2021. Disponible en: https://biblioteca.guardiacivil.es/cgi-bin/koha/opac-detail.pl?biblionumber=23000

Todas las características de las estrategias híbridas encajan a la perfección con las posibilidades operativas que otorga el ciberespacio para el desarrollo de operaciones militares. Esto es más acusado si lo observamos desde la perspectiva de las operaciones ofensivas y de explotación.

En este artículo centraremos la atención en la capacidad de explotación y cómo con ella se pueden identificar y aprovechar las oportunidades operacionales que otorga el ciberespacio. Se tratará de explicar que esta capacidad implica la ejecución de actividades relacionadas con la inteligencia, vigilancia y reconocimiento, sirviendo de elemento precursor de cualquier tipo de operación en el ámbito. Junto con estos conceptos, se describirán las capacidades auxiliares a desarrollar para poder acometer estas tareas. También se detallará brevemente cómo estas capacidades pueden ser útiles para apoyar a las operaciones de información.

2. Ciberespacio

El ciberespacio es un entorno artificial que consiste en una serie de sistemas interconectados y debidamente configurados, cuyo objetivo es el tratamiento de información. Una información que resulta más valiosa que los sistemas que la almacenan o transportan. Esta información nos permite representar y modelar la realidad para que personas, organizaciones, sociedades, gobiernos y, cada vez más profusamente, máquinas desarrollen sus actividades, actúen según sus intereses y establezcan las relaciones que, en cada momento, puedan considerar con el resto de actores o usuarios que operan en este entorno.

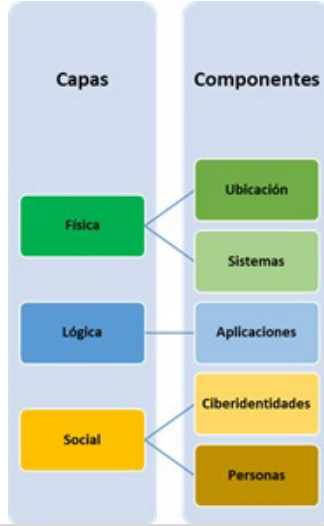


Ilustración 2. Capas y componentes básicos del ciberespacio

Por lo tanto, podemos decir que el ciberespacio tiene una doble vertiente. Por un lado, estaríamos hablando de un conjunto de sistemas y aplicaciones, una vertiente puramente tecnológica que proporciona accesibilidad y

persistencia a la información y, por otro lado, hablaríamos de información, una vertiente puramente cognitiva que influye decisivamente en la forma en la que se percibe el mundo real (economía, política, sociedad, etc.).

Estas dos vertientes se articulan en tres capas (física, lógica y social), que interactúan mediante cinco componentes (sistemas, aplicaciones, usuarios, ciberidentidades y ubicaciones geográficas). Para entender el ciberespacio, se debe comprender la relación existente entre cada uno de los componentes.

3. Operaciones en el ciberespacio

Por consiguiente, podría afirmarse que las operaciones en el ciberespacio tienen dos tipos de objetivos principales; operaciones dirigidas contra los sistemas y operaciones focalizadas en la información. Como podemos intuir, estos dos escenarios no son necesariamente excluyentes. Serán las necesidades operacionales y los efectos deseados los que determinen el tipo de operación a realizar y la necesidad de priorizar unos objetivos sobre otros.

Un ejemplo que puede ilustrar este concepto se observa en el planeamiento de una operación ofensiva de denegación. En este tipo de operación se pretende negar al adversario el empleo de un sistema determinado. Por lo tanto, en este caso, los sistemas serán el objetivo fundamental. Sin embargo, en una operación de explotación intrusiva, la información es el elemento que cobra un valor principal. En esta situación, toda la maniobra deberá ser confeccionada para conseguir obtener la información sin interferir con el buen funcionamiento de los sistemas objetivo. Tampoco hay que olvidar que para acceder a la información será un requisito previo acceder a los sistemas que la contienen, transportan o procesan. Es decir, se deberá atacar a los propios sistemas sin causarles ninguna disrupción, entender el funcionamiento interno de una organización para localizar la información buscada, extraerla de los sistemas adversarios y, por último, explotarla oportunamente.

Junto con los anteriores ejemplos, no debemos olvidar añadir las operaciones de información. Las operaciones realizadas en el ámbito cognitivo, cuyo objetivo es específicamente la información, se desarrollan en multitud de ocasiones a través del ciberespacio, al ser este ámbito el principal vector de difusión que la sociedad conoce hoy en día. En este sentido, el ámbito ciberespacial, si bien no debe involucrarse directamente en la elaboración de los mensajes, puede colaborar con el ámbito cognitivo convirtiéndose en un vector de ataque y de difusión.

En este aspecto, la capacidad de explotación cobra especial relevancia, ya que para desarrollar sus cometidos debe contar con habilidades técni-

cas y operativas que le permitan desenvolverse con agilidad y eficacia en el entorno operativo de información. Las unidades de explotación pueden colaborar estrechamente con el ámbito cognitivo en la difusión de mensajes y campañas, en la ejecución de operaciones de influencia, tanto ofensivas como defensivas, o mediante vigilancia especializada, en la detección y caracterización de campañas dirigidas contra intereses propios. A estas tareas de detección y caracterización se pueden añadir tareas de disrupción de operaciones adversarias mediante la interactuación o infiltración en redes de influencia adversarias.

4. Capacidad de Explotación de Información y Operaciones (CISRO). Inteligencia, vigilancia y reconocimiento en y a través del ciberespacio

Cuando se creó el MCCE[1], se puso especial énfasis en la ejecución de operaciones militares en el ciberespacio. El desarrollo posterior de la normativa de creación articuló tres capacidades militares en el ciberespacio como pilar fundamental para ejecutar estas operaciones. Estas tres capacidades fueron denominadas defensa, ataque y explotación. Si bien las dos primeras tienen actividades, responsabilidades y objetivos más concretos, la tercera es quizá la más compleja de definir.

La capacidad de explotación centra sus actividades sobre el principal recurso que existe en el ciberespacio, la información. El objetivo es facilitar su aprovechamiento para crear oportunidades operativas. Para ello, debe identificarlas y poner la información oportunamente al servicio del resto de operaciones (ofensivas o defensivas propias del ciberespacio o de otros ámbitos).

Ilustración 3. Componentes fundamentales de la amenaza

[1] MCCE: Mando Conjunto del Ciberespacio. Su creación se produjo originalmente como Mando Conjunto de Ciberdefensa (MCCD) el 19 de febrero de 2013. La Orden DEF/710/2020 de 27 de julio fusiona el MCCD con JCISFAS (Jefatura de Sistemas de Información y Telecomunicaciones de las FAS) para que el MCCD se convierta en MCCE.

Cuando se habla de una amenaza creíble, esta debe contar con tres elementos. El primer componente es la capacitación para conseguir sus objetivos. Este elemento debe ir acompañado de la intención o motivación necesarias. Pero indiscutiblemente, la amenaza debe ser capaz de encontrar o fabricar las oportunidades que le permitan lograr que sus capacidades sean puestas de manifiesto.

En este contexto, el rol de la capacidad de explotación es el de explotar la información disponible para crear o encontrar oportunidades operativas. Esto se consigue ejecutando tareas de reconocimiento, vigilancia e inteligencia de objetivos y amenazas.

En términos de acciones ofensivas, las oportunidades se generan encontrando vectores de ataque, vulnerabilidades o potenciales alternativas de maniobra contra un objetivo en cualquiera de las tres capas que conforman el ciberespacio (física, lógica y social) y esto incluye la manipulación e ingeniería social.

En cuanto a operaciones defensivas, la capacidad de explotación debe contribuir descubriendo y analizando motivaciones, entendiendo las capacidades del adversario (TTP –tácticas, técnicas y procedimientos–, esquemas y patrones de comportamiento) para contribuir a su descubrimiento, detección y también para dificultar o denegar su maniobra. Otro aspecto importante será el de desarrollar actividades que identifiquen potenciales ventanas de oportunidad en los recursos propios aprovechables por los adversarios. En definitiva, conocimiento de las capacidades, intenciones y oportunidades que manejan los adversarios (inteligencia de ciberamenazas) para mejorar la respuesta y postura defensiva propia.

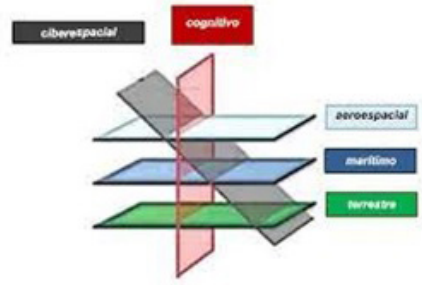


Ilustración 4. Interrelación entre ámbitos de las operaciones según la doctrina de empleo de las FAS. Fuente: PDC-01. Disponible en: https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html

En consecuencia, es lógico pensar que la mayoría de productos obtenidos como resultado de las actividades asociadas serán productos de inteligencia. Estos productos contribuyen al conocimiento de la situación del

ciberespacio y a su caracterización, y deben apoyar el planeamiento y conducción de las operaciones de cualquier ámbito.

La capacidad de explotación y sus actividades CISRO asociadas son un elemento habilitador con un propósito eminentemente táctico, aunque puede tener repercusiones en otros niveles de conducción y planeamiento. La ejecución de estas actividades requiere un planeamiento adecuado que pueda ser implementado para su ejecución sobre un sistema de información que permita gestionar las actividades operativas y del ciclo de inteligencia asociadas.

Este sistema deberá tener capacidad de obtención, procesado y almacenamiento. Funcionalmente facilitará la continua actualización de la información. Debe ser un elemento integrador que permita el trabajo colaborativo, implicando a todos los equipos como consumidores de inteligencia. A su vez, los usuarios se convertirán en generadores de inteligencia, al verter en el sistema el resultado de sus actividades de consumo. Con ello, la capacidad de explotación se convierte en la herramienta de gestión de conocimiento sobre amenazas y objetivos, que necesita el desarrollo de operaciones.

Para facilitar este trabajo, el sistema deberá permitir el mando y control de los recursos y tareas asignadas. Así se maximizará la eficacia potenciando el aprovechamiento de la información y realimentando el sistema para incrementar las capacidades propias y generar nuevas oportunidades de maniobra.

Para obtener resultados óptimos y acometer todas las misiones propias de la capacidad de explotación, los sistemas deben estar atendidos por el personal adecuado, tanto en número como en formación. La fuerza de trabajo debe dominar el entorno de información en el que opera, debe comprender cómo actúan las amenazas y la forma en la que pueden mitigarse, debe ser capaz de obtener, procesar y analizar información técnica y no

Ilustración 5. Competencias básicas de los analistas de explotación

técnica. Además, debe contar con las habilidades necesarias para comunicarse con equipos de especialistas en el ciberespacio y, a la vez, con personal que debe tomar decisiones de índole operativa. En definitiva, el personal debe contar con una alta especialización, alcanzable únicamente mediante la profesionalización desde el inicio de sus carreras y la dedicación en exclusiva al ámbito.

5. Actividades relacionadas con la capacidad de explotación

Como precursor necesario para el desarrollo de las operaciones, una actividad fundamental a desarrollar por la capacidad de explotación es la Preparación de Inteligencia del Entorno Operativo aplicada al ciberespacio, lo que por sus siglas en inglés se conoce como C-IPOE[2].

El C-IPOE deberá estar integrado con el planeamiento de las operaciones y requerirá de un detallado planeamiento propio, previo a su ejecución. Durante la misma se recopilarán los datos y la información necesaria que, junto con su análisis, proporcionarán al mando un verdadero entendimiento del «ciber-terreno» que afecta a las operaciones en curso. Este entendimiento se generará mediante la descripción de las capas y componentes que conforman el ciberespacio.

Para obtener una visión completa, en la capa social se incidirá en la conexión entre las identidades reales y las ciberidentidades para averiguar quiénes son los verdaderos actores en el ciberespacio. La descripción de las capas lógica y física ayudará a definir cómo emplean el ciberespacio los actores hostiles o neutrales y permitirá vincular, cuando sea posible, la ubicación geográfica de los sistemas.

El mapeo de toda esta información permite detallar las redes, sistemas, aplicaciones, usuarios o ciberidentidades de interés, teniendo en cuenta que esta actividad deberá ser realizada continuamente, ya que el ciberespacio está sometido a cambios constantes.

Esta información otorga al comandante una visión de conjunto del ciberespacio que le permitirá plantearse nuevas alternativas de maniobra u objetivos y entender cómo puede el ciberespacio afectar a sus actividades. Además, la interconexión de todas las capas con las identidades reales y las ubicaciones geográficas permitirá plantearse acciones en otros dominios, ya sean en apoyo a las operaciones en el ciberespacio o como actividades independientes.

Una de las características del C-IPOE es su espíritu multidisciplinar. Entender y aprovechar la información de todas las capas que constituyen el ciberespacio requiere la colaboración de múltiples disciplinas de inteligencia

[2] C-IPOE: Cyber Intelligence Preparation of the Operational Environment.

(inteligencia de señales, de fuentes abiertas, humana u otras), y necesita la participación de expertos en diferentes disciplinas del conocimiento, desde disciplinas técnicas a otras más humanistas del ámbito de la psicología o la sociología. Esta complejidad implica un trabajo detallado de investigación y un trabajo analítico que consumen tiempo y recursos.

La visión que proporciona el C-IPOE permite identificar las fuentes y plantear un verdadero plan de ISR que incluya la recolección de información de forma pasiva, activa, intrusiva o no intrusiva, en función de las fuentes de información, de las capacidades propias y de las ROE aplicables.

6. Capacidad de explotación y Operaciones Ofensivas en el Ciberespacio (OCO)

La ejecución de una OCO necesita de tres elementos; la definición y caracterización del objetivo, tener acceso al mismo y disponer de las herramientas que generen los efectos deseados.

Mediante el *targeting* en el ciberespacio, la capacidad de explotación apoya a las OCO ayudando a definir objetivos y encontrar relaciones entre los efectos deseados y las vulnerabilidades de las capacidades adversarias. Orientar sobre los vectores de ataque o acceso en forma de vulnerabilidades, en cualquiera de las capas del ciberespacio, es parte de los productos suministrados por esta capacidad. Para ello, se realizarán actividades de escaneo y monitorización continuas del estado de los sistemas, aplicaciones, organizaciones y sus operadores.

El *targeting* también contribuye al planeamiento y ejecución de una operación, identificando amenazas para la ejecución de la operación o caracterizando otros actores relevantes (fuerzas propias o agentes neutrales) que empleen el ciberespacio de interés. Con esta información desarrollarán planes de contingencia. El conocimiento de los adversarios contribuirá a caracterizar las TTP (tácticas, técnicas y procedimientos) y CoA (cursos de acción) empleados por el adversario. El conocimiento de las TTP permitirá desarrollar acciones de falsa bandera, imitando actividades adversarias para dificultar la atribución, mientras que el conocimiento de los CoA facilitará la ejecución de las acciones ofensivas propias, al predecir la posible respuesta adversaria ante un ataque.

Durante la conducción de operaciones, desde la capacidad de explotación, también se puede contribuir a valorar la rentabilidad de atacar a un objetivo determinado con medios cinéticos o medios ciberespaciales orientados a la destrucción del mismo. El análisis de los objetivos puede ayudar a determinar si es más valioso seguir explotando la información o inteligencia que se obtiene de ellos mediante acciones intrusivas o destruirlos, con la consiguiente pérdida de la fuente de información.

7. Capacidad de explotación y Operaciones Defensivas en el Ciberespacio (DCO)

En lo que respecta a las DCO, la capacidad de explotación contribuirá desarrollando indicadores y alertas en colaboración con todos los elementos que se dedican a monitorizar y defender las redes. Generar un sistema de inteligencia que permita modelar las amenazas, almacenar el conocimiento adquirido sobre ellas e incorporar toda la información de fuentes externas de forma ordenada y aprovechable por la propia organización es una tarea de alto valor para cualquier organismo, al rentabilizar recursos e incrementar la eficacia. Para contribuir oportunamente se deberá disponer de una plataforma de inteligencia que sirva de repositorio de información de amenazas. Esto permitirá que la inteligencia elaborada sea accionable por todos los actores, mediante el desarrollo de protocolos propios, la consolidación de lecciones aprendidas y la generación y consumo de inteligencia de amenazas.

El sistema de indicadores y alertas deberá extenderse también al exterior de las redes propias, para identificar potenciales amenazas que actúan sobre terceros, identificar brechas de información, campañas de ingeniería social, monitorizar la actividad de actores de interés y un sinfín de actividades que permitan monitorizar todo el ciberespacio de interés, basándose también en el C-IPOE para tener un completo conocimiento de la situación.

La atribución será otro ámbito en el que los analistas de inteligencia en el ciberespacio pueden contribuir aportando su conocimiento sobre las TTP de los actores y el análisis de las actividades realizadas por los adversarios en las redes propias. Esta actividad requiere de un elevado conocimiento técnico y experiencia y se basará en la colaboración estrecha con los equipos forenses e incluso equipos de simulación de amenazas. El trabajo de atribución contemplará la determinación de los motivos e intenciones de los atacantes, sus capacidades y oportunidades aprovechadas para identificar posibles patrones de actuación futuros y recursos potencialmente en riesgo que deben ser protegidos.

Con el adecuado nivel de experiencia y capacitación, los analistas podrían contribuir a desarrollar nuevas contramedidas contra nuevos tipos de ataques o nuevas vulnerabilidades todavía no descubiertas. Esta situación, que sería la ideal para un Mando del Ciberespacio, requiere que la actividad del cibercombatiente sea entendida como una trayectoria profesional completa, que requiere del desarrollo de capacidades muy específicas que deben ser adquiridas desde los primeros momentos de su andadura profesional.

ALCANCE	FUENTES	PRODUCTOS	CARACTERÍSTICAS DE LOS PRODUCTOS
OPERACIONAL	• ABIERTAS • PAGO • DARK WEB • ORGANISMOS PÚBLICOS	• VALORACIONES DE AMENAZAS, VULNERABILIDADES E IMPACTOS	• INFORMACIÓN A LARGO PLAZO • INFORMES EJECUTIVOS (QUIÉN, POR QUÉ, DÓNDE) • SUPERFICIE DE ATAQUE GEOGRÁFICA • APOYO A LA DECISIÓN OPERACIONAL • VALORACIÓN DE OBJETIVOS

TÁCTICO – PLANEAMIENTO	• ABIERTAS
	• PAGO
	• DARK WEB
	• ORGANISMOS PÚBLICOS
		• EVALUACIÓN DEL ENTORNO
		• EVALUACIÓN DE ADVERSARIOS
		  • TTP
		  • COA
			• INFORMACIÓN A CORTO PLAZO
			• INFORMES PARA DIRECCIÓN DE OPERACIONES (CUÁNDO, DÓNDE, CÓMO)
			• SUPERFICIE DE ATAQUE PERSONAS Y/O SISTEMAS

TÁCTICO - EJECUCIÓN	• LOGS ENDPOINTS
	• LOGS TRÁFICO RED
	• LOGS WEB
	• SIEM
	• SISTEMAS PERIMETRALES
	• FORENSES
	• PROVEEDORES CTI
		• COMPARTICIÓN DE INFORMACIÓN
		  • MISP
		  • PLATAFORMAS INTELIGENCIA DE CIBERAMENAZAS
			• INFORMACIÓN DE CONSUMO INMEDIATO
			• DIRIGIDA A LA RESPUESTA A INCIDENTES / DEFENSORES (CÓMO, QUÉ)
			• SUPERFICIE DE ATAQUE APLICACIONES Y SISTEMAS

Ilustración 6. Tareas y productos relacionados con la actividad de inteligencia de ciberamenazas

8. Capacidad de explotación y operaciones de información

Otro tipo de actividades que puede acometer la capacidad de explotación son aquellas que contribuyen a la ejecución de operaciones de información. La capacidad de explotación requiere del despliegue de sensores para recopilar información. En ocasiones, los sensores actuarán de forma pasiva o con bajo nivel de interactuación, pero, otras veces, se requerirá que el nivel de interactuación con la fuente sea elevado.

En apoyo a las operaciones de información, esta red de sensores puede ser empleada para reconocer los mensajes, las audiencias objetivo y caracterizar las redes de distribución, identificando, por ejemplo, campañas de influencia adversarias. En un plano ofensivo, la capacidad de explotación puede ser empleada como vector de ataque, contribuyendo con su red de sensores y capacidades a crear las condiciones para distribuir los mensajes propios creados por el ámbito cognitivo, interactuar con redes adversarias para identificar potenciales objetivos o contribuir a su disrupción.

9. Conclusión

La capacidad de explotación es un elemento novedoso en el ámbito de las operaciones en el ciberespacio. Su vocación de servicio al resto de

capacidades o ámbitos requiere del desarrollo de capacidades propias que tienen que ver principalmente con recopilación de información y su aprovechamiento para la identificación de oportunidades y la generación de la inteligencia necesaria para que esas oportunidades se transformen en actividades operativas reales.

Para ello, es fundamental que esta capacidad se desenvuelva ágilmente en el ciberespacio, pudiendo formar una red de sensores que permita ejercer vigilancia y reconocimiento del ciber-terreno. Esto debe basarse en unos sistemas adecuados para ejecutar estas tareas, pero también, incluso más importante, en un personal con capacidad para conocer el ciberespacio, sus posibilidades técnicas y operativas y el comportamiento de las amenazas que en él operan.

Traducir esta información para que se puedan tomar decisiones adecuadas es uno de los principales retos, como lo es el proporcionar la información en formatos y contextos correctos para su rápido consumo por el resto de unidades del ciberespacio o de otros ámbitos. Por ello, esta capacidad debe esforzarse para proporcionar al escalón superior la visión y perspectiva del ciberespacio lo más accionable posible. De esta forma, se podrá comprender más fácilmente que el ciberespacio es una nueva dimensión donde la cercanía física con el adversario no es relevante. La comprensión y aprovechamiento de este hecho diferencial del ámbito permitirá abrir un abanico de posibilidades operativas.

Normas de envío

A. Directrices para el envío de artículos

Los autores/as están obligados a comprobar que su envío cumpla todas las directrices que se muestran a continuación. Se devolverán a los autores/as aquellos artículos que no las cumplan.

- 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 la revista.
- Se confecciona en formato OpenOffice, Microsoft Word, RTF o WordPerfect.
- Se cumple con los requisitos estilísticos y bibliográficos resumidos en el apartado B.
- Se adecua a la política de detección de plagio que asegura la originalidad de los manuscritos.
- Cumple los criterios de las normas **UNE 50-104-94** e **ISO 690-2013**. La bibliografía –esto es, solo aquella a la que se haga referencia en el texto– se recoge al final del trabajo, ordenada alfabéticamente por apellido y nombre del autor según las normas citadas.
- Se registran todos los metadatos del artículo en el apartado correspondiente: título, resumen, autoría y colaboradores, palabras clave y citas/referencias.

B. Directrices para autores/as

1. Proceso de recepción y aprobación de originales

Todos los trabajos tendrán entrada en el buzón[1] del *Cuaderno de Inteligencia* no más tarde del mes de febrero de cada año, en caso de que se quiera publicar en ese mismo año.

Una vez comprobado el interés del tema y la adecuación a las normas de la publicación se comunicará al autor la aceptación de su trabajo para ser evaluado.

[1] ESFAS_CuadernoInteligencia@mde.es

Tras la comunicación de aceptación de las colaboraciones, el proceso de revisión de las mismas no excederá de ocho semanas. Durante este periodo, el Consejo de Redacción decidirá sobre la conveniencia de la publicación.

Asimismo, el Consejo de Redacción acusará recibo de los originales en un plazo de siete días hábiles desde su recepción e informará a los autores de la fecha en la que remitirá el dictamen motivado.

Una vez devuelto el artículo al autor, con las correcciones y sugerencias correspondientes, este dispondrá de veinte días hábiles para enviar la versión definitiva al Consejo de Redacción.

La aprobación del artículo por parte del Consejo de Redacción implica que la revisión por parte de los autores, previa a la publicación del trabajo, debe limitarse a la corrección de errores. No está permitido realizar modificaciones del contenido.

2. *Criterios para la selección de artículos*

Entre los artículos recibidos se seleccionarán aquellos que, cumpliendo las normas específicas para autores, destaquen por su originalidad, relevancia, interés y actualidad.

3. *Sistemas de evaluación*

Por su parte, el *Cuaderno de Inteligencia* asegura una política de detección de plagio, revisando, antes de su envío a la Subdirección General de Publicaciones, la originalidad de los manuscritos.

Una vez enviadas al autor las propuestas de modificación, se recomienda que la nueva versión del documento incorpore control de cambios.

4. *Instrucciones a los autores*

Las personas que envíen trabajos para publicar en la *Revista de Inteligencia* deberán verificar previamente que el texto enviado cumple las normas siguientes:

— Antes de enviar el artículo, el autor deberá verificar que el contenido del mismo se adapta a la temática y a la finalidad de la revista. Los artículos que no estén dentro de la temática propuesta podrán ser rechazados sin que se proceda a su evaluación.

Para cualquier duda sobre la realización de este proceso, pueden enviar un correo a la dirección: ESFAS_CuadernoInteligencia@mde.es

5. *Normas de publicación*

Los trabajos originales se enviarán en un único archivo Word y se adjuntará al envío, en formato PDF, el *curriculum vitae* de los autores, junto a un resumen de ese mismo curriculum que no excederá de 150 palabras.

El texto del artículo deberá tener una extensión entre 6.000 y 12.000 palabras.

Las notas al texto se presentarán siempre a pie de página y no deberán ocupar más de una cuarta parte del total de esta.

En el caso de los artículos, el texto incluirá un resumen del contenido que no debe superar las 200 palabras; se adjuntarán también cinco palabras clave del documento que no deben coincidir con el título. Ambos se presentarán en español y en inglés.

La estructura del texto será la siguiente:

— Título.

— Resumen.

— Palabras clave.

— Abstract.

— Key words.

— Capítulos, apartados y subapartados: toda la numeración referida a dichas partes, secciones y apartados, se numerará con números arábigos. Como norma general, se utilizarán los niveles inferiores hasta un tercer nivel para evitar las excesivas subdivisiones (ej. nivel 1: 1, nivel 2: 1.1, nivel 3: 1.1.1).

— Separaciones: los títulos de los apartados estarán separados del texto anterior por dos espacios interlineales, y del texto posterior por un espacio interlineal. Los títulos de los subapartados estarán separados, tanto del texto anterior como del posterior, por un espacio interlineal.

— El texto incluirá paginación en la parte inferior central con números arábigos.

— Para el envío de una reseña de libro, el autor deberá seguir las instrucciones anteriores y, además, aportar los siguientes datos al final del documento: título del libro, autores, año de publicación, páginas, editorial e ISBN. La imagen de la portada, en formato jpg, se adjuntará en otro documento. Ambos documentos se mandarán en el mismo envío.

6. Normas tipográficas

Las normas de estilo de la Revista de Inteligencia se ajustan a lo estipulado por la Subdirección General de Publicaciones y Patrimonio Cultural del Ministerio de Defensa (2022).

Los autores deberán seguir las normas ortográficas de la Real Academia Española, en su edición de 2010.

7. Consideraciones generales

El texto se remitirá «plano», sin saltos de página, de sección o similar.

Márgenes de texto: 3 cm a cada lado.

El documento se remitirá en formato Word.

No se emplearán en ningún caso las «negrillas».

Citas literales: menos de 4 líneas dentro del párrafo; más de 4 líneas en párrafo aparte, con sangría y con un espacio superior e inferior en blanco.

Se emplearán comillas latinas « (Alt+174), » (Alt+175); comillas inglesas solo para entrecomillar: «Antonio me dijo: "Vaya 'cacharro' que se ha comprado Julián"».

Fuente

Título obra:	Arial 14
Cuerpo del texto:	Arial 12
Pie de imágenes y notas al pie:	Arial 9
Citas textuales:	Arial 11

Capítulo y apartados

Primer nivel:	1.
Segundo nivel:	1.1.
Tercer nivel:	1.1.1.

- No se sobrepasará el tercer nivel de epígrafes.
- No se empleará la herramienta de Word para numerar, se escribirán los números del apartado como parte del epígrafe.

Referencias y notas al pie

Libros y artículos de revistas científicas (indexadas) según Modelo Harvard, en el propio texto (Apellido minúsculas, año: página/s). Ejemplos:

— (Casado, 2011), (Casado, 2011: 213), (Casado, 2011: 213-214).

— Según Casado (2011); Para Casado (2011: 213-214).

— (Casado, 2011a: 213), (Casado, 2011b: 22).

— (Kay y Tisdall, 1994), (Kay y Tisdall, 1994: 36).

— Si son 3 o más autores (Casado et al., 1994).

Resto de documentos y notas aclaratorias al pie de página

El superíndice que marca el número (siempre latino) de la nota al pie debe situarse ANTES del signo de puntuación que pudiera haber. Ejemplo:

Texto[1]. Correcto.

Texto[1]. Incorrecto.

Ejemplos de notas al pie:

Musilli, P. y Smith, P. (junio 2013). The lawless roads: and overview of turbulence across the Sahel. *Norwegian Peacebuilding Resource Center Report*. Disponible en: https://www.files.ethz.ch/isn/165438/e2cc78a2ce-149944b9a35b4ce42759b9.pdf

Global Terrorism Index 2022. Institute for Economics and Peace, pp. 2-10. Disponible en: https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web.pdf

Mueren cinco soldados chadianos en un ataque achacado a Boko Haram en la cuenca del lago Chad. *Europa Press* (23 de febrero de 2022). Disponible en: https://www.europapress.es/internacional/noticia-mueren-cinco-soldados-chadianos-ataque-achacado-boko-haram-cuenca-lago-chad-20220223145642.html

Se debe poner la fecha de consulta de las páginas web o una nota en la primera nota al pie que diga: «Todos los enlaces se encuentran activos a fecha de cierre del presente documento, xx de xxxxxx de xxxx»).

Bibliografía

Incluirá exclusivamente los libros y artículos de revistas científicas (indexadas) que hayan sido citadas en el texto (recordando que lo han sido en sistema Harvard).

Por orden alfabético.

De antiguo (documento publicado hace más años) a moderno (más reciente).

Caso de igualdad de autor y fecha en varias publicaciones, se ordenan alfabéticamente y se incluye una letra en el año de publicación –por orden

alfabético– para marcar el orden de antiguo a moderno. Ejemplo (2017a) (2017b).

Ejemplos:

Alda, E. y Sala, J. L. (2014). Links between terrorism, organized crime and crime: the case of the Sahel region. *Stability: International Journal of Security & Development*. 3(1), pp. 1-9. Disponible en https://www.stability-journal.org/articles/10.5334/sta.ea/

Echeverría Jesús, C. (2019). El Sahel. Tráfico y Terrorismo. En: *El Sahel y G5: desafíos y oportunidades*. Madrid, Ministerio de Defensa, Secretaría General Técnica. Pp. 67-102. Cuadernos de Estrategia, 202. Disponible en: https://www.ieee.es/Galerias/fichero/cuadernos/CE_202_El_sahel_y_g5_desafios_y_oportunidades.pdf

MADOC Mando de Adiestramiento y Doctrina. (2008). Contrainsurgencia. *Publicación Doctrinal PD3-301*.

MADOC Mando de Adiestramiento y Doctrina. (2013). Operaciones de estabilización. *Publicación Doctrinal PD2-001* (vol. 3).

Mesa, B. (2022). Les groupes armés du Sahel. Conflits et économie criminelle au nord du Mali. Perpignan, Halfa Books.

Imágenes

Las imágenes que no reúnan los requisitos señalados serán directamente eliminadas.

Deberán incluir al pie el título de la misma y la fuente, e ir numeradas de manera correlativa. Ejemplo:

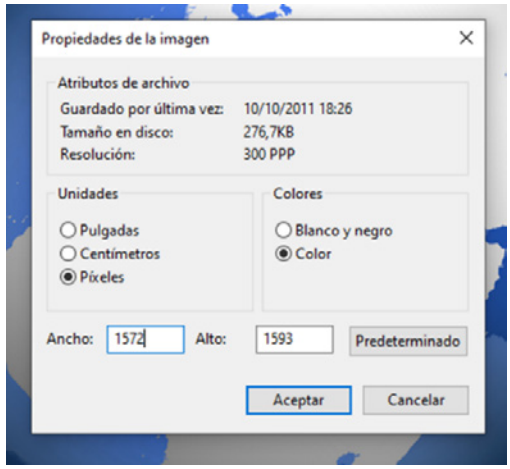
Imagen 1: El Sahel. *Fuente:* https://www.ieee.es/Galerias/fichero/cuadernos/CE_202_El_sahel_y_g5_desafios_y_oportunidades.pdf

Formato: TIFF o JPG.

Resolución: 300 píxeles por pulgada.

Deberán remitirse en archivo aparte (dejando clara su ubicación dentro del documento).

Comprobación abriendo la imagen: Paint > Archivo > Propiedades.



7. Repositorio y base de datos

El *Cuaderno de Inteligencia* está incluido en la página de la Subdirección General de Publicaciones y en el repositorio Dialnet.

Cómo citar esta publicación

Cuaderno de Inteligencia. Escuela Superior de las Fuerzas Armadas, Centro Superior de Estudios de la Defensa Nacional. Madrid: Ministerio de Defensa.

8. Aviso de derechos de autor/a

El autor deberá cumplimentar el documento de cesión de derechos que acompaña a las presentes normas, como Apéndice 1.

Se permite y anima a los autores a difundir sus trabajos electrónicamente (por ejemplo, en repositorios institucionales o en su propio sitio web), después de la publicación del *Cuaderno*, para favorecer intercambios productivos.

Apéndice 1

DOCUMENTO CESIÓN DE DERECHOS EXPLOTACIÓN

Autor:

NIF:

Dirección postal:

Teléfono:

Email:

Título del documento:

Por el presente documento cede, en favor del Ministerio de Defensa, los derechos de explotación de la propiedad intelectual y, en especial, los derechos de reproducción, distribución y transformación en cualquiera de sus modalidades y de comunicación pública del citado documento.

El autor se responsabiliza de la obtención de todas las autorizaciones y licencias de los elementos incluidos en el trabajo (imágenes, gráficos, etc.), que se encuentren amparados por la propiedad intelectual.

La cesión se otorgará para cualquier medio o soporte gráfico, fonográfico, audiovisual, telemático, electrónico, digital, multimedia o informático y para un ámbito territorial mundial, y tendrá una duración equivalente a todo el tiempo de protección que conceden a los autores, sus sucesores y derechohabientes las actuales leyes y convenciones internacionales propias de la materia de propiedad intelectual.

El autor renuncia a percibir de la Subdirección General de Publicaciones y Patrimonio Cultural cantidad alguna por la cesión de los derechos de explotación del citado trabajo.

Fecha y firma del autor

En _____, a _____de _____de 202___

Composición del grupo trabajo

Presidente	**D. Juan Ramón Sabaté Aragonés** *General de brigada del Ejército de Tierra* *Jefe de Estudios de la ESFAS–CESEDEN*
Vocal y coordinador	**D. Ángel Segundo Gómez González** *Coronel del Ejército de Tierra* *Departamento de Inteligencia ESFAS-CESEDEN*
Vocales	**D. Miguel Sánchez de Toca Alameda** *Coronel del Ejército de Tierra* *Sección de Inteligencia y Seguridad (SINTSEG)*
	D. Jorge Díaz Muriana *Teniente coronel del Ejército de Tierra* *Sección de Inteligencia y Seguridad (SINTSEG)*
	D. Raul Martín Martín *Teniente coronel del Ejército de Tierra* *Sección de Inteligencia y Seguridad (SINTSEG)*
	D. Antonio Muñoz Galdeano *Comandante del Ejército de Tierra* *Centro de Situación del ET (CESET)*
	D. Julio Albaladejo López *Capitán de navío y jefe de Inteligencia de la Flota*
	D. Sergio Flores Friaza *Teniente coronel del Ejército del Aire y del Espacio.* *EMA/DOP/SINTE*
	D. José Lorenzo-Penalva Lucas *Teniente coronel de Infantería de Marina* *CIFAS*
	Dña. María del Carmen Ariñez Fernández *Coronel del Cuerpo Militar de Sanidad* *Instituto de Medicina Preventiva de la Defensa*

D. Álvaro Álvarez Álvarez
Teniente coronel del Ejército del Aire y del Espacio
Inteligencia Actual, J2 MOPS

D. Francisco Javier López Cuevas
Capitán del Ejército de Tierra
Collection Management, J2 MOPS

D. Pablo Caneda González
Collection Management, J2 MOPS

D. Jesús Antonio Vicente Montaña
Comandante de la Guardia Civil

D. Juan Soriano Paradinas
Teniente coronel del Ejercito del Aire y del Espacio
J-2 Inteligencia, Cuartel General de la UME

PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL