

Capítulo sexto

El mando y control de la guerra electrónica en el nivel operativo

José Luis Rodríguez Méndez

Resumen

El modo en el que normalmente han operado las Fuerzas Armadas se ha fundamentado en una premisa hasta ahora indiscutible: la garantía de la disponibilidad de acceso al espectro electromagnético. El desarrollo extraordinario de la tecnología está conformando el escenario de los futuros conflictos, la superioridad tecnológica de uno de los contendientes ya no será un factor determinante para garantizar el éxito en un hipotético enfrentamiento. El empleo de estrategias de denegación de área o de antiacceso (A2/AD) de un adversario pueden resultar suficientes para frenar las capacidades operativas tradicionales de una fuerza militar hasta el punto de hacerlas ineficaces en determinados entornos.

En el caso del entorno electromagnético, las nuevas tecnologías han permitido el desarrollo de sistemas de uso militar y civil que utilizan el espectro electromagnético como medio donde desarrollar su actividad. Son tecnologías de fácil acceso y relativamente económicas que han provocado que el uso del espectro sea cada vez más un entorno saturado y por ende disputado.

En este contexto, disponer de la adecuada información del entorno electromagnético que permita a un comandante y a su

elemento asesor alcanzar una mejor comprensión de la situación será primordial. La guerra electrónica jugará un papel clave para el éxito de las operaciones militares pues, quien logre el dominio del espectro conseguirá una ventaja fundamental que determinará el éxito o el fracaso de la misión.

Palabras clave

Guerra electrónica, operaciones electromagnéticas, mando y control de guerra electrónica.

Command and control of electronic warfare in the operational level

Abstract

The way the Armed Forces normally performed its actions has been based on an undisputed premise: the granted access to the electromagnetic spectrum. The extraordinary development of technology is shaping the scenario of future conflicts, the technological superiority of one of the contenders will no longer be a determining factor for the success during an hypothetical engagement. The employment of A2/AD strategies could be enough to curb a force's traditional combat capabilities to the point of making them ineffective or useless in certain environments.

This is the case of the electromagnetic environment, new technologies have enabled the development of new systems that depend on the electromagnetic spectrum for their performance. They are easily available and relatively inexpensive provoking the access and use of spectrum to become increasingly disputed and congested.

In this context, to get the adequate information from the electromagnetic environment will be paramount to allow the commander and his staff to achieve a better understanding of the operational situation. The electronic warfare will play a key role in the success of military operations, whoever achieves spectrum dominance will gain a fundamental advantage that will be decisive for the mission's success or failure.

Keywords

Electronic warfare, electromagnetic operations, electronic warfare command and control.

Introducción

En febrero de 1904 estalla la guerra de Tsushima entre Rusia y Japón, iniciada por este último mediante un ataque por sorpresa contra buques de guerra rusos. Para la coordinación de sus acciones, la armada nipona empleaba sencillos equipos de radio que operaban en frecuencia fija, lo que fue aprovechado por los rusos para prevenirse de sus ataques mediante la interceptación de sus comunicaciones¹. Estas acciones podemos considerarlas como las precursoras de la guerra electrónica actual en apoyo a las operaciones.

Desde entonces hasta ahora, la aparición de nuevas tecnologías y su aplicación al ámbito militar es de gran interés, especialmente de la guerra electrónica, acuñándose internacionalmente el término de «revolución de las tecnologías de la información en los asuntos militares» (IT-RMA)² en clara referencia a los cambios producidos por las nuevas tecnologías en el modo de empleo de la fuerza militar.

Hoy en día las nuevas tecnologías contribuyen al aumento en la velocidad de procesamiento, lo que unido a las posibilidades que ofrece la inteligencia artificial (AI) y el *Machine Learning* (ML) para el manejo de grandes volúmenes de datos y de información en apoyo a la toma de decisiones y al control de las actividades de la fuerza, implicará una adaptación de las organizaciones operativas, de sus doctrinas de empleo y del personal especializado en guerra electrónica, así como de los procesos utilizados³.

La información será por tanto el factor clave⁴ a tener en cuenta para alcanzar el éxito de las operaciones; la gestión eficaz de la misma se considerará fundamental en el futuro entorno de las

¹ De Arcangelis, M. (1983). *Historia de la guerra electrónica. Desde la batalla de Tsushima al Líbano y las Malvinas*. Madrid, Editorial San Martín.

² IT-RMA (en inglés). Information Technology Revolution in Military Affairs. El término está basado en la irrupción de numerosos avances tecnológicos que están transformando los conceptos, doctrinas y las organizaciones militares, haciendo que los procesos de innovación formen parte intrínseca en casi todos los asuntos militares. (Dombrowski & Ross, 2008).

³ Dombrowski, P. y Ross, A. (2008). The Revolution in Military Affairs. Transformation and the Defence Industry. *Security Challenges*. [Consulta: 15/3/2021]. Disponible en: <https://www.jstor.com/stable/26459804>

⁴ Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa. El Ministerio de Defensa en su Política CIS/TIC declara «la información como recurso estratégico sustentado por las TIC».

operaciones donde la incertidumbre y el caos serán sus elementos definitorios.

Con este trabajo se pretende resaltar la importancia que tiene la guerra electrónica (GE/EW⁵) para ejercer el control del espectro electromagnético en apoyo a las operaciones militares, concluyéndose la necesidad de adaptación o transformación de los actuales sistemas de mando y control para adecuarse a los requerimientos del previsible escenario de actuación de la Fuerza Conjunta en el entorno operativo 2035.

En este sentido, la Directiva de política de defensa señala entre sus directrices principales, que «el Ministerio de Defensa y las Fuerzas Armadas deben potenciar las capacidades y fortalezas propias, que permiten contribuir a una seguridad nacional concebida como un todo integrador, que atiende a misiones permanentes en los espacios de soberanía e interés» para la defensa⁶.

Las FAS dependen cada vez más del entorno electromagnético para llevar a cabo sus operaciones, convirtiéndose por derecho propio en un nuevo espacio de confrontación y requiriendo un alto grado de coordinación y control para una oportuna y acertada ejecución de las mismas. En el ámbito de las operaciones electromagnéticas, disponer de la necesaria capacidad de mando y control será un requisito imprescindible para lograr el éxito de las mismas⁷.

Como lección identificada por nuestras Fuerzas Armadas adquirida de la experiencia durante sus despliegues en operaciones, se deriva un interés creciente por las capacidades de protección electromagnética⁸ propia, así como por la potenciación de las

⁵ En este texto se emplearán indistintamente los términos GE (guerra electrónica) y EW (*Electrónica Warfare*) al ser de uso generalizado en el ámbito doctrinal de nuestras Fuerzas Armadas.

⁶ MINISDEF. (2020). Directiva de política de defensa 2020. *Boletín Oficial de Defensa* n.º 159 de 6 de agosto de 2020. Disponible en: <https://publicaciones.defensa.gob.es/bod-acceso-libre-21641.html>

⁷ MINISDEF. Entorno operativo 2035. [Consulta: 7/12/2020]. Disponible en: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2019/entorno_operativo_2035.pdf

⁸ Conjunto de acciones, activas o pasivas, utilizadas por una fuerza militar durante la ejecución de las operaciones y que tienen como objetivo la seguridad del personal y de los materiales mediante el uso de la energía electromagnética. Un claro ejemplo de esto último son los equipos de perturbación contra explosivos improvisados accionados por radiofrecuencia conocidos como Remote Controlled – Improvised Explosives Devices (RC-IED).

de apoyo electrónico⁹ que permitan la búsqueda, interceptación, identificación y localización de emisores hostiles o enemigos. Por otro lado, es notable el esfuerzo por dotarse de nuevas capacidades de guerra electrónica y la adopción de nuevos procedimientos y doctrinas que están experimentando las fuerzas armadas de nuestro entorno.

Especialmente reseñable es la transformación que están llevando a cabo en este ámbito las Fuerzas Armadas de los Estados Unidos. El Departamento de Defensa de los EE. UU. (DoD)¹⁰ se encuentra actualmente en un periodo de transformación desde el concepto tradicional de la guerra electrónica como conjunto de actividades separadas de la gestión del espectro electromagnético, hacia un enfoque integrador denominado operaciones en el espectro electromagnético (EMO)¹¹, mediante la unificación en una única «estrategia de superioridad en el espectro electromagnético» tanto la dedicada al espectro electromagnético como a la enfocada a la guerra electrónica¹², las cuales habían sido hasta el momento estrategias separadas.

Mando y control de las operaciones militares

Uno de los primeros problemas con el que nos encontramos al hablar de *mando y control* será la adecuada delimitación de este concepto. La búsqueda de una definición que le caracterice suficientemente no es una tarea fácil, dada la multitud de definiciones ofrecidas por la doctrina y publicaciones de todo tipo que tratan sobre este tema.

En primer lugar, encontraremos que el concepto de mando y control se puede definir de acuerdo al papel que desempeña dentro del ámbito de las Fuerzas Armadas, distinguiéndose por un lado como *función mando y control*, y por otro lado como *sistema de mando y control*.

⁹ Medidas de apoyo electrónico, utilizan la actividad del adversario en el entorno electromagnético para obtener información proveniente de las emisiones y señales del adversario.

¹⁰ DoD (en inglés). *Department of Defense*.

¹¹ EMO (en inglés). *Electromagnetic Operations*.

¹² Department of Defense. (Octubre de 2020). US Electromagnetic Spectrum Superiority Strategy. [Consulta 3/5/2021]. Disponible en: https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF

Como función, la doctrina conjunta de las FAS, establece la función mando y control como una función conjunta, y la define como:

«[...] el ejercicio de la autoridad y dirección, por un mando específicamente designado para ello, sobre las fuerzas que le han sido asignadas para el cumplimiento de la misión», y se realiza mediante «conjuntos de elementos interrelacionados que desarrollan las acciones necesarias para proporcionar al mando, en tiempo útil, el conocimiento de la situación, constituyendo el soporte necesario para la toma de decisiones, la transmisión de órdenes y el control de su ejecución¹³».

El conjunto de personal, medios y procedimientos dedicados a proporcionar al mando el necesario conocimiento de la situación que ayude a la toma de decisiones, convertirlas en órdenes y transmitirlos a aquellos elementos encargados de su ejecución facilitando el control de lo ejecutado, constituye lo que se denomina *sistema de mando y control (C2S)*. La función mando y control es ejercida, sin embargo, por el comandante o jefe designado para una operación, así como por su elemento de apoyo (su estado mayor o plana mayor). El mando, por tanto, se refiere al ejercicio de la autoridad y a la toma de decisiones por parte del jefe o comandante, mientras que el control está referido a la coordinación y supervisión de la ejecución de las actividades de una fuerza o unidad.

Para una mejor comprensión haremos referencia a la doctrina OTAN que en su publicación conjunta define el mando y control de la siguiente forma:

- El mando es la autoridad con la que es investida un militar o fuerza armada para dirigir, coordinar y controlar fuerzas militares. Mediante la dirección se definen los objetivos, las acciones a ejecutar y los recursos a emplear para alcanzar dichos objetivos. Mediante la coordinación se armonizarán y guiarán las fuerzas asignadas para alcanzar los objetivos asignados.
- El control se define, como la autoridad que es ejercida por un comandante sobre las actividades desarrolladas por organizaciones directamente subordinadas o no y que lleva implícita la responsabilidad de implementar órdenes o directivas. Mediante el control se verifican las acciones que se están ejecutando

¹³ MINISDEF. (2018). *PDC-01 (A). Doctrina para el empleo de las FAS*.

y su efectividad en relación con la intención y objetivos establecidos para la fuerza.

Con lo expresado hasta ahora, se puede concluir que el mando y control tiene dos componentes claramente diferenciadas: el ejercicio de la autoridad, y la conducción¹⁴ de las operaciones. Mediante el mando se definen las acciones y objetivos a alcanzar y, mediante el control se supervisará su ejecución en relación con dichos objetivos.

Una vez acotado el mando y control como una función, pasaremos a contextualizarlo desde el enfoque de la teoría de sistemas, para lo cual se utilizará la doctrina del ejército norteamericano sobre el mando orientado a la misión o *mission command*, que define el sistema de mando y control como «la organización de personal, manejo de información, procedimientos, equipamiento y estructuras esenciales para que el comandante conduzca las operaciones»¹⁵.

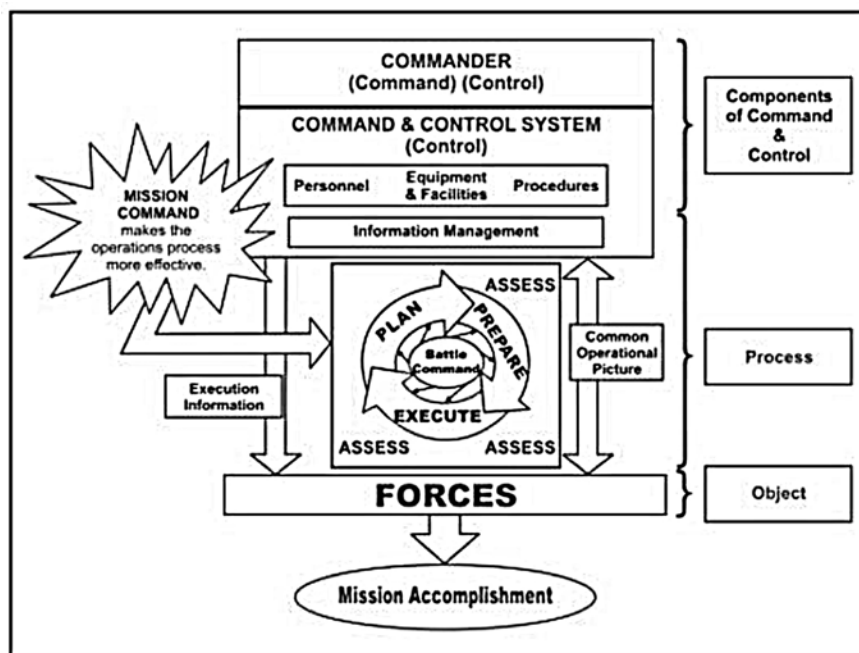


Figura 1. Mando y control (fuente: US Army)

¹⁴ La PDC-01 (A) define conducción como el «proceso por el que se dirigen, coordinan y controlan las acciones en una operación militar. Tiene una componente de dirección donde se toman las decisiones, otra de coordinación de la secuencia de acciones y una última componente de control para la supervisión del desarrollo de la decisión».

¹⁵ US Army. (2003). *FM 6-0, Mission Command: Command and Control of Army Forces*.

Por tanto, la relación que se puede establecer entre ambos conceptos es, que el sistema de mando y control (C2S) es la herramienta que utilizará un comandante y su estado mayor para la conducción de las operaciones, facilitando de esta manera el conjunto de actividades que forman parte de la función mando y control.

El comandante forma parte, por consiguiente, tanto del proceso de toma de decisiones para la conducción de las operaciones, como del propio sistema de mando y control, por lo que ambos, función y sistema, estarán orientados a facilitar el cumplimiento de la misión asignada.

Como se ha establecido anteriormente, el mando y control se compone de dos partes, el ejercicio de la autoridad y la conducción de operaciones. Para determinar quién tiene atribuida la conducción de operaciones en las FAS españolas, se volverá nuevamente a la PDC-01 (A). En esta publicación, se determinan tres niveles de conducción: el nivel estratégico, el nivel operacional y el nivel táctico. Es en el nivel operacional donde se planean, conducen y sostienen las campañas y las operaciones militares. Además, su situación intermedia entre el nivel estratégico y el táctico, lo convierte en pieza y elemento clave para la dirección y coordinación de las operaciones, o lo que es lo mismo, da sentido a las acciones que se ejecutan sobre el terreno y que ayudan a alcanzar la situación final deseada definida en el nivel estratégico.

Un sistema de mando y control contribuirá fundamentalmente a apoyar el proceso de decisión (ciclo de decisión¹⁶), facilitando la realización de los siguientes procesos:

1. Obtener información (observar).
2. Procesar, analizar, sintetizar, presentar y difundir la información obtenida (orientar).
3. Facilitar el planeamiento y el proceso de toma de decisiones (decidir).
4. Transmitir las órdenes y directrices del comandante (actuar).
5. Permitir el control de la ejecución de las operaciones mediante los nuevos datos que vayan apareciendo, empezando de esta manera un nuevo ciclo (verificar).

¹⁶ Este ciclo así definido fue identificado por el coronel John Boyd en su teoría del «OODA Loop».

En primer lugar, resaltar el papel clave de la información durante el proceso de toma de decisiones de un comandante, llegando a ser un factor diferencial para el éxito o el fracaso de la misión. Del procesado, análisis, síntesis, presentación y difusión de la información surge la necesidad de su gestión y administración adecuadas, lo que nos lleva a concluir en la necesidad de disponer de un sistema de información para llevar a cabo el proceso de recogida, procesado, almacenamiento y entrega de datos, que en su conjunto constituirán los elementos definitorios de dicha información. Mediante la realización de estas tareas se termina cerrando el ciclo que volverá a iniciarse nuevamente con la información resultante de la actividad que se ha ejecutado u otra información de interés que pueda surgir durante la fase o proceso de observación.

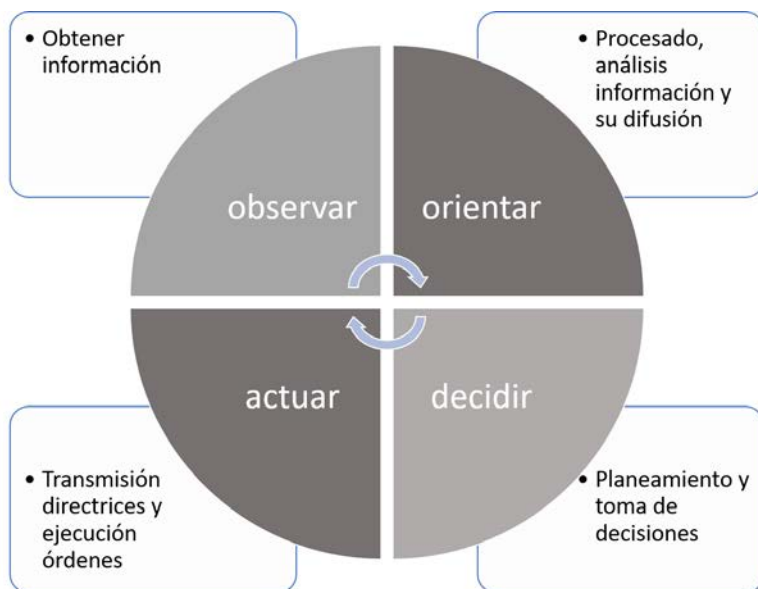


Figura 2. Teoría del OODA Loop. (Fuente: elaboración propia)

El coronel John Boyd estableció en su teoría del OODA loop que para obtener una ventaja significativa sobre un adversario habría que tomar decisiones de la forma más rápida y eficaz posible, de tal forma que se lograría superioridad sobre el adversario cuando nuestro ciclo de decisión fuese más rápido que el suyo. Por lo tanto, se requerirá obtener un conocimiento de la situación adaptado al ritmo, cada vez mayor, de toma de decisiones, lo que inexorablemente nos llevará al empleo de sistemas de información y herramientas de apoyo para facilitar

este proceso. Las nuevas tecnologías son sin duda el mejor aliado para llevar a cabo el proceso anterior, facilitando las tareas de observación y orientación con la necesaria celeridad, ayudando a la toma rápida de decisiones y, por último, al control de las actividades ejecutadas como parte del proceso que completaría el ciclo.

En este sentido, los sistemas de información para el mando y control de guerra electrónica en el ámbito de las operaciones militares ayudarán a obtener la ventaja necesaria para alcanzar una adecuada comprensión de la situación (SA)¹⁷ que facilite la toma de decisiones y la coordinación de las actividades en el espectro electromagnético¹⁸.

Adicionalmente, se implementarán las adecuadas estructuras en los diferentes cuarteles generales y puestos de mando, tales como elementos y células específicas de guerra electrónica que orienten la toma de decisiones y verifiquen los efectos de las acciones de GE que se hayan decidido durante el proceso de planeamiento.

Por último, en el ámbito de la Alianza Atlántica se están llevando a cabo diversos desarrollos que han dado como resultado la introducción de conceptos novedosos en relación al mando y control, mejorando la eficacia de los sistemas gracias a la integración de capacidades de GE en red. Como ejemplo de ello se destaca el concepto NNEC¹⁹²⁰. En aplicación de este concepto se están desarrollando sistemas que permitirán el flujo y el intercambio de información, mediante la integración en red de sensores, vectores de armas y sistemas C2, mejorando con ello los procesos de obtención en apoyo a la toma de decisiones.

Llegados a este punto parece adecuado concluir que sería recomendable disponer de un sistema de mando y control en cualquier nivel de conducción de las operaciones, desde el estratégico al táctico.

¹⁷ SA (en inglés). *Situational Awareness*.

¹⁸ Bamford, E. y Von Spreckelsen, M. (2019). Future Command and Control of Electronic Warfare. *The Journal of the JAPCC*, 28, pp. 60-66. [Consulta: septiembre 2020]. Disponible en: <https://www.japcc.org/future-command-and-control-of-electronic-warfare>

¹⁹ NATO Military Committee. (2007). *MCM-0142-2007, Military Committee Transformation Concept for Future NATO Electronic Warfare*.

²⁰ NNEC (en inglés). *NATO Network Enabled Capabilities*

Operaciones electromagnéticas. Un concepto en continua evolución

Las operaciones electromagnéticas hicieron su aparición en sendas cumbres de la OTAN en Praga (2002) y Riga (2006) en las que las naciones aliadas llegaron a un acuerdo sobre el nuevo concepto de transformación de la futura guerra electrónica²¹. Este documento tiene la intención de preparar la «transición» de las naciones y ejércitos aliados desde el concepto tradicional de empleo de la fuerza hacia el nuevo concepto de operaciones basadas en efectos²². A partir de entonces «el concepto de la guerra electrónica se encuentra en permanente evolución»²³.

Esta transformación de la guerra electrónica tiene su acomodo dentro del concepto de operaciones electromagnéticas (OEM), en el que además encuentran su sitio otras dos disciplinas más: la gestión del espectro (SM)²⁴ y la inteligencia de señales (SIGINT)²⁵. La conjunción de estas tres capacidades permitirá el acceso y la maniobra electromagnética propia a la vez que se dificultará el acceso y la maniobra al adversario.

Las operaciones electromagnéticas, son aquellas mediante las cuáles las fuerzas propias y/o amigas utilizan la energía electromagnética en su beneficio, mientras que el adversario lo utiliza para amenazar las operaciones propias. Esta amenaza se verá agravada por el crecimiento exponencial del uso civil del espectro electromagnético debido al abaratamiento de costes de las tecnologías de origen comercial o COTS²⁶ de acceso libre, provocando limitaciones y restricciones al uso del mismo por parte de todos los actores involucrados en un teatro o zona de operaciones.

Un entorno electromagnético (EME)²⁷ saturado y competido dificultará el empleo eficaz de las capacidades militares desplegadas, y por ende el mando y control de las operaciones militares

²¹ OTAN. (Noviembre de 2007). *MCM-0142-2007, Military Committee Transformation Concept for Future NATO Electronic Warfare*.

²² OTAN. (2018). *MC 0064/11, Nato Electronic Warfare Policy*.

²³ Nieto, I. (2021). *La capacidad de disuasión estratégica de las operaciones electromagnéticas*. Documento Marco 04. Madrid, IEEE.

²⁴ SM (en inglés). *Spectrum Management*.

²⁵ SIGINT es el acrónimo que hace referencia a las actividades de inteligencia de señales.

²⁶ COTS (en inglés). *Commercial Off-The Shelf*. Tecnología disponible para uso civil no sujeta a estándares militares.

²⁷ EME (en inglés). *Electromagnetic Environment*.

que tendrán que hacer frente al análisis de datos procedentes de multitud de emisores, militares y civiles, debiendo ser gestionados de forma ágil y eficiente, de tal forma que se facilite tanto el ejercicio del mando como el control de las acciones de guerra electrónica (EW)²⁸.

La guerra electrónica como elemento clave de las operaciones electromagnéticas

Las acciones de EW contribuyen a conformar el espacio de batalla o de enfrentamiento mediante el uso deliberado de la energía electromagnética, en un intento de dominar el espectro²⁹.

Podemos definir la guerra electrónica como las acciones llevadas a cabo por una fuerza militar que implican el uso deliberado de la energía electromagnética para controlar el espectro electromagnético a su favor o utilizarlo contra un adversario negándole el acceso al mismo o degradándolo hasta un punto que sea inviable su utilización por sus sistemas de armas o equipamiento. En este punto, es necesario señalar, que la doctrina española de guerra electrónica está basada en la publicación aliada conjunta de guerra electrónica³⁰, que identifica la guerra electrónica como el elemento clave de las operaciones electromagnéticas (EMO³¹).

La guerra electrónica consiste fundamentalmente en la realización de tres grupos de actividades diferenciadas y que son integradas, coordinadas y ejecutadas en beneficio de las operaciones por los componentes de una fuerza militar:

- Ataque electrónico (EA).

Es la rama de la GE que implica el uso deliberado de la energía electromagnética contra sistemas de armas, radares y comunicaciones inalámbricas con la intención de degradar, neutralizar o destruir las capacidades de combate del adversario. Estas acciones se pueden dividir a su vez en ofensivas y defensivas y, por

²⁸ EW (en inglés). *Electronic Warfare*. En este trabajo se empleará el término EW indistintamente con el de GE, por ser de general conocimiento y aplicación en el campo de la defensa y las operaciones militares.

²⁹ Hoehn, J. R. (Septiembre 2021I). Defense Primer: Electronic Warfare. *CRS IN FOCUS*. Disponible en: <https://crsreports.congress.gov/product/pdf/IF/IF11118>

³⁰ OTAN. (2020). *AJP-3.6. Allied Joint Doctrine for Electronic Warfare*. Ed. C, v.1.

³¹ EMO (en inglés). *Electromagnetic operations*.

otro lado, en activas y pasivas dependiendo de si implican la radiación o no de emisiones.

- Protección electrónica (EP).

Las acciones de EP están pensadas para reducir o eliminar los efectos de las acciones de ataque electrónico del adversario sobre los elementos sensores, radares y de radio propios.

- Apoyo electrónico (ES).

Rama de la GE encargada del reconocimiento de la posible amenaza presente en el entorno operativo, mediante la detección, clasificación, almacenamiento, identificación y localización de emisores en la banda de frecuencias. Estos sistemas, son por lo general, elementos pasivos, ya que no emiten radiación.

La guerra electrónica, más allá de su tradicional rol de inteligencia pasiva y de protección de las actividades de la fuerza, así como de ataque mediante acciones de perturbación, ha venido evolucionando en los últimos años hasta convertirse en elemento esencial de las operaciones electromagnéticas (EMO).

Por los motivos que se han enunciado, se puede asegurar, que la guerra electrónica no se limita únicamente al despliegue de sensores y perturbadores, sino que forma parte constituyente de las plataformas y sistemas de armas, y en el caso de los *sistemas de sistemas*, la GE será una función de alto-nivel que formará parte intrínseca del mismo.

Las actividades de guerra electrónica son planeadas en el nivel operacional, ya que sus efectos tendrán incidencia en el logro de los objetivos militares, y son ejecutadas en el nivel táctico. Haciendo un símil con otras capacidades militares podemos encontrar cierto grado de equivalencia con las acciones ejecutadas por unidades o elementos de operaciones especiales, pudiendo afirmarse que «las acciones de guerra electrónica, al igual que las operaciones especiales, se ejecutan en el nivel táctico, pero tienen consecuencias en el nivel operacional o incluso estratégico»³².

³² General de división Joaquín Salas, general jefe de la Jefatura de Sistemas de Información y de Telecomunicaciones y de la Asistencia Técnica del Ejército de Tierra en entrevista concedida al autor el 22/4/2021.

El espectro electromagnético. Nuevo espacio de confrontación

La OTAN ha reconocido al entorno electromagnético como un entorno operativo³³ más donde se llevan a cabo las acciones militares y se producen los efectos necesarios para lograr los objetivos que contribuirán a alcanzar la situación final deseada, y en el que los comandantes de una fuerza militar desplegada deberán conseguir y mantener la superioridad mediante un mando y control efectivo y ágil, el éxito de las operaciones militares dependerá, en gran medida, del empleo eficaz que se haga del espectro.

Este cambio de paradigma viene motivado por tres factores fundamentales. En primer lugar, las operaciones militares son cada vez más complejas y dinámicas. En segundo lugar, los ejércitos aliados están aumentando su actividad en el entorno electromagnético y, al mismo tiempo, están desarrollando nuevas capacidades para influir en el mismo, lo que sin duda alguna llevará a un creciente desafío en su gestión y control, y en último lugar, los potenciales adversarios están invirtiendo de forma significativa en capacidades de guerra electrónica en un intento de alcanzar una posición de ventaja que enfrente la tradicional superioridad tecnológica de la OTAN³⁴.

El espectro electromagnético es un recurso limitado y escaso. Los diferentes estados y gobiernos están implementando políticas tendentes a controlar el acceso al espectro electromagnético de soberanía mediante la gestión eficaz y eficiente de bandas y rangos de frecuencia, basándose principalmente en factores de tipo económico-comercial, debido fundamentalmente al impulso que las nuevas tecnologías están dando a las sociedades modernas (redes wifi, SDR³⁵, 5G, etc.)³⁶.

³³ Los entornos operativos son los tradicionales (terrestre, marítimo y aeroespacial) a los que se suman el entorno cognitivo y de la información.

³⁴ Howard, G. E. y Czekaj, M. (eds.). (2019). *Russia's Military Strategy and Doctrine*. Washington, The Jamestown Foundation.

³⁵ SDR (en inglés). *Software Defined Radio*. Tecnología actual que utiliza modelos de ondas electromagnéticas obtenidos digitalmente mediante programas software de definición espectral, independizando de esta forma la estación o equipo de radiofrecuencia de su plataforma hardware. Este tipo de sistemas digitales de radio es ampliamente utilizado en los equipos de radio comercial como la telefonía móvil, radiotransmisores, telemandos, radiocontrol de drones, entre otros sistemas.

³⁶ Informe UIT-R SM.2012-6 (06/2018) – Aspectos económicos de la gestión del espectro. Apto. 2.1. resalta el interés de las administraciones públicas por los enfoques

En los términos anteriores, se ha referido el Ministerio de Energía, Turismo y Agenda Digital español refiriéndose al espectro radioeléctrico como un «recurso estratégico, valioso y demandado»³⁷ tanto para aplicaciones fijas como, y especialmente, de banda ancha dedicado a la movilidad.

La tecnología es el motor «más determinante del cambio del entorno operativo futuro»³⁸, sin embargo, lo que a priori puede parecer una ventaja puede convertirse en una gran vulnerabilidad sobre todo en ambientes degradados electrónicamente, sin comunicaciones, sin internet, sin información de navegación, etc. Además, a medida que las EMO se vuelven más demandantes, los ejércitos se dotan de nuevas capacidades que sin duda tendrán su impacto en el espacio de batalla³⁹ volviéndose cada vez más dependientes del espectro electromagnético⁴⁰.

El control del espectro electromagnético es, hoy en día, una necesidad si se quiere alcanzar el éxito en las operaciones, ya que estas se han vuelto cada vez más dependientes del mismo, por lo que es necesario garantizar el acceso sin restricciones⁴¹.

Para garantizar la libertad de maniobra en el empleo del espectro electromagnético, los comandantes y sus estados mayores tendrán que llevar a cabo un planeamiento, preparación, ejecución y evaluación de las acciones de GE contra un amplio conjunto de objetivos dentro del espectro electromagnético⁴².

económicos de la gestión del espectro, acorde a los objetivos y metas establecidos por la misma para una «utilización y gestión del espectro eficaz y eficiente».

³⁷ Real Decreto 123/2017, de 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico y el espectro radioeléctrico, publicado en el *Boletín Oficial del Estado* n.º 57 de 8 de marzo de 2017, p. 17029.

³⁸ Ministerio de Defensa. *Entorno operativo 2035*.

³⁹ US. Joint Chiefs of Staff. (Julio 2016). Joint Operating Environment 2035. The Joint Force in a contested and disordered world. US. Joint Force Development. [Consulta: 27/4/2021]. Disponible en https://www.act.nato.int/images/stories/events/2012/fc_ipr/joe-2035.pdf

⁴⁰ Nayak, A. (2009). Strategic Foresight. Costanzo y MacKay (eds.). *Handbook of Research on Strategy and Foresight*. L.A.

⁴¹ Lambert, G. (2016). Electronic Warfare: Rethinking the importance of its role in military operations. National Defense University, JFSC, JAWS. [Consulta: 3/4/2021]. Disponible en: <https://apps.dtic.mil/dtic/tr/fulltext/u2/1010558.pdf>

⁴² Elsworth, A. T. (ed.). (2010). *Electronic Warfare in Operations*. Defense Security and Strategy Series. New York, Nova Science Publishers.

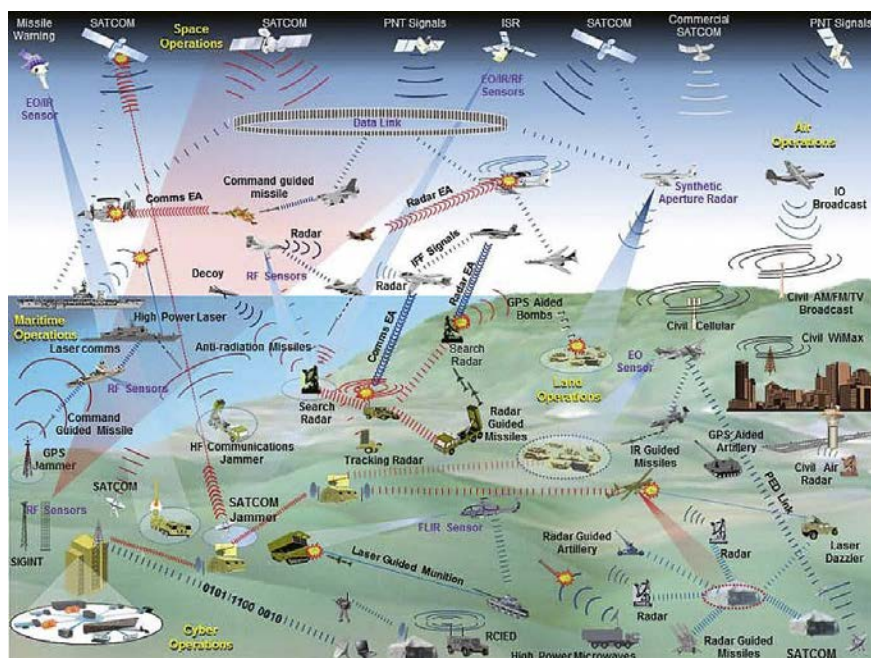


Figura 3. Complejidad del entorno electromagnético. (Fuente: OTAN)

En la doctrina aliada encontramos que los «comandantes deberán disponer, en todos los niveles de conducción de las operaciones, de la necesaria capacidad de GE adecuada a la intensidad y características de la operación»⁴³. Como se ha visto anteriormente, la GE jugará un papel fundamental como parte de las actividades incluidas dentro de las operaciones electromagnéticas (EMO), proporcionando al comandante del nivel operacional los recursos necesarios para poder conformar el entorno electromagnético (EEM) en apoyo a las operaciones⁴⁴.

Pero, las operaciones electromagnéticas no solo consisten en actividades relacionadas con la GE, sino también en varias otras disciplinas que operan en el espectro electromagnético y que son planeadas, coordinadas y controladas dentro de las diferentes áreas funcionales de un cuartel general, entre las cuales se inclu-

⁴³ NATO Military Committee. (2018). MC 0064/11, NATO Electronic Warfare Policy.

⁴⁴ AJP 3.6C párrafo 1.2. Debido a la evolución en la forma en que la OTAN lleva a cabo las operaciones aliadas como a la aparición de nuevas tecnologías, el enfoque de la GE ha pasado de operaciones aisladas en el espectro electromagnético a las operaciones electromagnéticas en el EEM. Las EMO consisten no solo en GE, sino también en varias otras disciplinas que operan en la EEM. La GE es considerada como la disciplina de combate de las EMO.

yen, sin carácter de exclusividad, no solo el control y gestión del espectro sino también otras disciplinas como la guerra de navegación (NAVWAR)⁴⁵, actividades ciber-electromagnéticas (CEMA)⁴⁶, las operaciones de información (IMO)⁴⁷, la vigilancia electrónica (ES), el ataque electrónico (EA), la defensa electrónica (ED) y la inteligencia de señales (SIGINT).

Entre las diversas capacidades, en referencia a sistemas y/o plataformas, que utilizan el EEM nos encontramos con que muchas de ellas se pueden considerar como críticas, dado que implican, no solo un valor añadido a la capacidad de combate de una fuerza, sino que además tienen implicaciones en el resto de capacidades de dicha fuerza.

Entre las capacidades críticas que utilizan el espectro electromagnético podemos citar, a modo de ejemplo, las siguientes:

- NAVWAR, conjunto de acciones dirigidas a obtener la superioridad en el posicionamiento, navegación y señales de tiempo (PNT)⁴⁸. Estas acciones se pueden clasificar en ofensivas, defensivas y de apoyo (Nieto, 2020).
- Early Warning, capacidad de alerta temprana, especialmente diseñado para la lucha contra misiles y la amenaza aérea.
- GNSS⁴⁹, conjunto de tecnologías que utilizan los sistemas de navegación por satélite para proporcionar posicionamiento geoespacial y cobertura global. Como el sistema de posicionamiento global o GPS, de uso extendido hoy en día.
- SATCOM⁵⁰, sistemas de comunicaciones de teatro que proporciona enlaces satélites en zonas de operaciones alejadas. Estos enlaces se clasifican según su capacidad en enlaces de gran, media y baja capacidad.
- Mando y control (C2), puede considerarse como la capacidad transversal a todas las demás que un comandante procurará siempre tener disponible. Se basa en el ejercicio de la autoridad y la dirección de las operaciones, apoyándose

⁴⁵ NAVWAR (en inglés). *Navigation Warfare*. Este concepto es definido por la OTAN en el STANAG 4621 Ed.1, sobre Navigation Warfare Definition, ratificado por España en octubre de 2005.

⁴⁶ CEMA (en inglés). *Cyber Electromagnetic Activities*.

⁴⁷ IMO (en inglés). *Information Operations*.

⁴⁸ PNT (en inglés). *Positioning, Navigation and Timing*.

⁴⁹ GNSS (en inglés). *Global Navigation Satellite System*

⁵⁰ SATCOM (en inglés). *SATellite COMMunication*.

principalmente en el establecimiento de un robusto sistema de comunicaciones e información o CIS.

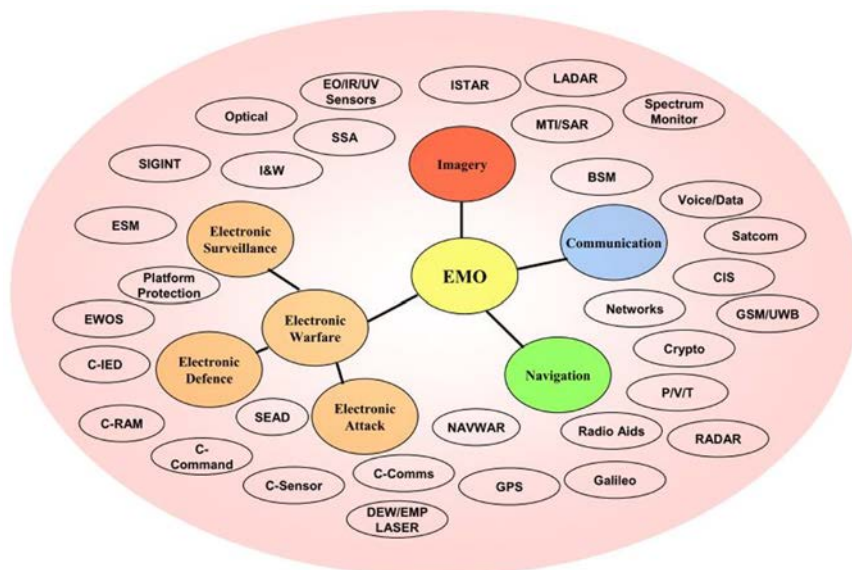


Figura 4. Ámbito de las EMO. (Fuente: NATO)

Será, pues, un requisito, que las organizaciones operativas estén lo suficientemente adiestradas, desde tiempo de paz, en un entorno electromagnético complejo para garantizar que sus capacidades sigan siendo eficaces en caso de guerra o conflicto. En este punto coincide el general Salas cuando declara, en entrevista concedida para la realización de este trabajo, que en los estudios de Fuerza 2035 ya se contempla que nuestras unidades puedan «operar en ambientes electrónicamente degradados».

Además, los medios de GE y SIGINT, «deberían cooperar durante la realización de ejercicios y adiestramiento de las unidades si se pretende proporcionar el apoyo adecuado a las operaciones militares»⁵¹.

En entrevista realizada a los coroneles Sasot y Escusol⁵², ambos convienen en destacar la importancia de la GE y el SIGINT en el futuro entorno operativo, en el que las operaciones en red

⁵¹ NATO Military Committee. (2018). *MC-0064/11. NATO Electronic Warfare Policy*.

⁵² El coronel Fernando Escusol fue el jefe del Regimiento de Guerra Electrónica n.º 31 durante los años 2019 y 2020. El coronel Manuel Sasot es el actual subdirector de actividades en el ciberespacio y electromagnéticas de la Jefatura CIS y AT del Ejército de Tierra.

asegurarán la suficiente coordinación de medios, conocimiento y herramientas necesarias para integrar la GE, ya sea en la misma o diferentes plataformas formando lo que se conoce como un sistema de sistemas.

El C2 y la GE en las Fuerzas Armadas

Una vez definidos y enmarcados los conceptos de mando y control y de operaciones electromagnéticas, así como determinada la importancia que para estas últimas tienen las acciones de guerra electrónica pasaremos a analizar el estado actual de la capacidad de mando y control de las actividades de guerra electrónica.

Si consideramos que el entorno electromagnético se caracteriza por su constante evolución y en continuo cambio, la degradación del mismo puede considerarse como algo normal y no como una excepción. Las perturbaciones sobre sistemas que utilizan servicios de posicionamiento, navegación y tiempo (PNT) y los cibertales a redes y sistemas de comunicaciones tendrán un impacto directo en las operaciones militares.

Estructuras de coordinación de EW

El aumento en la complejidad del entorno operativo, actual y futuro, tendrá como consecuencia inevitable la necesidad de garantizar una mejor coordinación y sincronización de las operaciones electromagnéticas, las cuáles necesitarán de capacidades especializadas que permitan la obtención de información sobre la situación y estado de emisores propios y enemigos. Por consiguiente, el mando y control de las operaciones electromagnéticas se revela como una necesidad.

Durante la conducción de las operaciones se necesita integrar y sincronizar las operaciones de guerra electrónica desde el nivel estratégico hasta el nivel táctico de conducción de las operaciones. En este sentido las operaciones electromagnéticas y especialmente las acciones de GE necesitan ser perfectamente coordinadas e integradas con el resto de actividades de la fuerza desde su planeamiento hasta su ejecución. Para integrar y coordinar dichas operaciones es preciso que todas las áreas funcionales del puesto de mando (operaciones, inteligencia y CIS) trabajen orientadas por un elemento de GE responsable ante el comandante de llevar a cabo dicha coordinación.

En el nivel operacional se necesitará, por tanto, establecer la apropiada estructura para el mando, control y coordinación de las operaciones electromagnéticas. Esta estructura estará dimensionada adecuadamente en función de los requisitos de la misión y del entorno operativo en el que se desarrollen las actividades de la Fuerza Conjunta.

Para concretar qué estructuras se están utilizando en la actualidad en las FAS españolas, hay que hacer referencia a la doctrina OTAN que, en su publicación de nivel conjunto (AJP-3.6), se señalan las siguientes estructuras en el nivel operacional⁵³:

- *Electromagnetic Battle Staff (EMB).*
- *Signal Intelligence and Electronic Warfare Operations Centre (SEWOC).*
- *Electronic Warfare Staff element (EWS).*

Electromagnetic Battle Staff (EMB)

Esta organización no tiene carácter permanente y tampoco una estructura fija predeterminada, será responsabilidad del comandante definir su estructura y composición para el apoyo adecuado a las operaciones.

Sus cometidos, en su composición más completa, abarcaría competencias relacionadas con la GE, la inteligencia de señales (SIGINT) y la gestión del espectro electromagnético (SM). Adicionalmente, podría incluir otros elementos del estado mayor, principalmente del área de operaciones, inteligencia o CIS.

El jefe o director del EMB será, por consiguiente, el responsable de coordinar todas las operaciones en el entorno electromagnético de una fuerza conjunta, así como mantener el necesario conocimiento sobre el entorno electromagnético de actuación.

Centro de operaciones de SIGINT y EW (SEWOC)

El Centro de operaciones de inteligencia de señales y de guerra electrónica se constituye cuando se identifica la necesidad de una estrecha coordinación entre las actividades ESM de las unidades de GE y la obtención de inteligencia de señales.

Normalmente, esto se produce en entornos donde la seguridad se caracteriza por su incertidumbre y complejidad, como es el

⁵³ Para una mejor comprensión se mantienen los términos en inglés, ya que son de uso y conocimiento generalizado en el campo de la guerra electrónica.

caso de los conflictos asimétricos. En estos entornos, disponer de una adecuada conciencia de la situación será clave para la dirección y coordinación de las operaciones militares.

El nivel operacional, en este caso, contribuye mediante la sincronización y coordinación de las actividades en el espectro electromagnético de tal forma que los sistemas y plataformas propios no obstaculicen o impidan el necesario conocimiento de las actividades electromagnéticas del adversario.

Como dato significativo, el SEWOC no contempla dentro de su estructura un elemento de gestión de frecuencias, como sí lo hace el EMB, por lo que, para la necesaria coordinación del espectro, este centro constituirá la base del grupo de trabajo del SEWOC donde tendrán cabida otros elementos del cuartel general o del estado mayor de la Fuerza Conjunta.

Elemento de control y coordinación de guerra electrónica

El oficial de GE de la Fuerza Conjunta, será la base de constitución del elemento de GE. Tendrá bajo su responsabilidad la coordinación de las actividades de GE de sus unidades subordinadas.

Si el tipo de operación y el escenario operativo así lo requiriera, el EW staff podría solicitar al comandante de la Fuerza la constitución de una célula de coordinación de EW (EWCC), esto suele suceder cuando la EW va a tener un papel o rol principal en el desarrollo de las operaciones militares (Lambert, 2016).

Situación actual de la EW en España

Las unidades y medios de guerra electrónica en España pueden dividirse entre medios permanentes de carácter estratégico y medios desplegables. Entre los primeros se destaca por su importancia el programa *Santiago*. Los programas principales que marcan el desarrollo de los sistemas de GE en España son los siguientes⁵⁴ (SOPT, 2009):

Programa *Santiago*

El programa *Santiago* nació en 1986 con el objetivo de dotar a las Fuerzas Armadas de un sistema de obtención y elaboración

⁵⁴ MINISDEF. (Octubre 2009). *La guerra electrónica en España*. Monografía del SOPT. [Consulta: 3/4/2021]. Disponible en: https://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/13/monografia_sopt_2.pdf

SIGINT que complementara las capacidades de que disponían los ejércitos.

Dirigido por el EMAD y coordinado por el Centro de Inteligencia de las FAS (CIFAS), el programa *Santiago* está compuesto por diferentes plataformas divididas en subsistemas dependiendo del tipo y método de recogida de señales:

- Subsistema SCATER (captación señales terrestre).
- Subsistema SCAPA (plataforma aérea).
- Subsistema SCAN (plataforma naval).
- Subsistema SIGLO (integración y evaluación de señales).
- Subsistema HF (SCAHF).
- Subsistema electro-óptico (OPTINT).

Las instalaciones en tierra están integradas dentro del Regimiento de Guerra Electrónica n.º 32, con diversos batallones desplegados en diferentes localizaciones.



Figura 5. Buque «ALERTA» A-111. Subsistema SCAN.
(Fuente: Armada Española)

En la Armada, el Buque Alerta A-111, es la plataforma principal del subsistema SCAN de SIGINT. Aunque no es el único sistema de GE con el que cuenta la Armada ya que casi todos los buques de superficie cuentan con sistemas de GE nacionales como el ALDEBARÁN/RIGEL y REGULUS, además se está trabajando en otros programas de GE para dotar a los nuevos submarinos clase S-80.

En cuanto al subsistema SCAPA sobre plataforma aérea, el EA disponía de un Boeing 707 del 47 Grupo, hoy en día dado de baja para el servicio⁵⁵.



Figura 6. Boeing 707 de guerra electrónica (Fuente: MINISDEF)

Programa «GESTA» y «DUBHE»

Estos programas tienen como objetivo la dotación al Ejército de Tierra (GESTA) y a la Armada (DUBHE) de sistemas completos de guerra electrónica táctica que permitan la captación, interceptación, escucha, localización y perturbación de señales en las bandas de HF, VHF, UHF y SFH⁵⁶.

El sistema realiza las siguientes funciones:

- ESM/ECM de las bandas de telecomunicaciones y radar.
- Evaluación, dirección y control.
- Comunicaciones e integración en SIMACET.

El sistema GESTA se compone de los siguientes subsistemas:

- Un subsistema de EW de telecomunicaciones (ST).
- Un subsistema de EW de no telecomunicaciones (SNT).
- Sistema de evaluación, dirección y control (EDC).
- Subsistema de comunicaciones e información.

El programa DUBHE, dota de capacidades de GE en la banda de telecomunicaciones en apoyo a las unidades de Infantería de Marina⁵⁷.

⁵⁵ Se está estudiando la posibilidad de incluir *Pods* de EW sobre plataformas RPAS capaces de proporcionar información SIGINT y ESM de amplias zonas del TO/ZO.

⁵⁶ Membrillo, A., *et al.* (2017). La guerra electrónica y la ciberdefensa desplegable. *Revista Ejército* 918, pp. 92-96.

⁵⁷ Romero, F. de P. (Mayo 2017). Y de la guerra electrónica. *Revista General de Marina*, mayo 2017, pp. 745-753.

Al igual que el GESTA, el sistema DUBHE se compone de diferentes estaciones ESM de telecomunicaciones, estaciones de dirección y control del subsistema, y de estaciones de ECM de telecomunicaciones integradas en vehículo tipo *piranha*.

Programa ALDEBARAN/RIGEL y REGULUS

El sistema de guerra electrónica RIGEL (evolución más económica del Aldebarán) es capaz de detectar y analizar señales en la banda radar en el entorno de misión del buque, posibilitando la identificación de la forma de onda y su relación con el tipo de plataforma, lo que le permite alertar sobre la posible amenaza. Además, cuenta con sistemas ECM para realizar contramedidas de perturbación y decepción electrónica para protección inmediata del buque.

La versión REGULUS de guerra electrónica permite realizar acciones ESM en la banda de telecomunicaciones, para captación y análisis de señales y obtención de información COMINT⁵⁸.

Alertadores ALR-300/400 y ALQ-500P

Los alertadores-perturbadores son elementos básicos de los sistemas de protección electrónica de plataformas aéreas.

El ALR 400 es un alertador basado en recepción digital en banda ancha, alta sensibilidad y protección frente a perturbaciones. Actúa en las bandas radar CD, E/J y Banda K.

El ALQ 500 dota a la aeronave de capacidad de perturbación en onda continua y de pulsos mediante técnicas digitales de alta velocidad y utilización de librerías de amenazas.

Estos sistemas, por tanto, podemos encasillarlos dentro de los sistemas de autoprotección electromagnética de la plataforma.

Otros programas de EW

Con carácter meramente informativo señalar que actualmente se encuentran en periodo de implementación dos programas de detección de amenazas en el rango de frecuencias infrarroja. Uno de ellos, el programa MANTA, dotará a las aeronaves del Estado y de transporte del EA de la capacidad de autoprotección frente a misiles tipo MANPAD⁵⁹.

⁵⁸ COMINT (en inglés). *COMMunications INTelligence*. Las actividades COMINT forman parte de la SIGINT, actuando principalmente en el campo de las telecomunicaciones, extrayendo información sobre el contenido de las transmisiones.

⁵⁹ MANPADS (en inglés). *Man Portable Aircraft Defense System*.

El segundo es el programa SIRIO que permitirá detectar misiles tipo «rozaolas» (Harpoon), mediante análisis multiespectral en la banda del infrarrojo sobre objetivos situados a menos de 10 Km.

Finalmente, otros desarrollos están teniendo su lugar dentro del campo de la protección frente a amenazas tipo dron. La Dirección General de Armamento y Material está desarrollando el proyecto *Condor* para combatir la amenaza RPAS, constando de dos tipos de elementos, fijos y móviles.

Entre los elementos fijos encontramos el sistema antidron para protección de área e instalaciones fijas. Es de destacar el sistema *Drone Hunter* de uso en la Base de Retamares. Utilizando diversos tipos de sensores es capaz de localizar e interferir la señal de control de un dron o enjambre. En relación con la protección de bases y unidades desplegadas en el exterior las FAS españolas han adquirido el sistema AUDS⁶⁰ que permite detectar pequeños drones (hasta 10 cm.) en un radio de 10 km.

Sistemas de mando y control. El problema de la interoperabilidad

Como se ha visto anteriormente, los sistemas de mando y control de GE son sistemas necesarios para gestionar entornos electromagnéticos cada vez más saturados y complejos. La guerra electrónica y las señales hostiles ya no se limitan a la tecnología militar, ya que dispositivos tan cotidianos como un mando a distancia pueden ser utilizados para detonar artefactos explosivos improvisados (IED). Además, hay un cambio en el entorno militar, donde las tecnologías actuales, como dispositivos móviles y las redes inalámbricas, han irrumpido con fuerza en la disputa por el uso del espectro electromagnético.

Se puede observar un cambio de tendencia en los sistemas de mando y control actuales, pasando del tradicional cometido centrado en la plataforma hacia un enfoque centrado en la red que facilite el intercambio de información. El enfoque centrado en la red tiene ventajas, pero también introduce el riesgo de ciberataques.

⁶⁰ La guerra electrónica en España. *Revista Ejércitos*. revistaejercitos.com

El sistema de mando y control nacional (SC2N)

El concepto de mando y control ha evolucionado enormemente en las FAS con la introducción de la Fuerza Conjunta como su instrumento principal de empleo en operaciones.

En este sentido, el JEMAD ha considerado adecuado dotar a esta Fuerza Conjunta de las capacidades necesarias para llevar a cabo las misiones que le sean encomendadas. Entre estas capacidades se encuentra el dotar a las FAS de un sistema de mando y control que permita la participación del «poder militar», tanto en operaciones nacionales como integrada en otros contingentes multinacionales⁶¹.

Las FAS han sentido la necesidad de dotarse de un sistema de mando y control único, que posibilite la toma de decisiones y el asesoramiento y compartición de información entre autoridades y organismos de forma ágil y fluida, así como su adecuada gestión y protección.

Y es que, en la actualidad, ante la necesidad de ejercer el mando y control, las Fuerzas Armadas han necesitado y necesitan hoy en día emplear diferentes sistemas como SIJE, SIMACET, SMN, JFAC, SICOMEDE, SIMENPAZ, SACOMAR, SICONDEF, y algún otro sistema más, que no se incluye por no hacer más larga la lista⁶².

Pero no solo queda este aspecto circunscrito al ámbito nacional. En el ámbito internacional, la OTAN también ha destacado como uno de sus principales problemas, la falta de interoperabilidad con los sistemas de mando y control nacionales. En este sentido, la OTAN ha lanzado una iniciativa para garantizar que se alcanza la necesaria interoperabilidad. Este proyecto conjunto lo ha denominado *Federated Mission Network* (FMN) y España se ha adherido al mismo en un intento de potenciar la interoperabilidad tanto internamente como en el ámbito aliado.

Con el objetivo de alcanzar la necesaria interoperabilidad se ha puesto en marcha la implantación del sistema de mando y control nacional (SC2N), que tiene como objetivo alcanzar la necesaria «interoperabilidad y la mayor eficacia en el empleo operativo de las FAS»⁶³.

⁶¹ MINISDEF/EMAD. (2019). Directiva 02/19 del jefe del Estado Mayor de la Defensa para el Sistema de Mando y Control Nacional (SC2N),

⁶² Listado de sistemas de información para el mando y control actualmente en uso en las FAS españolas. Este listado está obtenido del conocimiento directo que sobre la materia tiene el autor de esta investigación, debido a sus diversos destinos en relación con los sistemas de mando y control dentro de la estructura de las FAS, concretamente en la antigua Jefatura CIS del EMAD.

⁶³ Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política CIS/TIC del MINISDEF. *Boletín Oficial del Estado* n.º 295, de 10 de diciembre de 2015. Dis-

Si se parte del supuesto, comúnmente aceptado, de que el entorno de seguridad en el futuro escenario operativo en el que previsiblemente actuarán nuestras FAS en el año 2035, se encuentra caracterizado por su volatilidad, incertidumbre, complejidad y ambigüedad, lo que se viene denominando como entornos VUCA⁶⁴, se puede concluir que en este entorno se primará la capacidad de valoración e identificación de patrones de cambio ágil, de forma que reduzca la incertidumbre y que posibilite la adecuada comprensión de la situación en apoyo a la decisión, así como al planeamiento y ejecución de las operaciones.

Si tenemos en cuenta lo previsto en el documento «Entorno operativo 2035» podemos adelantar aquí que la «agilidad permitirá reaccionar con flexibilidad y adaptabilidad ante situaciones desconocidas o confusas».

Será, pues, conveniente el que la Fuerza Conjunta disponga de un sistema de mando y control adecuado a sus necesidades y en este sentido, según declara el coronel Escusol, el Ejército de Tierra está liderando el «Plan de modernización de los sistemas de mando, control y comunicaciones (Plan MC3)» con el objeto de aumentar las capacidades operativas, buscando la superioridad en el enfrentamiento y la protección de sus unidades en cualquier entorno operativo.

El plan MC3 permitirá modernizar los sistemas de comunicaciones tácticos, de tal forma que permita su integración en red siguiendo el concepto NEC y FMN del JEMAD y la OTAN respectivamente.

En este sentido, España está liderando uno de los proyectos de desarrollo de sistemas de mando y control, dentro del mecanismo europeo de cooperación estructurada permanente (PESCO). Se trata del *Strategic Command and Control (C2) System for CSDP Mission and Operations*, dentro del grupo *Cyber, C4ISR*, lo que permitirá obtener un sistema integrado desde el nivel táctico al estratégico, que permita el apoyo al proceso de decisión, planeamiento y conducción de las operaciones y misiones de las fuerzas de la UE.

ponible en: <https://www.boe.es/boe/dias/2015/12/10/pdfs/BOE-A-2015-13385.pdf>

⁶⁴ VUCA (en inglés). *Volatility, Uncertainty, Complexity and Ambiguity*. NATO Allied Command Transformation, Framework for Future Alliance Operations 2018. Disponible en: https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf

Tendencias en el mando y control de las actividades de guerra electrónica

En este apartado se realizará una exposición de las principales tendencias en el ámbito de la OTAN que se encuentran actualmente a vanguardia de los desarrollos en cuestión de doctrina, materiales y organización en cuanto a sistemas de GE.

Las tendencias actuales y futuras incluyen la integración de la guerra cibernética o ciberguerra y la guerra electrónica para formar un entorno ciber-electromagnético. Teniendo en cuenta, que el objeto de este trabajo es el mando y control de la GE, se pueden encontrar zonas de solape con las acciones en el ciberespacio, ya que las redes de comunicaciones, las bases de datos y el propio sistema de mando y control en general deben protegerse de los ataques basados o con origen en la red.

Otro desarrollo es el de la GE cognitiva, que tiene la capacidad de proporcionar de forma autónoma conciencia situacional, ataque electrónico y protección electrónica. Estos sistemas pueden ser análogos a los sistemas de información de gestión que utilizan la inteligencia artificial (AI) para automatizar los procesos en el ámbito de los negocios; en este caso, automatizan las operaciones de GE.

Gestión de las operaciones de guerra electrónica (EWBM)⁶⁵

El mando y control, como capacidad operativa, tiene una importancia considerable y forma parte del marco conceptual de todas las doctrinas y publicaciones sobre la materia. En el ámbito de la guerra electrónica, ocurre exactamente igual, pudiendo afirmarse que no hay documento ni doctrina sobre este asunto que no conceda importancia capital a la gestión de las operaciones de GE⁶⁶.

El *Electronic Warfare Battle Management* (EWBM) proporciona la necesaria coordinación y sincronización de las acciones de GE para un uso eficiente y eficaz del espectro electromagnético proporcionando a los comandantes el adecuado conocimiento y

⁶⁵ EWBM (en inglés). *Electronic Warfare Battlespace Management*.

⁶⁶ Kurt, E. (2013). Digital command and control (C2) in electromagnetic battlespace. *Modeling and Simulation for Defense Systems and Applications VIII*. SPIE. P. 87520G.

comprensión del entorno en apoyo al proceso de decisión y dirección de sus operaciones⁶⁷.

Sin embargo, debido al aumento de la complejidad en el entorno electromagnético se requiere la utilización de sistemas que puedan proporcionar una adecuada SA en apoyo a la toma de decisiones del comandante. Para que los sistemas de gestión de la GE puedan ejercer un control eficaz del espectro electromagnético, es necesario integrar tres conceptos principales⁶⁸:

- Gestión del espectro electromagnético (SM)⁶⁹: esto incluye la gestión del espectro y la resolución de posibles conflictos en el uso del mismo por parte de las fuerzas propias/amigas.
- Gestión de la guerra electrónica (EWBM): que incluye el necesario conocimiento de la situación electromagnética (REMP), y también herramientas para la adecuada planificación, coordinación y sincronización de las actividades de GE, perfectamente integradas con el resto de las operaciones militares mediante un mando y control eficaz.
- Arquitectura, estándares y datos asociados: estos son los CIS⁷⁰ y procesos relacionados, incluyendo los procedimientos y doctrina asociados.

El concepto de guerra electrónica en red

Actualmente hay muy pocos sistemas que integren la gestión del espectro dentro de un contexto centrado en la red (NEC), o como se ha expresado anteriormente, que sea la misma red de sensores (emisores y receptores) la que posibilite y facilite esta gestión. A pesar de que hay una serie de sistemas y conceptos actualmente en desarrollo, se puede afirmar que existe un vacío en la consideración de los requisitos operativos y funcionales para tales sistemas.

El desarrollo de las nuevas tecnologías posibilita el intercambio de gran volumen de datos gracias a la capacidad de las comunicaciones.

⁶⁷ Van Niekerk, B. y Cloete, C. (2015). Management Information Systems for Electronic Warfare Command and Decision Support. *Journal of Information Warfare*, 14(1), pp. 62-73. Disponible en: <https://www.jinfowar.com/subscribers/journal/volume-14-issue-1/management-information-systems-electronic-warfare-command-decision-support>

⁶⁸ Van Niekerk, B. y Cloete, C. (2015). Ídem.

⁶⁹ SM (en inglés). *Spectrum Management*.

⁷⁰ CIS (en inglés). *Communications and information systems*.

Esto ha permitido la extensión de las redes de comunicaciones que abarcan desde los escalones más bajos del nivel táctico hasta los puestos de mando de las grandes unidades en los niveles operacional y estratégico. Estas nuevas capacidades han permitido el desarrollo del concepto NEC⁷¹ o en equivalente en la doctrina americana NCW⁷².

El intercambio de datos entre plataformas, sistemas sensores y elementos de mando y control, permitirá disponer de la información necesaria, en tiempo oportuno, para la adecuada ejecución de la misión encomendada. Esta capacidad será uno de los elementos clave en las operaciones militares en el escenario operativo futuro, lo que permitirá disponer de la información necesaria que en cada momento pudiera considerarse de interés para integrar las capacidades desplegadas de forma que permitan obtener una imagen compartida de la situación operativa (*Shared Situational Awareness* – SSA), esencial para «la efectiva explotación, adquisición de objetivos, planeamiento defensivo y protección de la fuerza»⁷³.

Según el informe realizado por el sistema de observación y prospectiva tecnológica (SOPT)⁷⁴ en su monografía n.º 2 en el año 2009, la interconexión entre sensores y sistemas de GE «permitirá que dichos equipos funcionen de manera cooperativa, facilitará la obtención de la situación táctica común de GE y un uso más eficiente de los recursos de GE disponibles» (SOPT, 2009).

Tendencias en el ámbito OTAN

Dentro de los objetivos perseguidos por OTAN, se encuentran el desarrollo de políticas y doctrinas de GE que permitan un uso efectivo e integrado de todas las capacidades desplegadas por una fuerza en un entorno operativo dado y que utilizan el espectro electromagnético para la consecución de efectos en el nivel operacional, además del desarrollo de capacidades que incrementen el intercambio de información de inteligencia y de planeamiento automáticos en apoyo a la maniobra.

⁷¹ NEC (en inglés). *Network Enabled Capabilities*.

⁷² NCW (en inglés). *Network Centric Warfare*.

⁷³ Ejército de Tierra. (2014). PD3-312. *Guerra Electrónica*.

⁷⁴ El SOPT pertenece a la Subdirección General de Tecnología y Centros de la Dirección General de Armamento y Material, Secretaría de Estado de Defensa del Ministerio de Defensa de España.

En la siguiente figura podemos ver reflejada la complejidad y diversidad de desarrollos conceptuales en el ámbito de las operaciones electromagnéticas.



Figura 7. Nuevos conceptos doctrinales OTAN. (Fuente: OTAN)

Conceptos relacionados con el mando y control de GE como el *Cooperative ESM Operations* (CESMO), EMO, NAVWAR, Spectrum Management, son cada vez más empleados en las diferentes doctrinas y publicaciones sobre el tema. En concreto se analizarán el mando y control de GE y el CESMO de OTAN, ya que se consideran que tienen relación directa con el tema de estudio y están relacionados directamente con las actividades de guerra electrónica en el nivel operacional.

Mando y control de guerra electrónica en el ámbito OTAN⁷⁵

El mando y control de guerra electrónica o *C2ofEW*⁷⁶ es el nombre dado a todas las actividades de implementación asociadas con la

⁷⁵ La información proporcionada en este aptdo. ha sido obtenida gracias a la colaboración e información del ahora capitán de navío Ignacio Nieto anterior jefe del Centro de Operaciones Electromagnéticas del Mando de Operaciones (MOPS) y de su equipo.

⁷⁶ C2ofEW (en inglés). *Command and Control of Electronic Warfare*. Se utilizará este acrónimo dado su uso en el ámbito OTAN.

entrega de capacidades en apoyo al mando y control de guerra electrónica. Uno de los primeros objetivos será reemplazar la base de datos de emisores (NEDB)⁷⁷ de OTAN como proveedor de información para el C2ofEW⁷⁸.

El programa de desarrollo de capacidades C2ofEW forma parte de un conjunto completo de desarrollos que tienen en cuenta cada uno de los factores MIRADO-I para mejorar las capacidades de GE en el ámbito OTAN. Tiene como objetivo el proporcionar a los comandantes y autoridades de la estructura de fuerza de la alianza la capacidad de obtener una imagen electromagnética de la situación (REMP)⁷⁹ que permita planificar, dirigir, coordinar, sincronizar, supervisar y evaluar eficazmente las actividades y acciones de guerra electrónica en todos los dominios de las operaciones, tanto físicos como cognitivo y ciberespacial.

La OTAN ha identificado una serie de limitaciones en sus sistemas de mando y control derivados de la identificación de los riesgos y amenazas previstos en el futuro campo de batalla electromagnético, así como una serie de requisitos que deben de cumplir los mismos y que han dado origen a nuevos desarrollos conceptuales y doctrinales:

- Complejidad y dinamismo del entorno electromagnético.

Las fuerzas de la OTAN están obligadas a operar dentro de un entorno electromagnético cada vez más complejo, dinámico y saturado para lograr los objetivos militares. «La mayor parte de las capacidades de inteligencia, vigilancia y reconocimiento (ISR) de la OTAN, así como la capacidad de ofrecer efectos precisos, navegación, comunicaciones y llevar a cabo las operaciones dependen, cada vez más, de la energía electromagnética»⁸⁰. Sirvan como ejemplos el de los cazas de 5.^a generación o el sistema de vigilancia terrestre (AGS) tendrán una dependencia cada vez mayor del espectro electromagnético para realizar sus operaciones con eficacia.

También señalar el aumento de las amenazas derivadas de los desarrollos de capacidades de guerra electrónica por parte de las fuerzas armadas rusas y chinas, consideradas tradicio-

⁷⁷ NEDB (en inglés). *NATO Emitter Data Base*.

⁷⁸ Bamford, E. y Spreckelsen, M. (2019). Future Command and Control of Electronic Warfare. *The Journal of the JAPCC*, 28. [Consulta: 6/9.2020]. Disponible en: <https://www.japcc.org/future-command-and-control-of-electronic-warfare>

⁷⁹ REMP (en inglés). *Recognised ElectroMagnetic Picture*.

⁸⁰ MC 0064/11, Política EW de la OTAN, apartado 8.

nalmente como capacidades enfrentadas con las de la alianza, donde hasta ahora la superioridad tecnológica de la OTAN había sido incontestable⁸¹.

- Análisis de riesgo.

La falta de interoperabilidad entre los distintos sistemas sensores y plataformas de guerra electrónica de los aliados se puede traducir en las siguientes limitaciones que evidentemente habrá que analizar para soslayar los posibles riesgos operativos:

- Limitaciones para el uso del espectro por las fuerzas de la OTAN, dada la posibilidad de interferencias entre emisores propios, acciones de perturbación electromagnética contra fuerzas propias que no han sido suficientemente coordinadas, etc.
- Falta de conectividad crítica entre autoridades y elementos clave para las operaciones.
- Gestión limitada de los recursos de GE disponibles.
- Control limitado sobre el EEM para evitar posibles amenazas adaptativas.

La ausencia de integración de GE para la planificación, coordinación, sincronización y ejecución dará lugar a la imposibilidad de emplear eficazmente las capacidades aliadas en todos los escalones, lo que puede afectar directamente a la eficacia de las acciones militares que se puedan ejecutar. El mando y control y la SA se verán limitados por enlaces de comunicaciones muy degradados y/o negados (A2/AD).

Los sistemas de inteligencia también se verán limitados en ambientes electrónicamente degradados, denegando o anulando la capacidad de obtención de información por los sensores SIGINT/ESM.

Esta dificultad para explotar, acceder o controlar el EEM de manera efectiva, debido a acciones hostiles de GE o debido a fallos de coordinación entre fuerzas aliadas, afectará negativamente a los ciclos de decisión, aumentando la posibilidad de daños

⁸¹ El Joint Electronic Warfare Core Staff (JEWCS) de la OTAN con el apoyo del Centro de Fusión de Inteligencia de la OTAN ha puesto de relieve en sus valoraciones sobre capacidades de guerra electrónica, un incremento en las inversiones en capacidades de guerra electrónica, así como el desarrollo de nuevos conceptos y capacidades en los ejércitos de otras naciones (normalmente estos estudios se realizan sobre las fuerzas armadas rusas).

colaterales, limitando las operaciones en todos los dominios de enfrentamiento, impidiendo la creación de los efectos deseados y el posterior logro de los objetivos del comandante, aumentando consecuentemente, la probabilidad de fracaso y la no consecución de los objetivos de la misión.

Requisitos operativos

Para hacer frente a los riesgos y amenazas identificados anteriormente OTAN ha definido una serie de requisitos que deberán cumplir los sistemas C2 para EW aliados, y entre los que se han definido los siguientes:

- Conocimiento de la situación.

El C2ofEW proporcionará el necesario conocimiento de la situación prestando un apoyo fundamental para la toma de decisiones de un comandante sobre las fuerzas propias, neutrales y adversarias, así como el conocimiento y estado operativo de los recursos disponibles.

Para la comunidad de inteligencia, el C2ofEW ofrecerá información sobre los adversarios en un entorno operativo dado, proporcionando de forma simultánea información detallada sobre fuerzas propias y actores neutrales, además de datos sobre emisores que servirán para el reconocimiento de amenazas y la orientación de las operaciones futuras.

Permitirá, también, una mejor gestión del espectro electromagnético mediante el suministro de datos que faciliten la resolución de conflictos que pudieran presentarse en el uso compartido del EEM.

La representación gráfica mediante la implementación del servicio REMP, permitirá identificar las fuerzas propias y del adversario por medio de la fusión entre la imagen electrónica obtenida mediante el levantamiento del orden de batalla electrónico (OBE) en una zona de interés de GE y la localización geográfica del emisor. Adicionalmente, permitirá la integración de datos procedentes de distintas fuentes de obtención, permitiendo mejorar los procesos de análisis y evaluación técnica de los emisores (Bamford and Von Spreckelsen, 2019).

- Interoperabilidad.

El C2ofEW proporcionará interoperabilidad necesaria para integrar las actividades de GE en operaciones conjuntas. Esto requiere la capacidad de integrar capacidades, procesar infor-

mación y compartir datos de emisores con una gran variedad de medios GE, facilitando las acciones de apoyo electrónico (EWMS⁸²) mutuo y de información operativa casi en tiempo real.

La necesaria interoperabilidad deberá extenderse a los conceptos, a la doctrina y a los procedimientos operativos facilitando la integración modular de diferentes capacidades de GE aliada. A esto último, habría que añadir la interoperabilidad entre arquitecturas, interfaces de sistemas y modelo de datos para el desarrollo de sistemas en base a las normas NISP⁸³⁸⁴ y taxonomía C3⁸⁵⁸⁶ de OTAN.

Esto facilitará el intercambio de información y el diseño de servicios y sistemas mediante el uso de los estándares que posibiliten la necesaria conciencia situacional, el C2, así como también el apoyo en el análisis y la formación.

- Mando y control.

El C2ofEW tendrá la capacidad de planificar, dirigir, coordinar, supervisar y evaluar las actividades de GE de una fuerza conjunta. Un aspecto esencial del C2 es la capacidad de hacer estimaciones, desarrollar planes, ejecutar acciones directas y supervisar esas acciones mediante la evaluación de los efectos conseguidos y de los resultados pretendidos.

Para lograr lo anterior, será necesario el levantamiento del orden de batalla electrónico (OBE⁸⁷) del área de interés y su visualización mediante REMP, para lo que se requerirá cierto grado de intercambio de información sobre emisores propios previo al despliegue y operación de las unidades de GE de la OTAN. Esto último, podría representar un problema debido a

⁸² EWMS (en inglés). *Electronic Warfare Mutual Support*.

⁸³ OTAN. (2020). NATO Interoperability Standards and Profiles. *ADatP-34*. Volumen 3, ver.13.

⁸⁴ NISP (en inglés). *NATO Interoperability Standards and Profiles*. Consiste en la definición de estándares en apoyo a los órganos de planificación de capacidades, directores de programas y jefes de pruebas sobre sistemas OTAN que se obtengan mediante financiación común entre las naciones aliadas, en el corto y medio plazo. El NISP prescribe las normas técnicas y perfiles necesarios para lograr la interoperabilidad de las comunicaciones y los sistemas de información en apoyo de las misiones y operaciones de la OTAN. De acuerdo con la Estrategia C3 de la Alianza.

⁸⁵ C3 (en inglés). *Command, Control and Communications* (NATO, 2020).

⁸⁶ OTAN. (2020). AC/322-D, NATO C3 Taxonomy Baseline.

⁸⁷ Este concepto está basado en el estándar OTAN descrito en el STANAG 6545 (2020) Common Electronic Order of Battle (C-EOB), publicado por Comité de guerra electrónica de OTAN (NEWAC).

la falta de voluntad de las naciones de compartir datos sobre emisores que puedan afectar a su seguridad, o representar un compromiso de vulnerabilidad que pudiese afectar a sus medios de obtención y que normalmente están relacionados con las capacidades de inteligencia de señales (SIGINT) nacionales.

Además, será importante compartir información sobre emisores propios para la elaboración de listas restringidas de frecuencias esenciales para el adecuado control del espectro electromagnético.

- Entorno de análisis para apoyo y formación.

El C2ofEW dispondrá también de capacidad para llevar a cabo análisis de modelos y simulaciones en apoyo a la toma de decisiones. Estos modelos permitirán realizar análisis sobre previsiones de comportamiento, estableciendo pautas o patrones que ayuden a mejorar la calidad de la información sobre emisores adversarios, estableciendo posibles alternativas y previsiones sobre la eficacia de las acciones de guerra electrónica, especialmente de las medidas ESM.

Actividades de cooperación ESM en la OTAN. Concepto CESMO⁸⁸

La OTAN ha detectado la necesidad de disponer de un sistema que permita la triangulación en tiempo casi real de los emisores de potenciales amenazas. Conocer la ubicación relativa de las amenazas y las fuerzas propias con la necesaria precisión es una de las tareas esenciales a realizar en el entorno electromagnético con el objeto de aumentar la supervivencia de los combatientes, sus sistemas y plataformas. Los datos e información compartida mediante la ejecución de operaciones de ESM cooperativa (CESMO) proporcionan la necesaria visibilidad a las fuerzas de la coalición en operaciones OTAN o en coordinación con otras naciones⁸⁹.

CESMO es un concepto que agrupa medios de obtención SIGINT/ESM en un único sistema de alerta mediante el uso de protocolos de transmisión de datos tácticos (TDL)⁹⁰. En el caso de OTAN,

⁸⁸ CESMO (en inglés). *Cooperative ESM Operations*. Término utilizado en el ámbito de la alianza atlántica para referirse a la compartición de información SIGINT/ESM entre los diferentes medios de obtención nacionales de los países OTAN.

⁸⁹ Thaens, R., Fiore, F. y Schmidt, M. (Octubre 2006. NATO Cooperative ESM Operations: The Present and the Future. Military Communications Conference (MILCOM). ,Disponible en: https://www.researchgate.net/publication/321100900_NATO_Cooperative_ESM_Operations_The_Present_and_the_Future

⁹⁰ TDL (en inglés). *Tactical Data Link*. Término utilizado para referirse a los distintos enlaces de datos que permite el intercambio de información táctica entre plataformas

se ha adoptado dicho concepto mediante acuerdo ratificado en el STANAG 4658 en apoyo de la guerra electrónica (GE) y las operaciones electromagnéticas (EMO)⁹¹. Se trata de plataformas equipadas con sensores capaces de detectar emisiones de radiofrecuencia (RF) de todo tipo de plataformas terrestres, aéreas y marítimas, hostiles y propias/amigas. Las plataformas propias desplegadas en un área determinada podrán hacer uso de dicho protocolo, mediante la red de comunicaciones TDL, para intercambiar datos de forma casi instantánea, y determinar con precisión la posición de uno o varios emisores.

Mediante este protocolo de intercambio de datos e información de ESM, las fuerzas aliadas pueden determinar con precisión a qué tipo de amenaza se están enfrentando mientras, al mismo tiempo, tienen conciencia de la situación relativa del resto de fuerzas, ampliando de esta forma la necesaria conciencia situacional (SA).

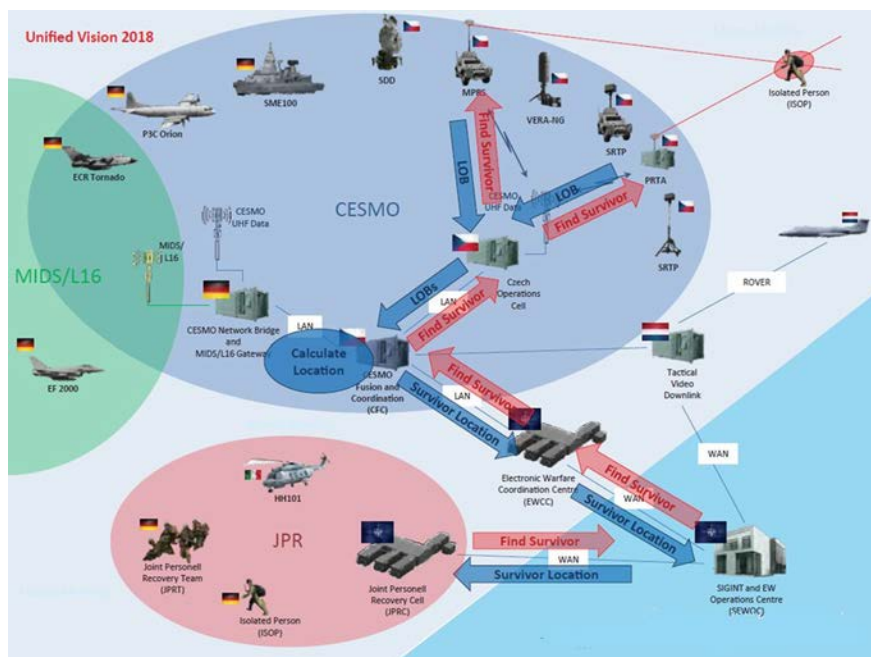


Figura 8. Arquitectura CESMO desplegada en el EX. Unified Vision 2018.
(Fuente: JAPCC, 2019)

y sistemas desplegados en un área o zona de operaciones.

⁹¹ ELLIS, P., *et al.* (Dicembre 2020). Why all NATO Members need to support CESMO Data. *Technology Whitepaper*. Curtiss-Wright Defense Solutions. Disponibile en: <https://www.curtisswrightds.com/infocenter/white-papers/why-all-nato-members-need-cooperative-electronic-support-measure-operations-cesmo-data.html>

Durante el pasado ejercicio *Unified Vision 2018*, se pudo adiestrar esta nueva capacidad, agrupando en una misma red TDL/CESMO varios cazas *Tornado* y un avión P-3 *Orion* que debidamente coordinados desde el EWCC pudieron realizar una triangulación efectiva sobre un caza derribado amigo, logrando determinar su posición y transmitirla a los órganos de mando y control en cuestión de ocho minutos⁹².

Además de mejorar dicha conciencia situacional (SA) y aumentar las posibilidades de supervivencia, las operaciones CESMO permiten a las fuerzas de la coalición aumentar la eficacia y eficiencia en la explotación del espectro electromagnético, al contribuir a la obtención del OBE y a la inteligencia, vigilancia y reconocimiento conjunto de la OTAN (JISR). Además, la información sobre emisores proporcionado por CESMO también forma una parte integral de las células de coordinación de guerra electrónica (EWCC) y de los centros de operaciones SIGINT y EW (SEWOC) en el nivel operacional.

A medida que se va implantando este protocolo en el ámbito OTAN, un número cada vez mayor de países lo están adoptando como estándar de intercambio de información de datos SIGINT/ESM. Este es el caso de España, que conjuntamente con otras naciones europeas están empezando a emplear estos protocolos durante la realización de ejercicios en el ámbito de la alianza.

Para el intercambio de datos se está empleando el Link 16 como protocolo de enlace entre plataformas ESM. En España este protocolo TDL se está implementando mediante el empleo del estándar MIDS⁹³. Algunos miembros de la OTAN ya utilizan TDL, como Link 16, para compartir información de forma segura entre plataformas y sistemas de GE, sin embargo, todo indica que sería demasiado lento, complejo y costoso de implementar en todos los medios de GE utilizados por los países miembros de la OTAN⁹⁴.

⁹² Bamford, E. y Spreckelsen, M. (2019). Future Command and Control of Electronic Warfare. *The Journal of the JAPCC*, 28. [Consulta: 6/9/2020]. Disponible en: <https://www.japcc.org/future-command-and-control-of-electronic-warfare>

⁹³ El STANAG 4175 *Technical Characteristics of Multifunctional Information Distribution System*. (MIDS). El estándar especifica los criterios de los equipos de comunicaciones, navegación y sistemas de identificación utilizados por las naciones aliadas en el ámbito OTAN, además de establecer los requisitos de supervivencia ECM y de compatibilidad eléctrica con otros usuarios en la misma banda de frecuencias.

⁹⁴ Thaens, R., Fiore, F. y Schmidt, M. (Octubre 2006). NATO Cooperative ESM Operations: The Present and the Future. Military Communications Conference (MILCOM).

Tanto CESMO como Link-16 son estándares de uso probado que la industria ya tiene suficientemente desarrollados, además su capacidad de ser interoperables permite su implementación conjunta mediante una pasarela que permite el intercambio rápido de datos e información entre ambas redes, de forma totalmente transparente para el operador, por lo que no requiere ninguna intervención por su parte, siendo totalmente automático.

Las fuerzas terrestres y las plataformas aéreas o navales tienen la posibilidad de compartir o intercambiar datos de interés para SIGINT/ESM sin tener que pertenecer necesariamente a la red de datos de la comunidad de sensores ESM. Gracias a la configuración de diferentes pasarelas de intercambio de información⁹⁵, hoy en día esta información puede alcanzar toda el área de operaciones donde despliegue una fuerza militar.

Conclusiones

Partiendo del análisis de los conceptos de mando y control y de guerra electrónica vistos anteriormente, se puede llegar a determinar la importancia que tiene para el jefe o comandante de una fuerza poder contar con un sistema (personal, medios y procedimientos) de mando y control capaz de integrar las capacidades de guerra electrónica dentro del planeamiento y ejecución de las operaciones militares.

Del mismo modo, como se ha podido comprobar a lo largo de este artículo, se pone de manifiesto la importancia del dominio y/o control del espectro electromagnético para el éxito de las operaciones en el horizonte 2035. En este sentido, se destaca el desarrollo exponencial de las capacidades y sistemas que emplean el espectro como medio para llevar a cabo su misión. La OTAN lo ha identificado como un dominio más de las operaciones, como puede ser el terrestre, el marítimo, el espacial, el cognitivo y el ciberespacial. Se concluye también, la importancia

Disponible en: https://www.researchgate.net/publication/321100900_NATO_Cooperative_ESM_Operations_The_Present_and_the_Future

⁹⁵ Este es el caso del TDL (MIDS-Link 16) y CESMO en el que usuarios de las dos redes tendrían la posibilidad de intercambiar datos operativos entre ellos mediante una pasarela sin necesidad de pertenecer a ambas redes de comunicaciones. Se trata simplemente de dotar a ambas redes de un interfaz común que posibilite el intercambio de información de acuerdo a unos requisitos funcionales y operativos previamente definidos y aprobados.

de las operaciones electromagnéticas (OEM), y de cómo la guerra electrónica tendrá un papel destacado en las mismas.

Si tenemos en cuenta la actual situación de la capacidad C2 dentro de nuestras fuerzas armadas se pone de manifiesto que el estado de la capacidad de mando y control de las operaciones electromagnéticas todavía se encuentra en fase de desarrollo, especialmente de nuevos conceptos⁹⁶, procedimientos y de materiales. Se destaca no obstante el interés del JEMAD por dotar a la Fuerza conjunta de un sistema capaz de integrar las capacidades desplegadas en un entorno de capacidades en red (NEC/FMN), resaltando los proyectos de desarrollo que está liderando España dentro de las iniciativas PESCO de la UE como es el de las capacidades de mando y control para misiones y operaciones en el seno de la PCSD.

Las capacidades actuales para ejercer el mando y control sobre las actividades de guerra electrónica tienen que utilizar sistemas de compartición de información de situación y estado de los sensores y bases de datos de emisores de forma semiautomática, ya que no disponen de un sistema para el mando y control capaz de integrar los elementos sensores de guerra electrónica, plataformas y sistemas de combate y elementos de los puestos de mando siguiendo el concepto de capacidades en red. Sin embargo, podemos afirmar que existen desarrollos en línea con dichos conceptos que hacen pensar que en el horizonte 2035 las Fuerzas Armadas españolas dispondrán de capacidades de mando y control capaces de integrar todos los servicios que hacen uso del espectro electromagnético.

Por último, se destacan los desarrollos que se están llevando a cabo en el seno de la Alianza Atlántica y que, sin duda alguna, están alineados con el objetivo de dotar a las fuerzas de OTAN de un mayor grado de interoperabilidad, como es el caso de la C2ofEW o CESMO.

Derivados del análisis anterior, se puede determinar que:

1. Según los estudios de prospectiva en el horizonte 2035 el espectro electromagnético será un entorno o dominio de actuación fundamental para la consecución de efectos mediante la ejecución de acciones de GE encaminadas a su dominio y control.

⁹⁶ El nuevo concepto conjunto de operaciones electromagnéticas está actualmente en fase de borrador final pendiente de aprobación por el JEMAD.

2. Para alcanzar ese dominio o control del espectro, se necesitará integrar todas las capacidades que lo utilizan de forma que se facilite el planeamiento, coordinación, sincronización y control de las actividades en el entorno electromagnético. Este nuevo paradigma se identifica con el concepto de operaciones electromagnéticas, en el que las FAS españolas, organismos como la OTAN y otras fuerzas armadas a la vanguardia tecnológica ya han identificado como fundamental para alcanzar el éxito en las operaciones.
3. Dado que es en el nivel operacional donde se planean, coordinan y dirigen las operaciones principales, se necesitará dotar a este nivel de los recursos necesarios para el mando y control eficaz, integrando en este nivel todas las capacidades de la fuerza conjunta, incluido las capacidades de guerra electrónica.

Por lo tanto, y a modo de conclusión final, se puede determinar la importancia inequívoca de disponer de la capacidad para el mando y control de guerra electrónica en el nivel operacional, capaz de proporcionar a la Fuerza Conjunta los elementos de juicio necesarios que faciliten el planeamiento, coordinación y control de las operaciones militares en el entorno electromagnético, de tal forma que permita enfrentar con suficiente garantía de éxito los retos que plantea el futuro entorno operativo en el horizonte 2035.