

Capítulo primero

Operaciones Electromagnéticas (EMO) e Information Warfare (IW). Posibilidades de armonización de ambos conceptos

Marcos de Sousa Fuchs

Sumario

En la actualidad, existe un vínculo indisoluble entre información y espectro electromagnético. En este sentido, el acceso ininterrumpido al espectro es un requisito irrenunciable para poder alcanzar la superioridad en la información. Y, este aspecto, será cada vez más demandante y complejo, con el dato erigido como activo central en la revolución de la información. Con este hilo conductor, y desde una perspectiva sistémica, el presente artículo investiga la complementariedad y sinergia de los conceptos de Operaciones Electromagnéticas (EMO) e *Information Warfare* (IW) en el nivel operacional de las Fuerzas Armadas españolas.

En primer lugar, se profundiza en la definición y el desarrollo de ambos conceptos, revisando sus fundamentos y evolución, así como la importancia de las tecnologías emergentes y disruptivas (EDT) y su incidencia en las operaciones multidominio. A continuación, se analizan las anomalías en los procesos y se buscan los aspectos de conflicto entre EMO e IW, ya que estas contradicciones son las que disminuyen la sincronización desde un enfoque sistémico. Finalmente, se evalúan diferentes órganos multifuncionales del Mando de Operaciones (MOPS) como herramientas de coordi-

nación e integración entre EMO e IW. Porque si el empleo de estos mecanismos aporta sinergias y permite eliminar las contradicciones identificadas, la contribución de EMO e IW a la superioridad de la fuerza conjunta (FC) se incrementará significativamente.

Palabras clave

Información, espectro electromagnético (EMS), tecnologías emergentes y disruptivas (EDT), efectos, procesos.

Electromagnetic Operations (EMO) and Information Warfare (IW). Possibilities of harmonization of both concepts

Abstract

Currently, there is an inseparable link between electromagnetic spectrum and information. Therefore, unimpeded access to the spectrum is an essential requirement to achieve information superiority. This aspect will become increasingly complex and demanding, with data established as the backbone in the information revolution. Applying a systemic approach, the present paper investigates the complementarity and synergy of the Electromagnetic Operations (EMO) and Information Warfare (IW) concepts at the operational level of the Spanish Armed Forces.

Firstly, both concepts are defined and developed, reviewing their foundations and evolution, as well as the importance of emerging and disruptive technologies (EDT) and their impact on multidomain operations. Then, the anomalies in the processes are analyzed, as well as the conflicting aspects between EMO and IW. In this regard, these contradictions are what decrease synchronization from a systemic approach. Finally, different multifunctional bodies of the Joint Operations Command (MOPS) are evaluated as tools for coordination and integration between EMO and IW. If they provide synergy and eliminate the identified contradictions, the contribution of EMO and IW to the superiority of the joint force will increase significantly.

Key words

Information, electromagnetic spectrum (EMS), emergent and disruptive technologies (EDT), effects, processes.

Lista de abreviaturas

AI	Artificial Intelligence
AJP	Allied Joint Publication
AOPE	Área de Operaciones
ATP	Allied Tactical Publication
BBDD	Bases de Datos
CCDC	Centro Conjunto de Desarrollo de Conceptos
CIMIC	Civil-Military Cooperation
CIS	Communication and Information Systems
CMI	Civil-Military Interaction
CO	Cyberspace Operations
COEM	Centro de Operaciones Electromagnéticas
COMINT	Communications Intelligence
COVE	Centro de Operaciones de Vigilancia Espacial
CTL	Collection Task List
CSG	Carrier Strike Group
C2	Command and Control
C2D2E	Command and Control in a Degraded or Denied Environment
DCO	Defensive Cyberspace Operations
EDT	Emergent Disruptive Technologies
EI	Entorno de la Información
ELINT	Electronic Intelligence
EME	Electromagnetic Environment
EMI	Electromagnetic Interference
EMO	Electromagnetic Operations
EMOWG	Electromagnetic Operations Working Group
EMS	Electromagnetic Spectrum
EA	Electronic Attack
ED	Electronic Defence

EMMOPS	Estado Mayor del Mando de Operaciones
EOEM	Elementos de Operaciones Electromagnéticas
ES	Electronic Surveillance
ESN	Estrategia de Seguridad Nacional
EW	Electronic Warfare
FAS	Fuerzas Armadas
FC	Fuerza Conjunta
FP	Force Protection
FVEY	Five Eyes Community
GNSS	Global Navigation Satellite System
IA	Information Activities
IACB	Information Activities Coordination Board
IAWG	Information Activities Working Group
IEA	Information Environment Assessment
IM	Information Management
INFOOPS	Information Operations
IoT	Internet of the Things
IPOE	Intelligence Preparation of the Operational Environment
IRC	Information Related Capability
ISR	Intelligence Surveillance and Reconnaissance
IW	Information Warfare
IWC	Information Warfare Commander
JCMB	Joint Coordination Management Board
JCWG	Joint Coordination Working Group
Jemad	Jefe de Estado Mayor de la Defensa
JIC	Joint Intelligence Centre
JISR	Joint Intelligence Surveillance and Reconnaissance
JOC	Joint Operations Centre
JTC	Joint Targeting Centre

JTCB	Joint Targeting Coordination Board
JTGT	Joint Targeting
JTWG	Joint Targeting Working Group
LEO	Low Earth Orbit
MCA	Mando Componente Aéreo
MCC	Mando Componente Ciberespacial
MCOE	Mando Componente Operaciones Especiales
MCM	Mando Componente Marítimo
MCT	Mando Componente Terrestre
MDO	Multidomain Operations
METOC	Meteorología y Oceanografía
MilPA	Military Public Affaires
Minisdef	Ministerio de Defensa
MIRADO-I	Material, Infraestructuras, Recursos humanos, Adiestramiento, Doctrina e Interoperabilidad
ML	Machine Learning
MOPS	Mando de Operaciones
NAI	Núcleo de Análisis de Influencia
NAVWAR	Navigation Warfare
OBE	Orden de Batalla Electrónico
OCO	Offensive Cyberspace Operations
OP	Objetivo Principal
OPSEC	Operations Security
OTC	Officer in Tactical Command
OS	Objetivo Secundario
PDC	Publicación de Doctrina Conjunta
PNT	Positioning, Navigation and Timing
PPP	Posture, Presence and Profile
PSYOPS	Psychological Operations
PTP	Plan de Trabajo de Prospectiva

RCIED	Radio Controlled Improvised Explosive Device
RPA	Remotely Piloted Aircraft
RRSS	Redes Sociales
SATCOM	Satellite Communications
SEW	Shared Early Warning
SIGINT	Signals Intelligence
SM	Spectrum Management
SpSC	Space Support Coordination
SSA	Space Situational Awareness
STRATCOM	Strategic Communication
STS	Sensor To Shooter
TDL	Tactical Data Link
TIC	Tecnologías de la Información y las Comunicaciones
UIT	Unión Internacional de Telecomunicaciones
UAS	Unmanned Aerial System
USN	United States Navy
USV	Unmanned Surface Vehicle

1. Introducción

En el actual contexto de las operaciones militares, alcanzar la superioridad en la información y asegurar un acceso ininterrumpido al espectro electromagnético constituyen dos requisitos esenciales para la fuerza conjunta. Ambos tienen un elemento en común, el cual es, además, la característica principal de la cuarta revolución industrial, según Oliver (2024): la ubicuidad de la tecnología digital.

En primer lugar, la superioridad en la información es un estado de ventaja relativa sobre el adversario que se obtiene mediante el empleo de información relevante y de capacidades relacionadas con la información (Minisdef, 2017). No solo implica obtener y procesar datos más rápidamente que el adversario, sino también proteger y explotar esta información para lograr ventajas decisivas. Con este objetivo nació la disciplina *Information Warfare* (IW) en el seno de la Marina de EE. UU., que se extendió posteriormente a sus socios de la comunidad *five eyes*¹, y, finalmente, fue incorporada en 2021 a la doctrina marítima de la OTAN. España ha ratificado e implementado sin reservas esta disciplina para su fuerza conjunta.

Paralelamente, el espectro electromagnético se ha convertido en el medio esencial a través del cual se transmite esta información crítica, siendo el soporte de comunicaciones, navegación y sistemas de armas. Un acceso ininterrumpido al espectro no solo permite comunicarse eficazmente y sincronizar acciones en el campo de batalla, sino que también ofrece nuevas oportunidades para degradar las capacidades operativas del adversario. Con el propósito de conformar y vigilar el entorno electromagnético y de garantizar la superioridad en el mismo, las operaciones electromagnéticas (EMO) terminaron viendo la luz en la OTAN en 2020. Aunque la transformación aliada de la *electronic warfare* (EW) se remonta a los primeros años del siglo XXI, fue el despliegue electrónico ruso durante la ocupación de Crimea en 2014 y la posterior guerra en Siria lo que aceleró dicha evolución (Nieto, 2021). Por su parte, España también ha ratificado e implementado las EMO sin reservas para su fuerza conjunta.

En definitiva, los conceptos EMO e IW proporcionan a las FAS herramientas operativas para poder combatir en el espectro elec-

¹ Es una alianza de inteligencia en la que participan EE. UU., Canadá, Reino Unido, Australia y Nueva Zelanda. Tuvo su origen formal al inicio de la Guerra Fría.

tromagnético y en el entorno de la información. De su empleo adecuado dependerá la superioridad de la fuerza conjunta en el espacio de las operaciones.

Aunque existen múltiples investigaciones y publicaciones sobre los conceptos EMO e IW, hasta la fecha no se ha realizado ningún estudio sobre los aspectos de conflicto entre ambos conceptos y sus herramientas de coordinación a nivel operacional². Por este motivo, se ha considerado relevante investigar sobre la complementariedad y sinergia de estos dos conceptos en el nivel operacional en las FAS españolas.

Para ello, se ha elegido como marco teórico la teoría de sistemas, actualizada e integrada con la teoría de las restricciones de Goldratt, a través de la obra de Birrell (2023). Por una parte, la teoría de sistemas ofrece un marco integral para analizar las organizaciones y fenómenos complejos, enfatizando la interdependencia y las interacciones entre sus componentes. Por otra, la teoría de las restricciones se centra en identificar y optimizar el eslabón más débil en cualquier cadena de procesos para mejorar el rendimiento general. Asimismo, cabe destacar que la aproximación sistémica es fundamental en las operaciones militares actuales y está presente en toda la doctrina militar.

Por último, el propósito de este artículo es divulgar de manera extractada y comprensible las principales conclusiones alcanzadas en la investigación académica relativa a la armonización de los conceptos EMO e IW, cuya fecha de cierre fue en mayo de 2024. Por este motivo, en el artículo no se encontrarán detalles profundos ni extensos sobre la aplicación del marco teórico, sobre las técnicas de investigación aplicadas, ni la bibliografía completa.

2. Conceptos EMO e IW en las operaciones militares

2.1. Concepto EMO en las operaciones militares

Las operaciones electromagnéticas (EMO) son definidas, en su Concepto Básico (2021) aprobado por el JEMAD, como el «conjunto de acciones militares dirigidas a conformar y vigilar el

² «El nivel operacional es en el que, basándose en las directrices del nivel estratégico militar, se planean, conducen y sostienen las campañas y las operaciones militares, para alcanzar los objetivos operacionales, que contribuyen a conseguir los estratégicos, dentro de una zona de operaciones». [PDC-01(A), 2018, p. 123].

entorno electromagnético (EME) y garantizar la superioridad en el mismo mediante el empleo de la energía electromagnética con fines ofensivos y defensivos». Con las EMO, se ha producido un salto conceptual relevante, pasando de realizar actividades aisladas de EW a desarrollar un amplio abanico de operaciones sincronizadas en el EME (NATO, 2020).

Como detalla Nieto (2021a), la transformación aliada de la EW comenzó a vislumbrarse a principios de los años 2000. Pero el protagonismo de la amenaza asimétrica durante estas décadas, que no confrontaba el acceso al espectro electromagnético, provocó, finalmente, la hibernación de las capacidades EW en el seno de la OTAN. En cambio, Rusia comenzó a modernizar sus Fuerzas Armadas con la guerra de Chechenia y desplegaron todo su potencial EW a partir de la ocupación de Crimea y de la guerra en Siria. La OTAN fue reaccionando con el paso del tiempo, a través de diferentes iniciativas, y acabó publicando su «Estrategia del espectro electromagnético» en 2019. Y un año después, las EMO se introdujeron formal y doctrinalmente en la OTAN a través del *AJP-3.6 (Ed.C V1)*, el cual pasó a utilizarse como vector de implementación en España (Ministerio de Defensa, 2021a).

En este sentido, el propósito de las EMO es asegurar que la FC opere de forma más efectiva en el EME, a la vez que se reduce o impide la capacidad del adversario en el mismo. El espectro está cada vez más saturado, disputado, y en ocasiones, degradado por adversarios. Por ello, el acceso y control del espectro es fundamental para la libertad de acción de la FC y alcanzar la superioridad en el enfrentamiento. Asimismo, todas las capacidades operativas, en mayor o menor medida, necesitan tener acceso al espectro (Ministerio de Defensa, 2021a). En palabras de Nieto (2022: 1): «ninguna operación militar se puede conducir o planear con éxito sin el concurso favorable del espectro».

«La ambigüedad de las operaciones electromagnéticas, su complejidad en determinar la atribución de una acción ofensiva, así como la capacidad de alcanzar efectos estratégicos sin el uso de la fuerza, hallan perfecto acomodo en las estrategias híbridas o en los conflictos que se desarrollan en la zona gris» (Nieto, 2021a: 22). Con esta afirmación, el autor también destaca la importancia de las EMO desde la perspectiva de los adversarios, rivales y potencias revisionistas (Nieto, 2021b).

El enfoque coordinado constituye el pilar fundamental sobre el que se asienta el concepto EMO. Debido al carácter transversal

del EME, a la dependencia cada vez mayor de la tecnología, y al predominio civil de la gestión del espectro, la coordinación horizontal y vertical es la principal herramienta para garantizar el acceso y las operaciones de la FC en el espectro (Ministerio de Defensa, 2021a).

En consecuencia, el «Concepto básico EMO» (2021a) establece una serie de actividades principales que concentran los recursos EMO de planeamiento, integración y sincronización. Entre ellas, se encuentran *electronic warfare* (EW), *signals intelligence* (SIGINT), *navigation warfare* (NAVWAR) y gestión del espectro (SM).

EW es la disciplina de combate de las EMO (Ministerio de Defensa, 2021a) y engloba las acciones militares que explotan energía electromagnética para contribuir al conocimiento del entorno y generar efectos ofensivos y defensivos (NATO, 2024). En otras palabras, las acciones EW³ permiten conformar el EME, incrementar el conocimiento del entorno y obtener inteligencia, defender a las fuerzas propias y atacar al adversario. En primer lugar, para la vigilancia electrónica se emplean sensores EW que monitorizan el espectro, tanto de forma pasiva como activa. En segundo lugar, la defensa electrónica abarca todos los cometidos relacionados con protección, perturbaciones, engaños e interferencias. Por último, el ataque electrónico se integra en el concepto de fuegos y está sujeto al ciclo de *targeting* (NATO, 2020).

Por su parte, SIGINT es la inteligencia que se obtiene a través de señales electromagnéticas o emisiones. Se trata de un término genérico que abarca tanto la inteligencia electrónica o *electronic intelligence* (ELINT) como la inteligencia de comunicaciones o *communication intelligence* (COMINT). Aunque las actividades SIGINT y EW compartan plataformas y sensores para su ejecución, tienen un propósito diferente y, por eso, se tratan de manera separada. La vigilancia electrónica (ES) está orientada al reconocimiento e identificación de amenazas, para proporcionar opciones tácticas de respuesta inmediata (NATO, 2020). En cambio, SIGINT es una disciplina de obtención que contribuye al ciclo de inteligencia a través de JISR (Ministerio de Defensa, 2020b). Por ello, SIGINT sigue un proceso de obtención dirigida y de elaboración de información, con el propósito de contribuir a identificar amenazas existentes y apoyar la toma de decisiones (Ministerio de Defensa, 2021e).

³ *Electronic surveillance* (ES), *electronic defence* (ED), y *electronic attack* (EA).

La saturación del EME y la dependencia del espectro es una realidad en las operaciones actuales, y para hacer frente a este desafío, nacieron los procedimientos de *spectrum management* (SM). SM se define como la coordinación práctica, asignación de empleo, gestión de conflictos y resolución de interferencias (EMI) en el entorno electromagnético. Esta disciplina afecta al empleo militar y no-militar del espectro y, por tanto, es especialmente sensible a los efectos que se puedan generar sobre el empleo comercial y legítimo de este (NATO, 2020). Según el «Concepto básico EMO» (2021a), SM «no solo se circunscribe a la gestión de las frecuencias, sino que también incluye el análisis del EME y el asesoramiento sobre el empleo de medios y la ejecución de actividades en el mismo» (Ministerio de Defensa, 2021a: 18).

Por último, NAVWAR consiste en la ejecución de acciones militares o medidas técnicas para garantizar la superioridad en la información de posicionamiento, navegación y sincronización de tiempo (PNT) (NATO, 2024). Esta disciplina se estructura en torno a tres pilares: ofensivo, defensivo y apoyo. Mediante el NAVWAR ofensivo se intenta interrumpir el acceso a la información PNT por parte del adversario. En contraposición, el objetivo del NAVWAR defensivo es mantener y proteger el acceso a la información PNT, tanto de unidades propias como de agencias civiles. Y, en última instancia, el NAVWAR de apoyo trata de mitigar o eliminar todas las amenazas que pongan en riesgo la información PNT (NATO, 2021).

Por otra parte, el «Concepto básico EMO» (2021a) detalla otras disciplinas que, debido a su dependencia del espectro, deben ser coordinadas mediante el planeamiento y ejecución de las EMO. En primer término, se menciona expresamente a las operaciones en el ciberespacio, porque, como se ha expresado previamente, este ámbito está íntimamente ligado al espectro electromagnético. En segundo lugar, se señala al espacio ultraterrestre porque el espectro electromagnético es el nexo que une el segmento espacial y los segmentos control y usuario. En tercer lugar, se detalla la necesidad de coordinar en materia de *force protection* (FP), porque muchas medidas activas o pasivas de protección contra amenazas asimétricas⁴ dependen del espectro de manera

⁴ Las amenazas asimétricas son aquellas que emplean medios o métodos no convencionales para soslayar las fortalezas del adversario y atacar directamente sus debilidades, con el propósito de obtener resultados desproporcionados en comparación con los medios empleados (NATO, 2024).

crítica. Por último, el concepto también menciona la posibilidad de tener que coordinar en materia de ISR o de actividades de información (Ministerio de Defensa, 2021a). Todas estas actividades no pertenecen al núcleo de las operaciones electromagnéticas, pero resulta fundamental aplicar mecanismos de coordinación con ellas.

En última instancia, conviene destacar que el «Concepto básico EMO» (2021a) está enfocado a dar una respuesta mediante la aplicación de una estructura adecuada de mando y control (C2). Aunque en el concepto se estudian los habituales factores MIRADO-I⁵, el foco de la solución se pone en los elementos organizativos. Por ello, este concepto ha sido la base sobre la que se ha desarrollado en las FAS españolas el Centro de Operaciones Electromagnéticas (COEM), la estructura EMO por mandos componentes y los procesos operacionales derivados. Todos ellos se estudian en detalle en el epígrafe 4 del presente artículo.

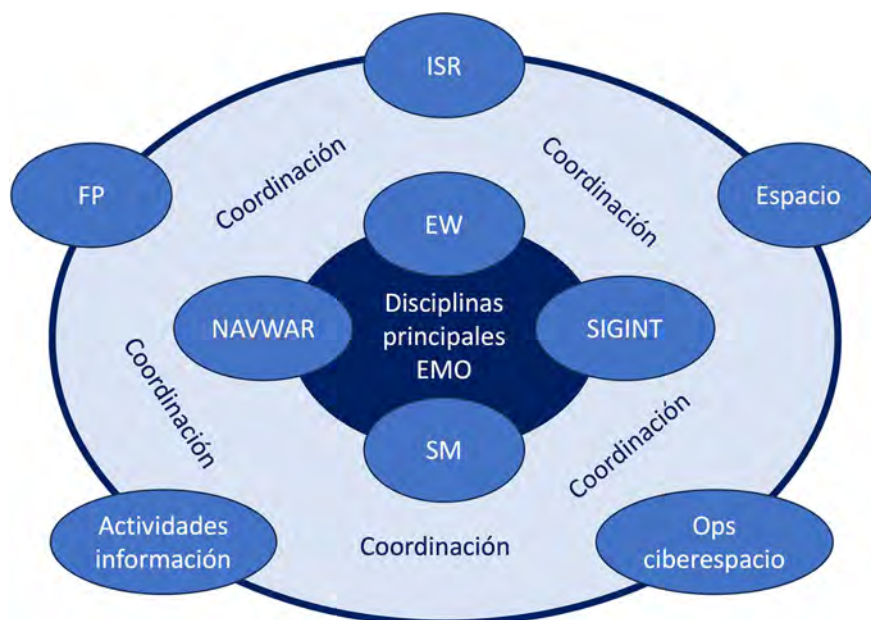


Figura 1. Disciplinas principales EMO (anillo interior) y otras actividades con las que es necesario coordinar (anillo exterior). Fuente: elaboración propia

⁵ Material, infraestructura, recursos humanos, adiestramiento, doctrina, organización e interoperabilidad. En las FAS, las capacidades militares se definen en base a estos siete elementos.

2.2. Concepto IW en las operaciones militares

Como detalla Ros (2024), la publicación aliada ATP-113 define *Information Warfare* (IW) como «el suministro, empleo seguro y protección de la información, de los procesos, sistemas y redes, y de su denegación y disrupción al adversario para lograr una ventaja operacional en el campo de batalla [...]»⁶. Para Conner (2023), IW engloba el conjunto de acciones militares llevadas a cabo para alcanzar la ventaja en la información sobre el adversario. Según Theohary (2018), IW consiste en proteger y explotar el entorno de la información (EI) mediante una combinación de esfuerzos ofensivos para influir y generar efectos deseados y de esfuerzos defensivos para asegurar la información. En cualquier caso, las actividades de IW se llevan a cabo en todo el continuo de la competición, desde la cooperación hasta el conflicto armado.

El desarrollo de esta disciplina se inició en noviembre de 2009, en el seno de la marina de Estados Unidos (USN). En ese momento, se decidió unir las ramas de inteligencia, comunicaciones, meteorología/oceanografía e información, y formar el cuerpo de *information dominance*. Ocho años más tarde, esta comunidad pasó a denominarse *information warfare* (IW). Desde ese momento, la USN ha desarrollado en profundidad el concepto IW y lo ha probado en combate. En paralelo, lo extendió a sus socios de la comunidad *five eyes* (FVEY), y, finalmente, fue incorporado en 2021 a la doctrina marítima de la OTAN a través del ATP-113. Se debe reseñar que IW es un concepto exclusivamente táctico y que todavía no ha dado el salto al nivel operacional⁷. Asimismo, cabe destacar que IW está ya incorporado en el cuerpo doctrinal nacional para el entorno marítimo, a través de la PDC-3.1 (2022b).

En este sentido, IW es la disciplina táctica que evalúa y conforma el EI, que permite alcanzar y mantener la superioridad en la información, y que desarrolla y ejecuta planes operativos relacionados con la información para alcanzar los objetivos del comandante. Para ello, el concepto IW se apoya en tres pilares

⁶ Cabe destacar que, en la OTAN, el término se circunscribe, actualmente, al entorno marítimo (*Maritime Information Warfare*). Para simplificar las explicaciones a lo largo del proceso de investigación, todas las referencias se realizarán al término *Information Warfare* (IW).

⁷ Ese proceso se encuentra actualmente en curso. Según Ros (2024), el último *ratification draft* del AJP-3.1 («Allied Joint Doctrine for Maritime Operations») ya incluye todo lo relativo a IW en el nivel operacional.

doctrinales: conocimiento del espacio de las operaciones, mando y control asegurado, e integración conjunta (Conner, 2023). A continuación, se va a describir cada uno de ellos.

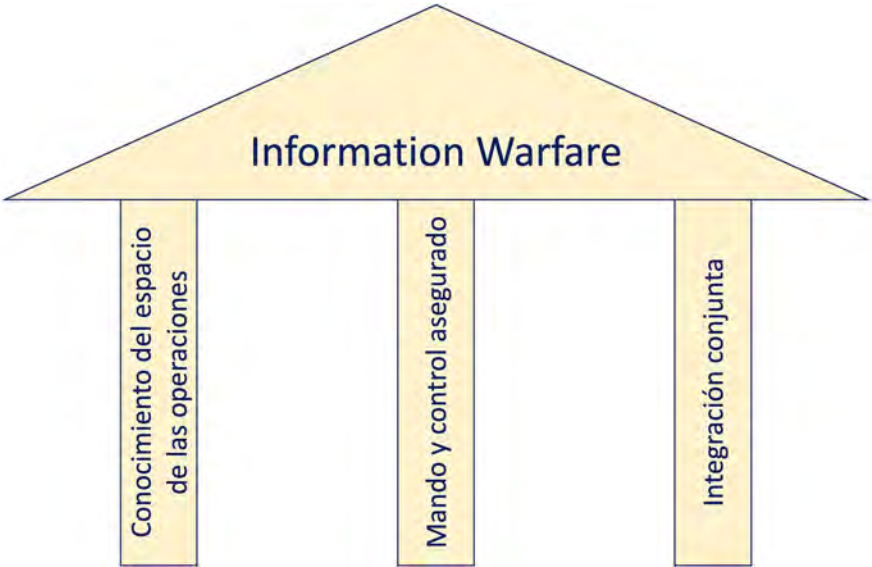


Figura 2. Pilares doctrinales de IW. Fuente: elaboración propia

El primer pilar, que consiste en proporcionar un conocimiento efectivo del espacio de las operaciones, aumenta la ventaja del comandante en la toma de decisiones (Aeschbach, 2022). Para ello, es necesario emplear con eficacia y de manera sinérgica los sensores y las capacidades de obtención, aunque cada vez sea más complicado gestionar un número de fuentes que crece exponencialmente. Este pilar incluye aspectos relacionados con el empleo efectivo de sensores y capacidades de obtención de información, vigilancia electrónica, vigilancia desde el espacio, inteligencia, meteorología, oceanografía, entorno físico y electromagnético, etc. (Conner, 2023). Asimismo, Braswell considera que el apoyo de la inteligencia al comandante es mayor cuando esta se integra con otras capacidades IW (2017).

El segundo pilar consiste en asegurar el mando y control (C2), con el propósito de garantizar que las operaciones puedan llevarse a cabo conforme a las directrices del comandante. Y como argumentan White *et al.* (2019), el espacio, el ciberespacio y el espectro electromagnético deben ser protegidos frente a los intentos de disrupción de los adversarios. Para ello, este pilar abarca aspectos vinculados con las comunicaciones, las operacio-

nes defensivas en el ciberespacio (DCO), la gestión de la información (IM), la gestión del espectro electromagnético y las redes de datos y comunicaciones (Conner, 2023). Para garantizar el mando y control, Braswell (2017) también incide en la importancia de la integración de los sistemas espaciales, en el impacto de la maniobra de la fuerza y en la preparación para escenarios de C2 degradado o denegado (C2D2E). Asimismo, uno de los grandes retos es el crecimiento exponencial de la cantidad de información que se maneja y la complejidad en la interconexión de cada vez más sistemas.

La integración conjunta de capacidades es el tercer pilar del concepto IW. Como detalla Conner (2023), este pilar incluye aspectos relacionados con la maniobra de la fuerza en el EME, operaciones en el espacio, fuegos, EW e INFOOPS. La integración conjunta de capacidades se lleva a cabo a través del proceso de *joint targeting*.

No obstante, para tener una visión completa de lo que supone la integración conjunta de capacidades, es necesario profundizar en el significado del concepto de las operaciones de información (INFOOPS). A este respecto, las INFOOPS son responsables de:

«coordinar las actividades de información para crear efectos deseados sobre los sistemas y procesos de información de los adversarios, reales o potenciales, y otras audiencias autorizadas, para influir en su voluntad, percepciones y capacidades, a la vez que se explotan y protegen los propios, en apoyo a la consecución de los objetivos operacionales y estratégicos» (Ministerio de Defensa, 2018: 131).

Según Theohary (2018: 2): «las INFOOPS tienen lugar en el nivel operacional, y enlazan las capacidades y tácticas de información con la estrategia de alto nivel».

En este sentido, la OTAN ha actualizado recientemente su doctrina sobre INFOOPS y estas han pasado a englobar las siguientes actividades: asuntos públicos militares (MilPA)⁸, operaciones psicológicas (PSYOPS), operaciones en el ciberespacio, EW, cooperación e interacción cívico-militar (CIMIC)⁹, destrucción física,

⁸ MilPA «son las acciones de planeamiento y ejecución de relaciones con los medios de comunicación y empleo de redes sociales, de comunicación interna y de relaciones públicas, para promocionar los objetivos y facilitar el conocimiento y comprensión de los aspectos militares de la operación» (Ministerio de Defensa, 2018: 131).

⁹ «La función conjunta CIMIC comprende un conjunto de capacidades que se utilizan en apoyo a la consecución de los objetivos de la operación, permitiendo al mando

seguridad de las operaciones (OPSEC), decepción, información garantizada, integración de EDT, encuentros¹⁰, y presencia, actitud y perfil (PPP).

Del párrafo anterior ya se infiere la fricción doctrinal que puede surgir entre los conceptos IW e INFOOPS, y sobre la que se profundizará más adelante. En cualquier caso, para Braswell (2017) este modelo de integración proporciona muchos beneficios. Aeschbach (2022) va incluso más allá y considera que, para los mandos operacionales, IW actúa como elemento integrador de capacidades a nivel táctico.

En definitiva, IW coordina y sincroniza a nivel táctico diferentes *information-related capabilities* (IRC) para contribuir a generar efectos y a crear condiciones operacionalmente deseables. Consiste en alcanzar una superioridad en el combate a través del entorno de la información (Conner, 2023). Estas IRC se definen como herramientas, técnicas o actividades empleadas dentro del entorno de la información que contribuyen a alcanzar objetivos específicos (Kirschbaum, 2021). Mediante la sincronización de dichas IRC, IW contribuye a la eficacia operativa de la fuerza en el EI.

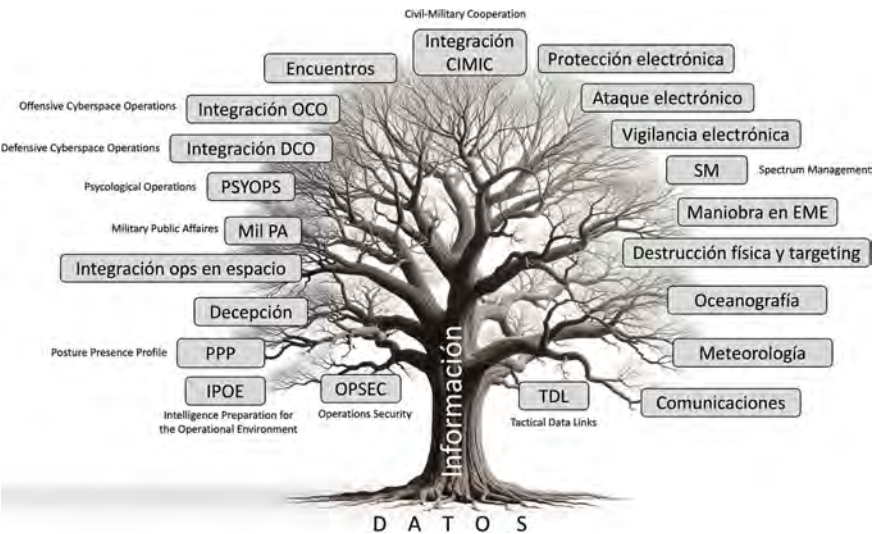


Figura 3. Conjunto de capacidades relacionadas con la información (IRC).
Fuente: elaboración propia

participar de forma efectiva en el amplio espectro de las interacciones cívico-militares (CMI) con los diferentes actores civiles» (Ministerio de Defensa, 2018: 131).

¹⁰ También conocidos como interacción personal y que incluyen *strategic engagement*, *key leader engagement* y *soldier level engagement*.

Por otra parte, cabe destacar que no existe un listado concreto de IRC porque el número de herramientas y técnicas que pueden emplearse en el EI es infinito (Kirschbaum, 2021). A modo de símil, las IRC pueden entenderse como ramas que nacen de un tronco basado en la información, y que emplean los datos como nutrientes absorbidos por las raíces. Según Ros (2024), la doctrina aliada tampoco enumera de forma finita el conjunto de IRC. No obstante, la siguiente figura representa las IRC que han podido ser identificadas por este experto.

Llegados a este punto, se puede afirmar que IW es una disciplina que permite «operacionalizar» el ámbito cognitivo en el nivel táctico. Por ello, su objetivo final podría ir más allá de la superioridad en la información y apuntar hacia la superioridad táctica en la decisión. Esta sería entendida como:

«el estado de ventaja competitiva en el enfrentamiento que permite a los comandantes e integrantes de la Fuerza tomar decisiones mejor informadas, rápidas y adaptadas a la situación que el adversario o competidor, mediante la optimización del empleo del instrumento de poder de la información propio y la alteración, en su caso, del empleado por el citado el adversario o competidor» (Ministerio de Defensa, 2020a: 2).

2.3. Mirando al futuro

En el entorno operativo a largo plazo (2035), el dato se erige como un activo estratégico. «Las acciones en el ciberespacio, el espacio ultraterrestre y el ámbito de operación cognitivo, junto con la utilización de tecnologías emergentes y disruptivas (EDT) [...], no cambian la naturaleza de la guerra, pero ya están cambiando las formas de hacerla» (Entorno operativo 2035, 2022: 31). Asimismo, la difícil atribución en los ámbitos ciberespacial y cognitivo, y el empleo ofensivo de medios de comunicación globales combinados con inteligencia artificial (IA), aumentan los riesgos del entorno. En este contexto, disponer y gestionar la información se convierte en el elemento clave para la fuerza conjunta.

Con el análisis documental del «Entorno Operativo 2035» (2022), se han identificado cuatro elementos que permitirán afrontar con mayores garantías los mencionados retos a los que se enfrentará la fuerza conjunta: empleo efectivo del espectro electromagnético, agilidad en la toma de decisiones, integración en el mul-

tidominio y explotación de EDT que contribuyan a alcanzar la superioridad en la información. El aspecto más relevante es que todos ellos están relacionados de forma transversal con los conceptos EMO e IW.

En particular, y como resultado del análisis del proyecto «EDT de mayor interés a nivel nacional» del (CCDC, 2023), se considera que cinco EDT mejorarán la capacidad de la fuerza conjunta para alcanzar la superioridad en la información: inteligencia artificial y *big data*, autonomía y robótica, tecnologías cuánticas y fotónicas, comunicaciones y tecnología espacial. La mayoría de ellas tienen su principal vulnerabilidad en la necesidad de mantener un acceso ininterrumpido al espectro electromagnético y, por tanto, se considera que las EMO juegan y jugarán un papel fundamental. Por otra parte, se abre un horizonte de oportunidades con las EDT, encabezado por la inteligencia artificial y el *big data* como potenciadores. Asimismo, la superioridad en la información va a implicar una carrera por el desarrollo y explotación de las EDT y, por tanto, el binomio entre IW y EDT será indisoluble.

Por último, cabe destacar que, dentro de esa mirada hacia el futuro, las FAS españolas se encuentran en el proceso de incorporar a medio plazo¹¹ las operaciones multidominio (MDO). Son la respuesta a los desafíos actuales de agilidad y complejidad, mediante la explotación de una adecuada interoperabilidad y conectividad que posibilite un control distribuido de los medios para permitir la integración de todas sus capacidades (Ministerio de Defensa, 2021e). En cualquier caso, el éxito de las MDO descansa sobre la superioridad en la información y, para ello, las MDO necesitan un acceso ininterrumpido al espectro electromagnético. Por este motivo, las MDO están muy relacionadas con los conceptos EMO e IW.

3. Aspectos de conflicto entre EMO e IW

3.1. Aproximación sistémica

Para aplicar el marco teórico, se ha utilizado un sistema militar genérico y simplificado como caso de estudio. Desde la perspectiva militar, un sistema consiste en un «conjunto de personal, material, procedimientos y, en su caso, organismos que actúan

¹¹ Con este propósito, el JEMAD sancionó en 2023 un concepto exploratorio de cómo debe evolucionar la fuerza conjunta hacia el multidominio.

íntimamente relacionados, desarrollando la misma función» (Ministerio de Defensa, 2018: 53). Según Birrell (2023), el propósito de un sistema es generar un determinado valor añadido a aquellos que lo operen. En este caso concreto, el propósito del sistema militar es alcanzar la superioridad en el espacio de las operaciones.

Para el caso de estudio, este sistema militar genérico se ha dividido en dos subsistemas. El primero de ellos está asociado a EMO y tiene como propósito garantizar la superioridad en el espectro. El segundo está vinculado a IW y su finalidad es alcanzar la ventaja en la información sobre el adversario. Ambos subsistemas están compuestos por los mismos elementos (capacidades, flujos de información y nodos) y los dos contribuyen a dicha finalidad superior común.

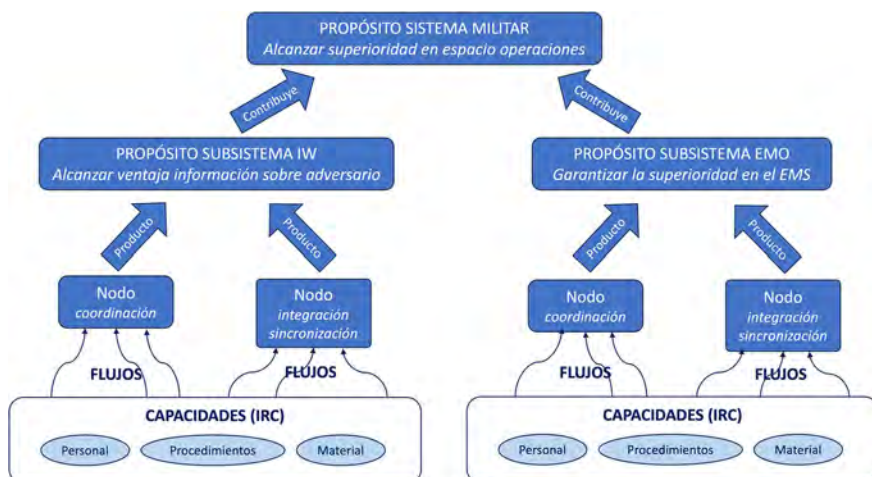


Figura 4. Mapa conceptual sobre el sistema militar estudiado. Fuente: elaboración propia

El primer aspecto que se infiere gracias a esta aproximación sistémica, y que se ha podido demostrar a lo largo de la investigación, es que los subsistemas EMO e IW son complementarios. Aunque tienen diversas capacidades en común, la forma de aplicarlas es diferente porque el propósito de cada subsistema es distinto. Asimismo, los aspectos diferenciadores completan la perspectiva individual de cada subsistema y aportan valor añadido al estudio del sistema como un todo.

En segundo lugar, y mediante la aplicación del marco teórico, se ha comprobado que el valor que proporcionan EMO e IW es

sinérgico, puesto que el efecto del sistema es superior a la suma de los efectos individuales. En otras palabras, el valor generado es producto de las interacciones como propiedad emergente del sistema y ninguna de las partes que compone el sistema puede producir dicho valor por sí sola (Birrell, 2023).

A pesar de lo anterior, todo sistema presenta anomalías en sus procesos y aspectos de conflicto internos que reducen su sincronización. Por ello, resulta indispensable identificar y eliminar dichas contradicciones, para así poder elevar el valor que genera el sistema en su conjunto (Birrell, 2023).

3.2. Aspectos de conflicto entre los subsistemas IW y EMO

Desde la óptica de la teoría de las restricciones, Birrell (2023) propone estudiar el flujo de un sistema, en este caso los procesos de trabajo, como si se tratara de una red fluvial para así poder identificar bloqueos, interrupciones o pérdidas que afecten a la productividad. Y como resultado de este análisis sobre el sistema militar genérico, se han identificado seis aspectos de conflicto entre los subsistemas EMO e IW.

3.2.1. Operaciones en el ciberespacio (CO)

Las CO se definen como «las acciones llevadas a cabo en o a través del ciberespacio con la finalidad de preservar la libertad de acción propia o causar efectos en apoyo a los objetivos del comandante» (Ministerio de Defensa, 2021e: 42). Pueden tener un carácter defensivo (DCO) u ofensivo (OCO).

Desde la perspectiva EMO, la coordinación con las CO es fundamental porque ambas disciplinas están vinculadas al espectro electromagnético. Como detalla la *PDC-3.20* (2021d), el empleo coordinado de acciones EW y de actividades en el ciberespacio genera efectos sinérgicos. Pero si las dos disciplinas ejecutaran sus acciones de manera independiente, se producirían conflictos e interferencias que degradarían su efectividad.

En cambio, el nexo entre IW y CO es la información en sí. En palabras de Millán (2022), el ciberespacio es el ámbito artificial que ha sido conformado alrededor de la información como activo estratégico. Por una parte, las CO permiten que la fuerza sea capaz de gestionar la información, garantizando su disponibilidad, integridad y confidencialidad. Y, por otra parte, tratan de

negarle al adversario la gestión de la suya. La primera aproximación está relacionada con el pilar IW de asegurar el C2 y la segunda con el pilar IW de integración conjunta. Según Theohary (2018), el ciberespacio es un multiplicador de fuerzas para IW.

Por otra parte, Millán (2022) asegura que todos los mandos componentes se ven afectados por las CO y que estas no son desarrolladas en exclusividad por el mando componente del ciberespacio (Millán, 2022). En consecuencia, es importante que existan mecanismos de coordinación y sincronización a nivel operacional. Estos mecanismos serán estudiados en el epígrafe 4, como herramientas para eliminar estas contradicciones.

3.2.2. ISR y SIGINT

El *joint* ISR se define como «el conjunto integrado de capacidades de operaciones e inteligencia, que sincroniza e integra el planeamiento y empleo de los medios de obtención, con el tratamiento, explotación y difusión de la información resultante, en apoyo directo al planeamiento, preparación y ejecución de las operaciones» (Ministerio de Defensa, 2018: 129). En otras palabras, es el proceso de trabajo que permite asignar, en tiempo y forma, los medios ISR más adecuados a las necesidades de los ciclos de inteligencia, operaciones y *targeting*.



Figura 5. Esquema conceptual de JISR. Fuente: elaboración propia

La relación entre EMO e ISR está vinculada a la explotación del espectro electromagnético en beneficio de la vigilancia y de la inteligencia (Ministerio de Defensa, 2021a). Por una parte, SIGINT es una disciplina de obtención, que incluye inteligencia electrónica (ELINT) y de comunicaciones (COMINT), y que alimenta el ciclo de inteligencia a través de los procesos de ISR conjunto (PDC-2.7, 2020). Por otra, la vigilancia electrónica (ES) contribuye al reconocimiento e identificación de amenazas y, aunque su objetivo sea proporcionar opciones de respuesta inmediata, también apoya el conocimiento del entorno y las necesidades de información. Por tanto, la sinergia de EMO e ISR permite apoyar el planeamiento y conducción de las operaciones, contribuir al orden de batalla electrónico (OBE), y recopilar información para la inteligencia actual (Ministerio de Defensa, 2021a).

En cambio, la aproximación IW al ISR es más amplia y está orientada a alcanzar la superioridad en la información. En primer lugar, IW trata de optimizar los flujos de información dentro de la fuerza, desde la obtención de datos por plataformas ISR hasta la diseminación de inteligencia al comandante (Conner, 2023). Por otra parte, y como apunta Trussler (2019), la cantidad de información obtenida por los sensores no es el factor relevante, sino su precisión y la velocidad a la que se gestiona. En tercer lugar, IW busca optimizar de manera holística la «sensorización» del campo de batalla (Aeschbach, 2022) y evalúa cómo se comporta el sistema ISR del adversario para explotar sus vulnerabilidades (Braswell, 2017).

Con esta argumentación se puede inferir la necesidad de disponer en el nivel operacional de un centro específico que optimice los flujos de información crítica en la fuerza, que maximice la «sensorización» del campo de batalla y que explote las debilidades de las capacidades ISR adversarias. Asimismo, también es necesario un elemento en el nivel operacional que integre y sincronice las misiones de obtención. Ambos serán estudiados en el epígrafe 4, como herramientas para eliminar estas contradicciones.

3.2.3. Apoyo Espacial

En la actualidad se está produciendo un aumento exponencial en el uso, tanto civil como militar, de capacidades espaciales. En particular, el apoyo espacial consiste en proporcionar datos, productos y servicios a través del espacio en beneficio de actividades, misiones y operaciones (NATO, 2024). En este sentido,

la OTAN ha establecido en los estados mayores la función *space support coordination* (SpSC), para integrar en las operaciones el apoyo espacial (NATO, 2016). En España, el *space support coordinator* es CMOPS (Lalinde, 2024).

Desde la perspectiva EMO, el espectro electromagnético es el elemento que une los tres segmentos que conforman un sistema satelital: el segmento espacial, el segmento de control, y el terminal o usuario. Por tanto, es necesario monitorizar, asegurar y proteger el espectro para garantizar el funcionamiento de los sistemas satelitales. Las comunicaciones satelitales, la información PNT y la meteorología espacial son tres de los aspectos espaciales más relevantes para las EMO (Ministerio de Defensa, 2021a).

Para IW, el aspecto relevante es la contribución de las capacidades espaciales a la superioridad de la información. En primer lugar, para apoyar el conocimiento del entorno con productos de observación de la Tierra, avisos de sobrevuelo de satélites, avisos de lanzamiento de misiles, previsión de impacto meteorológico espacial, etc (Waggoner, 2019). Y, por otra parte, para asegurar el mando y control (Braswell, 2017) con servicios de posicionamiento global (GNSS), comunicaciones satelitales, etc. El espacio es un ámbito que debe ser protegido de los intentos de disrupción por parte de adversarios cada vez más agresivos y sofisticados (White *et al.*, 2019). Asimismo, Aeschbach (2022) defiende que IW es la disciplina adecuada para integrar el apoyo espacial en el nivel táctico a las unidades desplegadas.

Por otra parte, un aspecto contemplado específicamente por IW son las operaciones en entornos donde la capacidad de mando y control ha sido degradada o denegada (C2D2E). El adversario consigue estos efectos atacando electrónicamente las comunicaciones vía satélite y la información PNT procedente del espacio, aunque también puede emplear otros vectores como la perturbación de comunicaciones o los ataques desde el ciberespacio. Uno de los desafíos de estos escenarios es la atribución, puesto que en ocasiones es difícil discernir su origen deliberado (ataque), accidental (interferencias) o natural (causas ambientales) (Medina, 2020). GNSS y SATCOM son tecnologías indispensables en las operaciones actuales, y aunque existen medios alternativos para operar en caso de disrupción, es necesario invertir tecnológicamente y prepararse con antelación (Scott, 2021).

Como conclusión, es necesario disponer en el nivel operacional de un centro específico que ejerza la función SpSC y coordine

todas las actividades relacionadas con el espacio en apoyo a las operaciones. Esta necesidad será estudiada en el epígrafe 4.

3.2.4. Navigation Warfare

Desde la óptica de las EMO, NAVWAR está vinculado, principalmente, a EW. Por una parte, el ataque electrónico (EA) puede bloquear o engañar la información PNT del adversario y afectar así a su toma de decisiones. Por otra, la defensa electrónica (ED) contribuye a garantizar el acceso propio a la información PNT. Y, por último, la vigilancia electrónica (ES) ayuda a localizar y caracterizar el origen de las perturbaciones del adversario (NATO, 2020). En cualquier caso, y debido a las características de las señales PNT, NAVWAR también tiene relación con el espacio y el ciberespacio (Martínez, 2022)

Por otra parte, NAVWAR participa en los tres pilares del concepto IW. En primer lugar, un ataque a la señal PNT propia afectaría tanto al pilar de conocimiento del espacio de las operaciones¹² como al mando y control asegurado (Medina, 2020). Por tanto, es necesario aplicar técnicas de NAVWAR defensivo y de apoyo en ambos pilares para mantener y proteger el acceso a la información PNT. En segundo lugar, las acciones para interrumpir el acceso del adversario a su información PNT (NAVWAR ofensivo) tienen la consideración de fuegos¹³ y, por tanto, se integran en el tercer pilar IW a través del *targeting* conjunto (White, Barrett y Bebbber, 2019).

En consecuencia, y para resolver este aspecto de conflicto sobre NAVWAR, se puede concluir que es necesario disponer de dos elementos en el nivel operacional. Por una parte, un centro específico que coordine las actividades NAVWAR defensivas y de apoyo, y, por otra, un elemento que permita integrar el NAVWAR ofensivo en los fuegos conjuntos. Ambas necesidades serán investigadas en el epígrafe 4.

3.2.5. Guerra electrónica (EW)

Para el concepto EMO, EW es su disciplina nuclear y de combate. Integra las acciones de vigilancia electrónica (ES), defensa

¹² Por ejemplo, los sistemas no tripulados y el resto de plataformas ISR que contribuyen al conocimiento del entorno necesitan señales GPS para poder navegar y operar (Kallenborn, 2023).

¹³ «Conjunto de actividades que emplean sistemas de armas con capacidades letales y no letales para generar los efectos deseados sobre el adversario» (Ministerio de Defensa, 2018: 129).

electrónica (ED) y ataque electrónico (EA), con el propósito de que la FC haga un uso más efectivo del EME y reduzca o impida la capacidad del adversario de operar en él. Esto incluye el empleo de sensores EW, el análisis y gestión del EME, y la ejecución de acciones para generar efectos (Ministerio de Defensa, 2021a).

Desde la perspectiva IW, EW participa activamente en los tres pilares sobre los que se asienta el concepto IW. Aunque en este caso, y a diferencia de lo que ocurre en las EMO, las herramientas se aplican en el nivel táctico de las operaciones (Braswell, 2017). En primer lugar, la vigilancia electrónica (ES) contribuye de manera sustancial al conocimiento del espacio de las operaciones (1.^{er} pilar IW). En segundo lugar, la protección y la defensa electrónica (ED) juegan un papel relevante en asegurar el mando y control (2.^o pilar IW). Y, por último, tanto el ataque electrónico como la maniobra en el EME se incardinan en el tercer pilar IW: la integración conjunta de capacidades (Conner, 2023).

En cualquier caso, la maniobra en el EME requiere una reflexión adicional. Para Braswell (2017), IW permite integrar y sincronizar la maniobra en el EME y en el EI con los dominios físicos, para generar un efecto multiplicador de la capacidad de combate. En su opinión, una mala integración impide alcanzar una posición de ventaja en la situación táctica. Y, en palabras de Garret (2023), las capacidades avanzadas de EW serán las que posibiliten la movilidad de la fuerza en los próximos años, junto a la robótica y los sistemas no tripulados. Asimismo, el espectro electromagnético debe ser tenido en cuenta para generar efectos psicológicos sobre determinados actores (NATO, 2023b), con el objetivo de influir y promover percepciones, actitudes y comportamientos favorables a las operaciones propias.

A modo de conclusión sobre los aspectos de conflicto EW, se percibe de nuevo la necesidad de disponer de dos elementos específicos en el nivel operacional. En primer lugar, un centro específico que coordine todo lo relativo a la vigilancia y defensa electrónica, incluyendo las aportaciones al conocimiento del espacio de las operaciones y al mando y control asegurado. Por otra parte, un elemento que permita integrar el ataque electrónico y la maniobra en el EME en los fuegos y efectos conjuntos. Ambas necesidades serán investigadas en el epígrafe 4.

3.2.6. Gestión del espectro (SM)

Desde el punto de vista de las EMO, *spectrum management* (SM) es una herramienta de apoyo al comandante operacional en la gestión del espacio de las operaciones (NATO, 2020). Como detalla Martínez (2022), las actividades SM no solo abarcan la habitual gestión de frecuencias, sino que también incluyen el análisis del espectro y de los medios que hacen uso de este, con el objetivo de asesorar en la optimización del empleo de capacidades.

Aunque IW comparte la misma aproximación a SM, en este caso hay un matiz diferenciador. Para IW, SM es una capacidad que apoya al comandante táctico en la coordinación de frecuencias y resolución de interferencias electromagnéticas para el combate (Conner, 2023). IW es la disciplina que asesora al comandante en cómo emplear el espectro y cómo posicionar a la fuerza para explotar las oportunidades que presente el EME. Sin duda alguna, esta perspectiva refuerza la visión táctica de IW sobre ello.

Como en términos generales ambas disciplinas tienen la misma aproximación, la existencia de un centro específico en el nivel operacional que coordine todas las actividades de SM es suficiente para resolver el conflicto identificado.

3.3. Síntomas de falta de sincronización

Birrell (2023: 11) considera que «el valor generado por los sistemas [empresas] es directamente proporcional a la sincronización que se logra entre sus elementos y partes relacionadas, tanto interna como externamente». Al estudiar un sistema, se pueden identificar una serie de hechos que evidencian falta de sincronización. Estos hechos bloquean el incremento de valor que produce el sistema o demandan un mayor esfuerzo para que el sistema sea capaz de alcanzar lo mismo. En todos ellos, existe una relación causa-efecto, por lo que resulta esencial encontrar esa causa raíz. Una vez eliminada o mitigada, se le habrá generado un importante beneficio al sistema (Birrell, 2023).

Como resultado de aplicar el marco teórico, se han identificado dos hechos no deseados que evidencian falta de sincronización en el sistema objeto de la investigación. Se describen a continuación en los siguientes apartados.

3.3.1. IW. Ausencia de lenguaje estandarizado

El primer síntoma está relacionado con la falta de un lenguaje común en todo lo relacionado con alcanzar la superioridad en la información. A este respecto, no existe un lenguaje estandarizado a nivel operacional y de mandos componentes y, por tanto, cada uno lo enfoca de manera diferente.

En este sentido, el concepto táctico IW se conoce y se aplica exclusivamente en la comunidad naval. Nació en el seno de la USN, se incorporó en 2021 a la doctrina marítima de la OTAN con el ATP-113 y se ha introducido en el cuerpo doctrinal nacional para el entorno marítimo, a través de la PDC-3.1 (2022b). Asimismo, el propio «Concepto básico EMO» (2021a) reconoce que todas las actividades que abarcan las EMO están contempladas como *information-related capabilities* de IW para el entorno marítimo.

En cambio, la doctrina española para las operaciones en el ámbito terrestre (Ministerio de Defensa, 2023) no hace ninguna referencia a IW. Esta publicación dedica un párrafo a desarrollar la actuación en el ámbito cognitivo y, para ello, incluye actividades de MilPA, INFOOPS, PSYOPS y CIMIC, adecuadamente armonizadas mediante la comunicación estratégica (STRATCOM). Y también explica someramente la función táctica de información, para actuar sobre el conocimiento, la capacidad y la voluntad del adversario y de las audiencias.

Asimismo, la doctrina española para las operaciones en el ámbito aeroespacial (Ministerio de Defensa, 2022a) tampoco hace ninguna referencia a IW. La publicación desarrolla en detalle las misiones aéreas de información, incluidas en la taxonomía de los cometidos de ataque aéreo y coordinadas mediante la función de INFOOPS. También presta una atención especial a la importancia de sincronizar y coordinar adecuadamente las acciones aeroespaciales con la campaña de información estratégica conjunta.

Por tanto, se puede inferir que la causa raíz de este problema se encuentra en que el concepto IW se emplea exclusivamente en la comunidad naval.

3.3.2. Función conjunta de información

El segundo síntoma está vinculado a la función conjunta de información, que actualmente comprende:

«aquellas actividades cuya finalidad principal se orienta a la gestión, denegación y uso de la información, así como a la integración deliberada de estas actividades con las del resto de funciones conjuntas, para promover percepciones, actitudes y comportamientos favorables a las operaciones propias de determinadas audiencias e influir en la toma de decisiones humanas o automatizadas» (Ministerio de Defensa, 2018: 130).

A pesar de la amplitud de su definición, cuando la publicación desarrolla esta función conjunta se limita a resaltar la vinculación estrecha que mantiene con INFOOPS y MilPA, y no establece ninguna relación con las capacidades operativas de información que puede proporcionar la fuerza conjunta¹⁴. Cabe destacar que estas capacidades de información no están atribuidas a ningún mando componente concreto y, por tanto, son transversales a todos ellos.

En este sentido, se debe tener en cuenta que las funciones conjuntas son agrupamientos de capacidades y actividades relacionadas entre sí, para que sea más fácil su integración, sincronización y dirección. Por tanto, la ausencia de un catálogo integral de actividades o capacidades basadas en la información sobre la que se desarrolle esta función conjunta puede considerarse un síntoma de falta de sincronización. Asimismo, tampoco se señala la especial relevancia que tiene esta función conjunta para operar en el ámbito cognitivo, según lo que determina el (Ministerio de Defensa, 2020a).

Desde la perspectiva OTAN, la doctrina recientemente sancionada establece cinco capacitadores clave para la función conjunta de información: las operaciones psicológicas (PSYOPS), los asuntos públicos militares (MilPA), las operaciones electromagnéticas (EMO), las operaciones en el ciberespacio (CO) y las actividades de interacción personal. Asimismo, señala que esta función conjunta es esencial para influir en las audiencias y poder comprender el impacto de las EDT en el entorno de la información (NATO, 2023a).

¹⁴ Las capacidades operativas de información que puede proporcionar la FC son: «coordinación de las actividades de los asuntos públicos militares, operaciones psicológicas, participación de actividades de *targeting*, actividades de seguridad de la información, actividades de interacción personal, contribución de operaciones de decepción, y conocimiento del ámbito cognitivo» (Ministerio de Defensa, 2018: 62). A las anteriores, la (Ministerio de Defensa, 2021b) añade también las actividades CMI/CIMIC.

Por otra parte, las actividades basadas en la información (*information activities*) son aquellas llevadas a cabo por cualquier medio o capacidad cuyo propósito sea generar efectos psicológicos¹⁵ (NATO, 2024). En particular, el nuevo AJP-10.1 (Ed.A V1) (2023) agrupa las actividades basadas en la información en tres bloques: aquellas orientadas a proteger la libertad de acción propia en el EI; aquellas enfocadas a inducir, reforzar, convencer o alentar comportamientos, percepciones o actitudes, y aquellas orientadas a luchar contra las capacidades de información y C2 del adversario. Esta taxonomía puede facilitar el necesario desarrollo conceptual de la función conjunta de información en España.

Por último, se puede determinar que la causa raíz de este problema se encuentra en que el desarrollo conceptual de la función conjunta de información en España todavía no ha incorporado las últimas tendencias doctrinales de la Alianza.

4. Herramientas de coordinación y sincronización

Al objeto de organizarse de manera permanente, un Estado Mayor de nivel operacional se divide en secciones, las cuales se numeran correlativamente por áreas funcionales. Esta organización suele ser común en todos los cuarteles generales aliados y europeos para facilitar la interoperabilidad (Ministerio de Defensa, 2021c).

Área de operaciones		Área de apoyos	
J2	Inteligencia	J1	Personal
J3	Operaciones	J4	Logística
J9	Influencia	JMED	Sanidad operativa
J7	Adiestramiento y lecciones aprendidas	J6	CIS
J5	Planes	J8	Asuntos financieros

Figura 6. Organización por secciones del Mando de Operaciones (MOPS).
Fuente: elaboración propia con datos de Cartelle y Torres (2019)

Sin embargo, las operaciones militares requieren un alto nivel de coordinación y sincronización que excede las capacidades de esta tipología clásica organizativa. Asimismo, la resolución de problemas operativos complejos demanda grupos multifuncionales y

¹⁵ *Cognitive effects* en su definición anglosajona.

multidisciplinarios de expertos. Por este motivo, y de forma complementaria a la mencionada organización funcional permanente, en un Estado Mayor de nivel operacional se forman una serie de centros, células, equipos de planeamiento, grupos de trabajo y juntas. Todos estos órganos trabajan de manera coordinada y sincronizada para apoyar el ciclo de la decisión del comandante durante una operación (Ministerio de Defensa, 2021c).

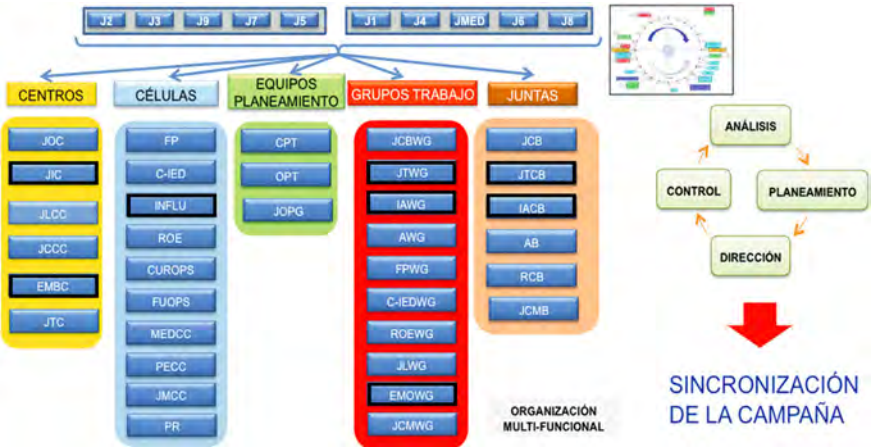


Figura 7. Organización del MOPS para la conducción y planeamiento de las operaciones. Fuente: Cartelle y Torres, 2019

Por tanto, estos órganos son las herramientas del comandante para garantizar la coordinación y sincronización a nivel operacional. La importancia de este aspecto es intrínseca al marco teórico de la investigación (Birrell, 2023: 155), puesto que «el valor que generan los sistemas es directamente proporcional al grado de sincronización de sus partes relacionadas». A continuación, se estudiarán cada uno de estos órganos relacionados con EMO e IW, y que se encuentran resaltados en negro en la figura 7: COEM, sección J9, célula de Influencia, JTCB/JTWG, IACB/IAWG, JCMB/JCMWG y JIC.

4.1. Centro de operaciones electromagnéticas

4.1.1. Descripción

El COEM es un órgano permanente del Estado Mayor del MOPS (EMMOPS) y que, desde el nivel operacional, es responsable de conducir las operaciones electromagnéticas y el resto de las

actividades relacionadas con la EW. Expresado de otra forma, el COEM coordina y sincroniza las EMO durante los procesos de planeamiento y conducción de las operaciones (Ministerio de Defensa, 2021a). Aporta sinergias mediante la priorización, coordinación, sincronización e integración de esfuerzos en el espectro (Nieto, 2022).

El COEM es un centro de reciente creación¹⁶, que ha ido asumiendo responsabilidades progresivamente y conformando una capacidad conjunta. En palabras de Nieto (2022), España es «una de las pocas naciones que dispone de un centro de estas características, conjunto y dotado de recursos». Esta estructura es también una solución eficiente ante la escasez de personal cualificado en esta materia, porque así este capital humano crítico se concentra en el nivel operacional para el planeamiento y conducción de las EMO. Como menciona este autor, estos «construc-tos» son «bienvenidos en la estructura orgánica porque utilizan sus recursos en las operaciones a pesar de no estar plenamente conformados como capacidad militar» y contribuyen a mejorarla.

Por otra parte, disponer de un COEM a nivel operacional facilita la comprensión de asuntos muy particulares y específicos, como los relativos al espectro electromagnético y genera confianza en el uso de la capacidad. El COEM enlaza el nivel táctico de las EMO, que tiene un marcado carácter técnico, con el nivel estratégico de la conducción de las operaciones y para el que es necesario emplear un lenguaje diferente (Nieto, 2022).

Según Martínez (2022), «el centro se encuentra ya dotado de personal para cubrir [...] las áreas de EW, SIGINT, gestión del espectro, NAVWAR, espacio y operaciones en el ciberespacio». Como detalla Lalinde (2024), en el COEM conviven especialistas de operaciones, de inteligencia y de comunicaciones, con una entidad variable en función de las actividades operativas.

Para ejercer sus cometidos de coordinación y sincronización, el COEM establece relaciones funcionales con los «Elementos de Operaciones Electromagnéticas» (EOEM) que se establezcan en las organizaciones operativas subordinadas¹⁷. Estos EOEM serán

¹⁶ A través de la Instrucción 55/2021, de 27 de octubre, del jefe de Estado Mayor de la Defensa, por la que se desarrolla la organización del Estado Mayor de la Defensa (2021).

¹⁷ Mandos componentes, mandos operativos permanentes y órganos nacionales militares relacionados con organizaciones internacionales o multinacionales encuadrados en la estructura operativa.

de composición y funciones variables, en virtud de las peculiaridades de cada operación (Ministerio de Defensa, 2021a).

En el caso particular del entorno marítimo, el «Concepto básico EMO» (2021a: 40) explica que, subordinado al

«mando componente marítimo (MCM) y siguiendo la doctrina OTAN (ATP-113), las fuerzas navales podrán disponer de un IWC (*Information Warfare Commander*) en su organización para el combate que, bajo la dependencia del OTC (*Officer in Tactical Command*), tiene la responsabilidad de coordinar y sincronizar todas las IRC (*Information-related capabilities*) para alcanzar los efectos deseados por el MCM en el entorno de la información. Dichas IRC incluyen todas las actividades que abarcan las EMO, y, por tanto, el IWC se convierte en su principal asesor y gestor del MCM/OTC al respecto».

Para la conducción de las operaciones a medio plazo, el COEM se apoya en el grupo de trabajo de EMO (EMOWG) para la coordinación, priorización y sincronización de todas las acciones operacionales en el EME. Bajo el liderazgo del COEM, en este grupo de trabajo participan los EOEM de los mandos subordinados y los representantes del MOPS de las áreas implicadas en EMO (Lalinde, 2024).

4.1.2. El COEM en los subsistemas EMO e IW

En términos generales, el COEM permite aumentar la sincronización del sistema, y, por tanto, incrementa los réditos que este proporciona. Como se infiere del análisis anterior, el COEM no solo es un mecanismo de coordinación y sincronización del subsistema EMO, sino que también contribuye al propósito del subsistema IW. Por tanto, esta circunstancia visibiliza la complementariedad de los conceptos EMO e IW.

En particular, el COEM aglutina la coordinación y sincronización de todas las acciones operacionales de EW, SIGINT, NAVWAR, SM y de apoyo en el espacio y ciberespacio, con independencia de que provengan del subsistema EMO o IW. Por ello, la existencia del COEM permite eliminar algunas anomalías en los flujos o aspectos de conflicto del sistema investigado, las cuales fueron analizadas en el epígrafe 3.2: asegurar el mando y control propio, coordinar las acciones EW con las actividades en el ciberespacio, coordinar la vigilancia y la defensa electrónica, ejercer la función

SpSC y coordinar las actividades relacionadas con el espacio en apoyo a las operaciones, coordinar las actividades NAVWAR de carácter defensivas y de apoyo, integrar la maniobra de la fuerza en el EME y coordinar las actividades de SM.

Suprimir estas anomalías en los flujos, o contradicciones, incrementa la sincronización del sistema y aumenta el valor que genera. En otras palabras, mejora la contribución del sistema a alcanzar la superioridad en el espacio de las operaciones.

4.2. Sección de influencia (J9)

4.2.1. Descripción

El cometido de la actual sección J9 del MOPS es integrar las acciones de influencia en el planeamiento, conducción y seguimiento de las operaciones, incluyendo la sincronización de las operaciones de información (INFOOPS), interacción y cooperación cívico-militar (CMI/CIMIC), y asuntos públicos militares (MilPA). Para ello, la sección se divide orgánicamente en cuatro áreas, como se señala en la figura 8 (Sierra, 2024).

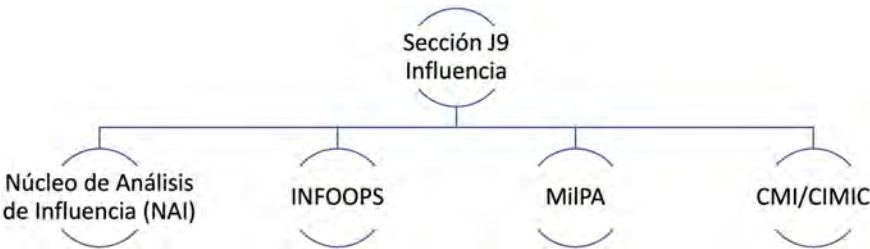


Figura 8. Estructura orgánica de la sección J9 del MOPS. Fuente: elaboración propia

El Núcleo de Análisis de Influencia (NAI) es responsable de analizar el entorno de la información (EI) en el nivel operacional. Mediante el empleo de herramientas específicas, el NAI identifica campañas contras los intereses nacionales, narrativas contrarias u oportunidades que pueden ser explotadas en las operaciones. Proporciona el necesario *information environment assessment* (IEA) y permite valorar las acciones propias que se llevan a cabo durante las operaciones (Sierra, 2024). Respecto a INFOOPS, MilPA y CMI/CIMIC, cabe destacar que los conceptos ya fueron explicados anteriormente en el epígrafe 2.2.

Como detalla Sierra (2024), la organización que adopta el MOPS se basa en el modelo francés de 2012, y por el que todas las actividades susceptibles de provocar cambios en las percepciones de las audiencias se integraron en una única sección del Estado Mayor. En cambio, la OTAN ha querido potenciar la función conjunta de información, mediante la creación de una nueva sección J10 (STRATCOM) en la organización de un Estado Mayor¹⁸. En la OTAN, esta sección lidera el análisis de audiencias y del entorno de la información, planea e integra las actividades relacionadas con la información para generar los efectos deseados, y desarrolla de manera sincronizada las actividades de comunicación con sus propias capacidades. Asimismo, esta nueva sección también es responsable de dirigir las actividades contra la desinformación y la lucha contra la información hostil (NATO, 2023b).

Durante la ejecución de las operaciones, se establece una Célula de Influencia dentro de la sección de J3 para apoyar la conduc-

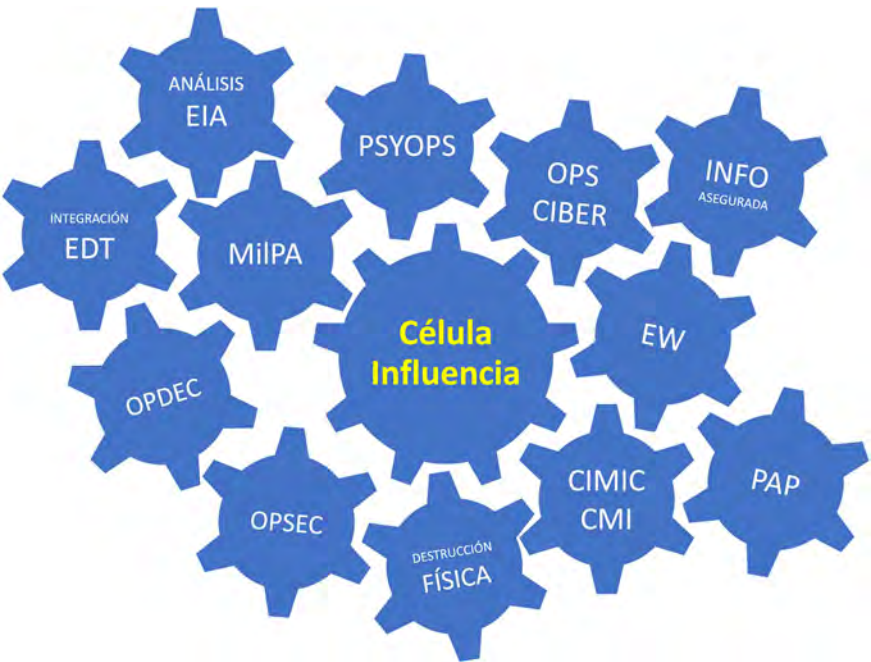


Figura 9. Actividades que puede coordinar la Célula de Influencia del JOC.
Fuente: elaboración propia

¹⁸ La sección J9 en la OTAN se queda para atender todas las necesidades derivadas de CIMIC/CMI.

ción a corto y medio plazo. Esta célula se integra en el Centro de Operaciones Conjuntas (JOC), que se mantiene activado en permanencia (24/7) (Cartelle y Torres, 2019).

Por tanto, la Célula de Influencia debe coordinar en operaciones todas las acciones relacionadas con la valoración del entorno de la información (IEA), asuntos públicos militares (MilPA), operaciones psicológicas (PSYOPS), cooperación e interacción cívico-militar (CIMIC/CMI), seguridad de las operaciones (OPSEC), decepción, información garantizada, integración de EDT, encuentros y presencia actitud y perfil (PPP). Asimismo, también coordina las acciones operacionales de EW, ciberespacio y destrucción física, cuyo objeto sea generar efectos psicológicos.

4.2.2. La célula de influencia en los subsistemas EMO e IW

La Célula de Influencia es, principalmente, un mecanismo de coordinación del subsistema IW, pero también contribuye en algunos aspectos al propósito del subsistema EMO. Nuevamente, esta circunstancia visibiliza la complementariedad de los conceptos EMO e IW.

Por otra parte, la existencia de la Célula de Influencia permite canalizar hasta el nivel operacional todos los flujos relacionados con INFOOPS y con el análisis del entorno de la información. Aunque en este caso no se eliminan directamente aspectos de conflicto del sistema investigado, los cuales fueron analizados en el epígrafe 3.2, la Célula de Influencia sí permite aumentar la coordinación de todo el sistema. De esta manera, se incrementa la sinergia y el valor que genera dicho sistema.

4.3. Procesos de *targeting* conjunto y actividades de información

4.3.1. *Targeting* conjunto (JTGT)

El JTGT se define como «el proceso transversal e iterativo por el cual se determinan los efectos necesarios para alcanzar los objetivos asignados al comandante, y se identifican las acciones necesarias para crear los efectos deseados con los medios disponibles» (Ministerio de Defensa, 2018: 118). En palabras de García (2023), el *targeting* es una herramienta ágil e integradora que permite la aplicación de efectos entre diferentes ámbitos de las operaciones, con una aproximación multidominio.

Por tanto, en el nivel operacional se llevan a cabo una serie de pasos secuenciales de JTGT. Los objetivos se descomponen en blancos, que son seleccionados y priorizados, se establecen y sincronizan acciones, se delimitan los efectos a producir, se asignan medios para su ejecución y se valoran los resultados. Debe tenerse en cuenta que las acciones a realizar pueden ser letales o no letales, y los efectos generados pueden ser físicos, psicológicos o virtuales. Por tanto, el JTGT es un proceso que se incardina en las funciones conjuntas de mando y control, fuegos, inteligencia e información (Ministerio de Defensa, 2019).

La Junta de Coordinación de Targeting Conjunto (JTCB) es el órgano de decisión en materia de JTGT, que se reúne con el objeto de recibir directrices del comandante operacional o someter asuntos a su decisión. Esta junta es un elemento esencial de la conducción a medio plazo de las operaciones y su principal cometido es el planeamiento y coordinación del JTGT, incluyendo las acciones letales y no letales. Adicionalmente, promulga directrices y prioridades, resuelve los conflictos que puedan surgir en la nominación de blancos y valida los cambios en las bases de datos (BBDD) de los blancos (Ministerio de Defensa, 2019).

Asimismo, la JTCB está auxiliada por el Grupo de Trabajo de Targeting Conjunto (JTWG) en la conducción a medio plazo de las operaciones. Este grupo no es un órgano de decisión y su misión es preparar, discutir, gestionar y coordinar con antelación suficiente todos los productos de JTGT que se llevan a la JTCB con posterioridad para la decisión del comandante. Para la ejecución de sus cometidos, el JTWG cuenta con el apoyo de todo el personal experto que se integra en el centro permanente de *targeting* conjunto (JTC) del Estado Mayor del MOPS (Ministerio de Defensa, 2019).

4.3.2. Actividades de información (IA)

Las actividades de información son «acciones diseñadas para lograr efectos en el entorno de la información» (Ministerio de Defensa, 2021b: 17), los cuales pueden ser de naturaleza física, virtual o psicológica. Por ello, resulta fundamental disponer de la adecuada organización para integrar, priorizar y sincronizar estas actividades.

A nivel operacional, el órgano que se forma en el MOPS para la conducción a medio plazo de dichas actividades es el Grupo de Trabajo de Actividades de Información (IAWG). Como indica

Sierra (2024), el IAWG es la herramienta principal de trabajo de la Célula de Influencia y permite mantener, dentro del Estado Mayor, una visión común del entorno de la información y de los objetivos de influencia a alcanzar. El IAWG es el foro en donde se coordinan y supervisan todos los planes y actividades relacionadas con el entorno de la información, de forma que estén sincronizadas con el resto de las acciones operacionales. En particular, el IAWG proporciona asesoramiento sobre los efectos que puedan generar otras acciones militares en el entorno de la información y puede proponer la designación de blancos relacionados con la información para su posterior armonización en la JTCB (Ministerio de Defensa, 2021b; NATO, 2023b).

En aquellos casos en los que se exceda el nivel del IAWG, el grupo de trabajo elevará la toma de decisiones directamente o a través de la JTCB. Asimismo, se podrá convocar la Junta de Coordinación de Actividades de Información (IACB), para ejercer la toma de decisiones en el ámbito de la influencia (Sierra, 2024). Cabe destacar que, aunque las juntas y los grupos de trabajo sean de carácter multidisciplinar, la sección J9 es la responsable de proporcionar los especialistas en la materia (Ministerio de Defensa, 2021b; NATO, 2023b).

Por último, conviene reseñar que cualquier acción en los ámbitos de operación físicos (terrestre, marítimo y aeroespacial) y virtual (cibespacio) puede generar efectos psicológicos. Estos efectos podrán ser positivos si las palabras están alineadas con las acciones y proporcionan una posición de ventaja, o negativos cuando presentan contradicciones. A este respecto, la herramienta que proporciona la necesaria coherencia del relato a todos los niveles de las operaciones es la comunicación estratégica (STRATCOM) (Ministerio de Defensa, 2021b). En este sentido, STRATCOM se define como «la integración de todas las capacidades de comunicación, técnicas y funciones de información, con otras actividades militares, para comprender y modelar el entorno de la información, en apoyo del logro de los objetivos de la defensa nacional» (Ministerio de Defensa, 2018: 106). Y como detalla Sierra (2024), la alineación de las actividades de información y del resto de acciones militares con los mensajes aprobados de STRATCOM se lleva a cabo en la IACB.

4.3.3. Confluencia de ambos procesos

Desde una perspectiva conceptual, el comandante operacional conduce a las fuerzas bajo su mando para que ejecuten acciones,

en tiempo, forma y espacio, que generen unos efectos deseados para alcanzar condiciones decisivas, las cuales acabarán llevando a la consecución de los objetivos operacionales. En otras palabras, el comandante operacional tratará de alcanzar una situación final deseada a través de la orquestación de efectos (Ministerio de Defensa, 2018). Por tanto, se puede inferir que los efectos son un elemento esencial del planeamiento y la conducción de las operaciones actuales.

En este sentido, el JTGT es la principal herramienta para el planeamiento y generación de efectos en apoyo a la consecución de los objetivos del comandante. Como se ha detallado anteriormente, el JTGT coordina y sincroniza acciones letales y no letales, para la generación de efectos físicos, virtuales o psicológicos.

En consecuencia, la confluencia de JTGB/JTWG y de IACB/IAWG, como órganos de decisión y trabajo para la generación de efectos, es fundamental en la conducción de las operaciones a medio plazo. Como detalla el *AJP-10 (Ed.A V1)* (2023: 12): «el éxito militar, a nivel operacional y por encima de él, depende casi siempre de la creación de efectos en el ámbito cognitivo»¹⁹.

Respecto a las operaciones electromagnéticas, el COEM tiene un representante de manera permanente tanto en el JTGW como en el IAWG del MOPS (Lalinde, 2024). Por su parte, el jefe de la sección J9-Influencia preside el IAWG, dirige la IACB y participa en JTGB/JTWG (Sierra, 2024).

4.3.4. JTGT e IA en los subsistemas EMO e IW

Se puede concluir que, en el sistema investigado, la JTGB/JTWG y la IACB/IAWG actúan como mecanismos de integración y sincronización de acciones operacionales para la generación de efectos. Por ello, resultan de aplicación tanto para EMO como para IW, ante la necesidad de crear efectos en el EME y en el entorno de la información. En consecuencia, la JTGB/JTWG y la IACB/IAWG permiten mejorar el grado de sincronización de las partes que componen este sistema y, en aplicación del marco teórico, contribuyen a aumentar el valor que este genera.

Asimismo, la JTGB/JTWG y la IACB/IAWG también permiten eliminar algunas anomalías en los flujos o aspectos de conflicto del sistema investigado (epígrafe 3.2). En concreto, permiten supri-

¹⁹ Traducción del autor.

mir las duplicidades EMO/IW que se producían en los siguientes aspectos: integrar en los fuegos y efectos conjuntos el ataque electrónico y la maniobra de la fuerza en el EME, integrar el NAVWAR ofensivo en los fuegos conjuntos, e integrar la generación de efectos desde el ciberespacio.

4.4. Coordinación y sincronización de medios ISR

4.4.1. Descripción

Con el propósito de conseguir la máxima optimización en el empleo de los medios ISR durante la ejecución de las operaciones, la junta conjunta de gestión de la información (JCMB) se reúne de manera periódica en el MOPS. Durante la JCMB se priorizan, coordinan, validan, asignan y sincronizan todas las actividades ISR planeadas a medio plazo. También se coordinan las soluciones a aquellas necesidades de obtención para las que no haya capacidades propias de ISR y se resuelven los conflictos o duplicidades de esfuerzos que hayan podido surgir. El producto final de cada JCMB es la lista de tareas de obtención (CTL) de los medios ISR (Ministerio de Defensa, 2020b).

La JCMB, como órgano de decisión, se apoya en un grupo de trabajo (JCMWG) que lleva a cabo a todas las labores preparatorias y de gestión antes de que se convoque la junta. En este grupo, participan representantes de todas las disciplinas relacionadas con ISR (inteligencia, planes, operaciones, EW, SIGINT, *imagery intelligence*, *human intelligence*, PSYOPS, *targeting*, etc.) (Ministerio de Defensa, 2020b). El COEM está representado en este grupo (Lalinde, 2024), así como la célula de influencia.

Por último, para la conducción de las operaciones se activa un centro de inteligencia conjunta (JIC). El JIC se integra en el centro de operaciones conjuntas (JOC) del MOPS, para apoyar al comandante desde la perspectiva de inteligencia en el seguimiento de las operaciones y la conducción a corto plazo (Cartelle y Torres, 2019). El centro canaliza la provisión de inteligencia en apoyo a las operaciones a corto plazo y proporciona respuestas inmediatas ante necesidades sobrevenidas de ISR.

4.4.2. JCMB, JCMWG y JIC en los subsistemas EMO e IW

De manera general, estos tres órganos permiten aumentar la sincronización del sistema y, por tanto, incrementan los réditos que

proporciona. Asimismo, con su coordinación contribuyen tanto al propósito del subsistema EMO como al del subsistema IW, lo que pone en valor nuevamente la complementariedad de los conceptos EMO e IW.

Por una parte, la JCMB actúa como elemento integrador y sincronizador en el nivel operacional de las misiones de obtención. Por otra, el JIC tiene la capacidad en el nivel operacional de optimizar los flujos de información crítica en la fuerza y maximizar la «sensorización» del campo de batalla. En cualquier caso, la existencia de estos órganos permite eliminar algunos aspectos de conflicto ISR/SIGINT del sistema investigado, que fueron analizados en el epígrafe 3.2, y canalizar de manera adecuada al nivel operacional todos los flujos ISR/SIGINT identificados.

5. Conclusiones

A este respecto, EMO es una herramienta conceptual dirigida, principalmente, al nivel operacional. OTAN ha desarrollado las EMO siguiendo una aproximación *top down* desde el nivel estratégico y España las ha implantado ratificando la doctrina aliada y elaborando un concepto básico sancionado por el JEMAD en 2021. Las EMO se apoyan en la armonización de las estructuras de mando y control mediante un enfoque coordinado, para asegurar la eficacia de la FC en el EME y limitar la libertad de acción del adversario en el mismo. Para conseguirlo, el concepto EMO integra cuatro actividades electromagnéticas principales (EW, SIGINT, SM y NAVWAR) y coordina otras acciones que también dependen del acceso al espectro. Las EMO son un potenciador de efectos en y a través del espectro electromagnético y su propósito es alcanzar la superioridad en el mismo.

Sin embargo, IW es una disciplina que se aplica a nivel táctico para alcanzar la ventaja en la información sobre el adversario. Tuvo su origen en la USN, y fue incorporada en la doctrina marítima de la OTAN en 2021. En este caso, la aproximación es *bottom up* desde el nivel táctico y en España se ha implementado exclusivamente para la fuerza naval a través de la doctrina aliada y su reflejo en la PDC-3.1. IW consiste en proteger y explotar el entorno de la información mediante la aplicación de esfuerzos, de naturaleza ofensiva para influir y generar efectos y de naturaleza defensiva para asegurar la información. En otras palabras, IW es una disciplina que permite «operacionalizar» el ámbito cognitivo en el nivel táctico mediante el empleo de capacidades relaciona-

das con la información. Para ello, el concepto IW se apoya en tres pilares doctrinales: el conocimiento del espacio de las operaciones, el mando y control asegurado y la integración conjunta.

En este sentido, existe un vínculo indisoluble entre la información y el espectro electromagnético. Debido al carácter global del entorno de la información, con tasas masivas de accesibilidad y conectividad mundial, prácticamente toda la información hoy en día se transmite a través del espectro. Por ello, el acceso ininterrumpido al mismo es un requisito irrenunciable para poder alcanzar la superioridad en la información, aspecto que demuestra la complementariedad conceptual entre EMO e IW. Asimismo, las prospectivas a largo plazo deparan escenarios todavía más demandantes, con el dato erigido como activo estratégico, y en donde EMO e IW serán previsiblemente conceptos críticos.

En dicha visión prospectiva, la integración en el multidominio destaca como uno de los principales retos en el empleo de la FC. El éxito de las MDO se basa en la superioridad en la información y se articula a partir de la transformación digital. Y al ser la conectividad una de sus características definitorias, el acceso continuo al espectro electromagnético se convierte un requisito crítico para las MDO. Asimismo, la integración de capacidades y de nuevos ámbitos que caracteriza las MDO está muy alineada con la necesaria sinergia de los conceptos EMO e IW.

Con la aproximación sistémica planteada, se ha podido demostrar que los conceptos EMO e IW son complementarios y sinérgicos entre sí. Por una parte, los aspectos diferenciadores completan la perspectiva individual de cada concepto y, por otra, el efecto del sistema como un todo es superior a la suma de los efectos individuales. No obstante, la aplicación del marco teórico ha permitido identificar hasta seis aspectos de conflicto entre EMO e IW: coordinación e integración de operaciones en el ciberespacio, coordinación de actividades ISR incluyendo SIGINT, coordinación del apoyo espacial, coordinación e integración NAVWAR, coordinación e integración de acciones EW, y gestión del espectro. Todos ellos son duplicidades en los flujos o procesos de trabajo y deben ser resueltas para aumentar la sincronización del sistema.

En paralelo, y al aplicar el marco teórico, se han identificado dos hechos que evidencian falta de sincronización en el sistema estudiado. El primero está relacionado con la ausencia, a nivel operacional y de mandos componentes, de un lenguaje estandarizado sobre cómo alcanzar la superioridad en la información. La

aplicación del concepto IW, exclusivamente a la fuerza naval, es la causa raíz de este problema. El segundo está vinculado a la función conjunta de información y a la ausencia de un catálogo integral de actividades o capacidades sobre el que esta función se pueda proyectar. No haber incorporado las últimas tendencias doctrinales al desarrollo conceptual de esta función conjunta se considera su causa raíz. Como establece el marco teórico, se le generará un importante beneficio al sistema analizado una vez se eliminen o mitiguen ambas causas.

Por último, se han analizado diversos órganos multifuncionales y multidisciplinares (COEM, sección J9, célula de influencia, JTCB/JTWG, IACB/IAWG, JCMB/JCMWG y JIC) a disposición del comandante operacional para apoyarle en el ciclo de la decisión y afrontar la conducción de las operaciones militares. Se concluye que todos ellos aportan sinergias, eliminan los aspectos de conflicto EMO-IW, aumentan la sincronización del sistema y, por tanto, incrementan el valor que este genera. En otras palabras, todos ellos son aplicables como herramientas de coordinación y sincronización del nivel operacional a los conceptos EMO e IW y, por tanto, mejoran la contribución del sistema para alcanzar la superioridad en el espacio de las operaciones.

A pesar de todo lo anterior, se han identificado cuatro actividades EMO-IW que actualmente no están coordinadas, integradas y sincronizadas a nivel operacional en el sistema: criptología, meteorología y oceanografía, *information management* y la explotación de las debilidades ISR del adversario. En cualquier caso, y atendiendo al criterio de que estas cuatro actividades están relacionadas con la información y el espectro electromagnético, existe margen para que sean incorporadas a los cometidos del COEM como nodo de coordinación.

Como síntesis final se puede afirmar que los conceptos EMO e IW son complementarios y sinérgicos a nivel operacional en las FAS españolas. No obstante, y para que esto se cumpla en toda circunstancia, es necesario eliminar los aspectos de conflicto EMO-IW mediante la aplicación de las herramientas operacionales de coordinación y sincronización que se han analizado.

Bibliografía

Aeschbach, K. (2022). IW Capabilities, Cyber Mission Force and the Future of IW Training. *CHIPS Magazine*. [Consulta: 2025].

- Disponible en: <https://www.doncio.navy.mil/CHIPS/Article-Details.aspx?ID=15759>
- Birrell, M. (2023). Sincronización y sinergia empresarial. Gestión sistémica con la teoría de las restricciones. Marge Books.
- Braswell, B. (2017). Evolving the Information Warfare Commander. *CHIPS Magazine*. [Consulta: 2025]. Disponible en: <https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=9422>
- Cartelle, J. A. y Torres, A. (2019). Quince años del Mando de Operaciones. *Revista General de Marina*. Madrid, Ministerio de Defensa. 277, pp. 773-783. ISSN 0034-9569.
- Centro Conjunto de Desarrollo de Conceptos. (2023). PTP 2022-2024, Tecnologías emergentes y disruptivas (EDT) de mayor interés/aplicación a nivel nacional (BITD). Ministerio de Defensa.
- Conner, F. (2023). NATO's Maritime Information Warfare Commander', Cutting the bow wave. Cutting the Bow Wave 2023. Norfolk, CJOE COE, pp. 30-33. [Consulta: 2025]. Disponible en: <https://www.cjoscoe.org/publications>
- García, F. (2023). El targeting de las operaciones I+I: el targeting estratégico. Cuadernos de pensamiento naval. Madrid, Ministerio de Defensa. 34, pp. 11-28. [Consulta: 2025]. Disponible en: <https://armada.defensa.gob.es/archivo/mardigitalrevistas/boletinpensamiento/2023/2023cpn34.pdf>
- Garret, P. (2023). Maneuver Warfare Is Not Dead, But It Must Evolve. *Proceedings*. U. S. Naval Institute. 149(11). [Consulta: 2025]. Disponible en: <https://www.usni.org/magazines/proceedings/2023/november/maneuver-warfare-not-dead-it-must-evolve>
- Kallenborn, Z. (2023). Perspective: time for a commission on information warfare. *Small Wars Journal*. Arizona State University, p. 3. [Consulta: 2025]. Disponible en: <https://smallwarsjournal.com/jrnl/art/perspective-time-commission-information-warfare>
- Kirschbaum, J. B. (2021). *Information Environment. DOD Operations Need Enhanced Leadership and Integration of Capabilities*. Washington DC, United States Government Accountability Office. [Consulta: 2025]. Disponible en: <https://www.gao.gov/assets/720/714091.pdf>
- Lalinde, L. (2024). Entrevista del autor a la actual jefa del COEM.
- López, T. E. (2021). Instrucción 55/2021. *Boletín Oficial del Ministerio de Defensa*. Madrid, Ministerio de Defensa. [Con-

sulta: 2025]. Disponible en: https://emad.defensa.gob.es/Galerias/emad/files/BOD_20211103_214.pdf

Martínez, J. (2022). Operaciones electromagnéticas: deshaciendo el nudo gordiano del multidominio. *Documento de Opinión*. Madrid, Ministerio de Defensa: Instituto Español de Estudios Estratégicos. 22, p. 8-12. [Consulta:2025]. Disponible en: https://www.ieee.es/Galerias/fichero/docs/opinion/2022/DIEEO22_2022_JUAMAR_Operaciones.pdf

Medina, Luis de. (2020). No perder el norte: un año entre el Báltico y los fiordos noruegos. *Revista General de Marina*. Madrid, Ministerio de Defensa: Armada española. 278(2), pp. 323-332. [Consulta: 2025]. Disponible en: <https://armada.defensa.gob.es/archivo/rgm/2020/03/rgmmarz20cap10.pdf>

Millán, J. M. (2022). Operaciones en el ciberespacio: ¿esas desconocidas? *Ejército*. 979, pp. 34.43. [Consulta: 2025]. Disponible en: https://www.defensa.gob.es/cectic/Galerias/ficheros/2022_11_12_OPERACIONES_EN_EL_CIBERESPACIO_ESAS_DESCONOCIDAS.pdf

Ministerio de Defensa. (2018). *Doctrina para el empleo de las FAS: PDC-01 (A)*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2019). *Doctrina de targeting conjunto: PDC-3.9 (A)*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2020a). *Concepto exploratorio del ámbito cognitivo*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2020b). *Doctrina del JISR: PDC-2.7*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2021a). *Concepto básico de operaciones electromagnéticas conjuntas*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2021b). *Doctrina de Comunicación Estratégica: PDC-10*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2021c). *Doctrina de operaciones: PDC-3*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2021d). *Doctrina de operaciones en el ámbito ciberespacial: PDC-3.20*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2021e). *Glosario de uso conjunto: PDC-00*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2022a). *Doctrina de operaciones en el ámbito aeroespacial: PDC-3.3*. Madrid, Ministerio de Defensa.

Ministerio de Defensa. (2022b). *Doctrina de operaciones en el ámbito marítimo: PDC-3.1*. Madrid, Ministerio de Defensa.

- Ministerio de Defensa. (2023). *Doctrina de operaciones en el ámbito terrestre: PDC-3.2*. Madrid, Ministerio de Defensa.
- NATO. (2016). *Allied Joint Doctrine for Air and Space Operations. AJP-3.3 (Edition B, Version 1)*. NATO Standardization Office. [Consulta: 2025]. Disponible en: <https://nso.nato.int/nso/nsdd/main/standards?search=ajp-3.3>
- NATO. (2020). *Allied Joint Doctrine for Electronic Warfare. AJP-3.6 (Edition Version NATO Standardization Office)*. <https://nso.nato.int/nso/nsdd/main/standards?search=ajp-3.6>
- NATO. (2021). *NAVWAR playbook*. NATO Standardization Office.
- NATO. (2023a). *Allied Joint Doctrine for Information Operations. AJP-10.1 (Edition A, Version, 1)*. NATO Standardization Office. [Consulta: 2025]. Disponible en: <https://nso.nato.int/nso/nsdd/main/standards?search=ajp-10.1>
- NATO. (2023b). *Allied Joint Doctrine for Strategic Communications. AJP-10 (Edition A, Version 1)*. NATO Standardization Office. [Consulta: 2025]. Disponible en: <https://nso.nato.int/nso/nsdd/main/standards?search=ajp-10>
- NATO. (2024). *Term Database*. NATO Standardization Office.
- Nieto, I. (2021a). La capacidad de disuasión estratégica de las operaciones electromagnéticas. *Documento Marco (04/2021)*. Instituto Español de Estudios Estratégicos, p. 23. [Consulta: 2025]. Disponible en: http://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM04_2021_IGNNIE_Operaciones.pdf
- Nieto, I. (2021b). The tool of revisionist countries to confront the international order. *Transforming Joint Air and Space Power. The Journal of the JAPCC*. 31, p. 6. [Consulta: 2025]. Disponible en: <https://www.japcc.org/articles/electromagnetic-operations-in-grey-zone-conflicts/>
- Nieto, I. (2022). La necesidad de contar con un Centro de Operaciones Electromagnéticas en las Fuerzas Armadas españolas. *Global Strategy Report*. Universidad de Granada. 1. [Consulta: 2025]. Disponible en: <https://global-strategy.org/la-necesidad-de-contar-con-un-centro-de-operaciones-electromagneticas-en-las-fuerzas-armadas-espanolas/>
- Ros, J. (2024). Entrevista del autor al oficial que participa en el desarrollo doctrinal de IW para la Armada, y la representa en los foros doctrinales de la OTAN en esta materia.

- Scott, S. (2021). Keeping warfare down to Earth. Can we still operate in a satellite denied environment? *Cutting the Bow Wave 2021*. Norfolk, CJOE COE, pp. 53-57.
- Sierra, J. F. (2024). Entrevista del autor al actual jefe de la sección J9 del MOPS.
- Theohary, C. A. (2018). Information warfare. Issues for Congress. *Congressional Research Service*, p. 19. [Consulta: 2025]. Disponible en: <https://sgp.fas.org/crs/natsec/R45142.pdf>
- Trussler, J. (2019). Adm. Trussler: Information Warfare 'All About Speed for Advantage'. *Sea Power*. [Consulta: 2025]. Disponible en: <https://seapowermagazine.org/adm-trussler-information-warfare-all-about-speed-for-advantage/?print=pdf>
- Waggoner, R. (2019). Basics of space support to NATO operations. *Cutting the Bow Wave*. Norfolk, CJOE COE, pp. 45-47. [Consulta: 2025]. Disponible en: <https://www.cjoscoe.org/publications>
- White, T.; Barrett, D. y Bebbler, R. (2019). The future of information combat power: winning the information war. Center for International Maritime Security. [Consulta: 2025]. Disponible en: <https://cimsec.org/the-future-of-information-combat-power-winning-the-information-war/>