ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TÍTULO: HACIA LA INTEGRACIÓN DE LAS OPERACIONES DE GUERRA ELECTRÓNICA Y CIBERDEFENSA EN EL ÁMBITO MILITAR CONJUNTO PARA EL LOGRO DE LOS OBJETIVOS MILITARES

AUTOR: MY GERARDO DANIEL ORTIZ

TUTOR: TC (R) CARLOS FEDERICO AMAYA

AÑO 2025

Resumen

Las operaciones de Guerra Electrónica y Ciberdefensa se desarrollan tanto en tiempo de paz como en tiempos de guerra y deben estar en capacidad de ejecutarse en un ambiente operacional cada vez más complejo. En una vertiginosa evolución tecnológica en la cual estamos sumergidos se destacan los avances de medios informáticos y de equipos radioeléctricos. Esta constante actualización de tecnologías de los materiales sumado a la aparición de una gran diversidad de protagonistas (estado-nación o no combatientes), propios de los conflictos actuales, provocan una seria amenaza a las propias infraestructuras críticas. Será necesario entonces, desarrollar acciones que permitan detectar ciberincursiones hostiles que atenten contra la integridad de la nación y ser capaces de actuar ofensivamente si la situación así lo requiere.

El enfoque multidominio requiere que se integren funciones y capacidades tanto de Guerra Electrónica como de Ciberdefensa pasando a ser estas una de las prioridades del comandante operacional para hacer frente a las amenazas actuales. Será necesario que las fuerzas militares operen en dominios físicos y no físicos, y para que estas operaciones se desarrollen efectivamente es imprescindible depender de sistemas de comunicación electromagnética en red que funcionen en el ciberespacio donde el espectro electromagnético es el protagonista más importante. Lograr la superioridad en este dominio no físico y transversal al resto de los dominios permitirá mantener la libertad de acción para la mayoría de las operaciones.

Al depender críticamente de redes y sistemas electrónicos interconectados, la infraestructura civil y militar genera una dependencia estructural y a la vez una superficie de ataque que diversos actores explotarán sistemáticamente. Podemos citar como ejemplos las Amenazas Persistentes Avanzadas (APTs), Estados Naciones hostiles o el cibercrimen organizado.

El riesgo no está solo en vulnerabilidades puntuales (fallas de seguridad documentadas, zero-days etc.), sino en la arquitectura misma de los sistemas y como ejemplos podemos mencionar los sistemas heredados sin actualizaciones de seguridad, convergencia IT/OT sin segmentación adecuada o la ausencia de redundancia operacional.

Por lo expuesto, tratare de plantear cómo la convergencia operacional entre Guerra Electrónica (también denominada guerra electromagnética) y la Ciberdefensa en el ámbito militar conjunto aportaría una reducción de superficie de ataque mediante la sincronización de contramedidas, una explotación de vulnerabilidades en ambos dominios (espectro electromagnético más cibernético) y en definitiva un efecto multiplicador materializado en acciones cinéticas coordinadas con operaciones no-cinéticas.

Esta integración transformaría dos capacidades paralelas en un sistema de efectos complementarios preparados para actuar sobre las redes del adversario.

Palabras claves
Integración – Guerra Electrónica – Ciberdefensa – Operacional - Guerra Electromagnética

Índice

Introducción

Este trabajo de investigación pretende contribuir al logro de una integración entre operaciones de ciberdefensa y guerra electrónica para tratar de evitar que ambas se ejecuten de manera aislada entendiendo que son actividades que, si bien son muy diferentes, las dos se complementan y se desarrollan en dominios (ciberespacio y electromagnético) que son transversales al resto de los dominios en los que se desarrollan las actuales operaciones militares.

Como objetivo general, se plantea analizar la integración de las operaciones que se desarrollan en el dominio del ciberespacio y electromagnético en un ambiente operacional cada vez más complejo para alcanzar los objetivos operacionales con eficacia en la Acción Militar Conjunta. Del objetivo general se desprenden tres objetivos particulares: el primero de ellos analizar las capacidades y tácticas de la guerra electrónica en el contexto de las operaciones militares, identificando sus fortalezas, debilidades para mejorar la eficacia en la Acción Militar Conjunta; el segundo objetivo, analizar las estrategias y tecnologías de ciberdefensa empleadas en operaciones militares para la determinación de su efectividad en la protección de infraestructuras críticas y limitación de amenazas cibernéticas.; y por último el tercer objetivo busca analizar la sinergia y diferencias entre las operaciones de guerra electrónica y ciberdefensa en el marco de las operaciones militares conjuntas, identificando áreas clave para la integración de ambas operaciones.

Trabajaremos con la hipótesis de que la integración de las operaciones de guerra electrónica y operaciones de ciberdefensa contribuye a optimizar el empleo de los medios disponibles para alcanzar objetivos operacionales.

En cuanto a la metodología, llevaremos adelante nuestra investigación explicativa a través de una metodología cuantitativa, en donde se realizará un análisis bibliográfico de doctrina y documentación vigente y en proyecto, artículos publicados relacionados con la temática y trabajos de investigación. Se buscará explicar cómo estos dos tipos de operaciones que, si bien son diferentes, se integran para hacer frente a las amenazas complejas y diversas que explotan el entorno de información concentrándonos en el ámbito militar conjunto.

Como técnica de validación se empleará el análisis bibliográfico y se estructurará en tres capítulos. El primer capítulo abordará un análisis de las

capacidades y tácticas y su impacto en el Acción Militar Conjunta. El segundo capítulo abordará el tema de ciberdefensa con respecto a sus estrategias y tecnología evaluando la efectividad en la protección de las infraestructuras críticas. El tercer capítulo desarrollará la integración y diferencia entre la guerra electrónica y la ciberdefensa en el contexto de operaciones militares conjuntas. Por último, se presentarán las conclusiones, donde se detallarán los principales resultados vinculados a los objetivos, y se responderá la pregunta de investigación.

Para introducirnos en la temática es necesario mencionar que con el acuerdo de Paz de Westfalia en el año 1649 surgen lo que conocemos como las Generaciones de la Guerra. Dentro de estas generaciones podemos mencionar cuatro: la Primera Generación de la Guerra Moderna es conocida como la guerra de la táctica de líneas y columnas, la Segunda Generación de la Guerra fue desarrollada por el ejército francés caracterizada por la guerra de trincheras y fortificaciones estáticas donde "La artillería conquista, la infantería ocupa" (Frente Occidental, Primera Guerra Mundial (1914-1918), la Tercera Generación de la Guerra surge luego de la Primera Guerra Mundial por el ejército alemán y es conocida como la guerra relámpago (Blitzkrieg) o guerra de maniobra y por último Wiliam S. Lind en su artículo de la revista Military Review (2005) nos dice que la Cuarta Generación de la Guerra señala el cambio más radical desde la paz de Westfalia. En la Guerra de Cuarta Generación el estado pierde su monopolio de la guerra y afirma que alrededor del mundo las fuerzas armadas se encuentran luchando en contra de oponentes no estatales tales como Al Qaeda, Hamas y Hesbolá.

Es dable mencionar que, en Occidente, se ha desarrollado en los últimos años el concepto de Guerras de 5ta Generación (5GW) el que se ha superpuesto en gran medida por el concepto de "guerra cognitiva" de la OTAN (introducido en 2021)

Krishnan, Armin, en su artículo "Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison." Publicado en el Journal of Strategic Security 15, no. 4 (2022): 14-31. Caracteriza la 5GW como aquella que se centra en la manipulación de percepciones, narrativas y el “terreno humano”, donde los actores pueden ser individuos o pequeños grupos con alta tecnología, el

objetivo no es conquistar el Estado, sino socavar su legitimidad y la violencia es mínima, dispersa y a menudo invisible; el enemigo puede no darse cuenta de que está en guerra. Ejemplo de ello son las campañas de desinformación o manipulación cultural.

Se crea aquí un concepto dado en llamar "Conflicto en la Zona Gris (GZC)" donde las estrategias de grandes potencias (Rusia, China, Irán) desafían el orden internacional sin llegar a guerra abierta. Se caracteriza por campañas prolongadas, uso de instrumentos civiles (diplomacia, economía, propaganda), y tácticas graduales materializadas en el ambiente cibernético por la exfiltración de datos en pequeños paquetes para evitar detección y el compromiso progresivo de redes mediante escalamiento gradual de privilegios, buscando evitar escaladas deliberadas y permanecer bajo el umbral de guerra convencional.

Continuando con lo desarrollado hasta ahora es necesario introducirnos en el término de Guerra Híbrida, en donde Frank Hoffman (2007: 14) nos dice que en este tipo de conflictos se incorporan un abanico de distintas formas de guerra, incluyendo capacidades convencionales, tácticas y formaciones irregulares, actos terroristas que comprenden coerción y violencia indiscriminada.

En lo que respecta a los medios, estos son híbridos en cuanto a su tipo y a su aplicación. Es decir, pueden recurrir tanto al uso de sistemas de comando encriptados, misiles tierra – aire portátiles, así como también a emboscadas, ciberataques, dispositivos explosivos improvisados y/o asesinatos (Hoffman, 2007).

Otro concepto que se encuentra íntimamente relacionado con las Guerras de Cuarta Generación y Guerra Híbrida es el concepto de Operaciones Multidominio, estas operaciones, como nos menciona un artículo de Congressional Research Service. Defense Primer: Army Multi-Domain Operations (MDO). 2021, son planificadas y ejecutadas por una Fuerza Conjunta para contrarrestar y derrotar a un adversario con capacidades similares capaz de disputar en todos los dominios (aire, tierra, mar, información, espacio electromagnético, ciberespacio, etc.) tanto sea durante la competencia como en un conflicto armado. Las MDO ofrecen a los Comandantes Operacionales numerosas opciones para ejecutar operaciones simultáneas y secuenciales

utilizando la sorpresa y la integración rápida y continua de capacidades en todos los dominios para presentar múltiples dilemas a un adversario con el fin de obtener ventajas físicas y psicológicas e influencia y control sobre el ambiente operacional.

En línea con lo anteriormente expresado cabe mencionar que dentro del diseño operacional multidominio nos interesan particularmente dos aportes a las líneas de operaciones desarrolladas en el (Boletín Informativo – EMCO, 2023):

> "Aporte del ámbito cibernético a las líneas de operaciones multidominio. Contribuirá esencialmente con lo atinente a acciones de ciberdefensa de las organizaciones y sistemas propios intervinientes en las operaciones; como así también, potenciales ciberataques propios a los sistemas del agresor para afectarlos y; ciberdefensa de los objetivos de valor estratégico asociados a infraestructura vital. Tomará importancia relevante mediante la ejecución principalmente de operaciones cibernéticas defensivas activas, de explotación pasiva y activa, y operaciones ofensivas y de respuesta. El ámbito se caracterizará por ser imposible la distinción de fronteras, enemigos visibles, y por constituirse el ciberespacio en un ambiente artificial y cambiante.
>
> Aporte del ámbito electromagnético a las líneas de operaciones multidominio. La explotación del espectro electromagnético actual excede ampliamente las concepciones tradicionales de uso de comunicaciones radioeléctricas, radares o sensores habitualmente conocidos. En la actualidad, la telefonía celular, las redes wifi, los radiocontroles de drones, sistemas de vigilancia y reconocimiento que emplean medios de comunicaciones especiales, los enlaces en todas las bandas de frecuencias admisibles, y todo modo de irradiación electromagnética que atraviesa el campo de combate, resulta de injerencia de este ámbito." (Estado Mayor Conjunto, 2023)

En la actualidad, las operaciones militares se desarrollan en un entorno operativo extremadamente complejo, en donde el factor de éxito se alcanza mediante el logro de efectos letales y no letales en dominios físicos y no físicos y dentro de estos últimos es en donde se desarrollan las operaciones de Guerra Electrónica y Ciberdefensa.

La doctrina conjunta argentina en su reglamento Guerra Electrónica para la Acción Militar Conjunta, la define como cualquier acción que implica el uso de Energía Electromagnética o dirigida para controlar el espectro electromagnético o

atacar al enemigo. Entendiendo como Espectro Electromagnético (EEM) al conjunto de ondas de diferentes características, las cuales se clasifican de acuerdo con su longitud, frecuencia y energía (Salcedo Meza 2021).

Desde el punto de vista de las operaciones de ciberdefensa, Anca (2015) concluye que los avances tecnológicos junto al elevado nivel de inserción de la cibernética en el nuevo ambiente operacional hacen que un ataque cibernético logre mayores efectos destructivos. De esta manera, debemos tener en cuenta avanzar hacia una gestión de las redes informáticas del teatro de operaciones, buscando alcanzar los requisitos mínimos de seguridad para la interoperabilidad de las diferentes Fuerzas, asegurando de manera confiable la defensa homogénea del sistema de información.

En la actualidad podemos encontrar, en doctrina militar conjunta (EMCFFAA, 2012), conceptos referidos a Guerra Electrónica donde se menciona la necesidad de poseer equipamiento con este tipo de capacidad y en redes donde los mismos son empleados no solo por personal militar sino también por civiles para realizar actividades de comunicaciones, inteligencia, navegación, almacenamiento y procesamiento de información. El reglamento de Guerra Electrónica para la Acción Militar Conjunta que resume los conceptos expuestos en el siguiente texto:

> "Las operaciones militares dependen, en gran medida, de dichos equipamientos para su consecución. Esto trae aparejado el uso del espectro electromagnético, el cual refiere al rango de frecuencias de radiaciones electromagnéticas que van desde cero hasta infinito y que, a su vez, está dividido en bandas que van desde frecuencias de radio hasta frecuencia de rayos-x y gama. Dicha utilización genera un ambiente, que forma parte de un entorno del manejo de la información, y que se lo denomina Ambiente Electromagnético (Electromagnetic Environment – EME)." (Estado Mayor Conjunto 2012).

A raíz de este planteo, surge el concepto de ambiente electromagnético que es desarrollado por la publicación conjunta de Guerra Electrónica de los Estados Unidos de Norteamérica (JCS, 2012) y nos establece que el ambiente operacional está compuesto por las condiciones, circunstancias e influencias que afectan el empleo de capacidades e influyen en las decisiones del comandante. Abarca áreas físicas y factores (de los dominios aéreo, terrestre, marítimo y

espacial) y el entorno de información (que incluye el ciberespacio). El ambiente electromagnético trasciende todos los dominios físicos y el entorno de información, y se extiende más allá de fronteras o límites definidos, complicando así a las Operaciones Conjuntas del Ambiente Electromagnético (JEMSO). Una variedad de factores, incluidos los tipos de equipos empleados, los usuarios del equipo (por ejemplo, fuerzas aéreas, navales y terrestres), las capacidades del oponente, la geografía y el clima también influyen significativamente en la conducta de JEMSO.

Con respecto a operaciones de ciberdefensa no encontramos doctrina vigente, solo un documento proyecto que hasta el día de hoy no está aprobado. Sin embargo, se han realizado varias investigaciones y artículos que definen conceptos como ciberespacio, ciberguerra y consecuentemente ciberdefensa. Se puede citar lo expresado por (Casarino, 2019) quien nos dice que, con la aparición del ciberespacio para la confrontación de intereses, surge también un nuevo ámbito para el desarrollo de los conflictos y que puede ser considerado como otra variante de las guerras modernas, pero que reúnen todas las características para tener una categoría propia, la Ciberguerra. Y dentro de la evolución de la terminología nos menciona que Norbert Winer, profesor del Instituto de Tecnología de Massachussets en el año 1964 creó el término de cibernética; el autor de obras de ficción, William Gibson fue quien desarrolló en el año 1984 el término de ciberespacio y por último Francois Huyghe, especialista francés en ciencias de la información estratégica, amplió la distinción entre ciberguerra que se orienta estrictamente a la conducción de operaciones militares tendientes a destruir o controlar los sistemas de comunicación del oponente.

Uzal (2012) nos agrega que la guerra cibernética es eminentemente asimétrica haciendo hincapié en que uno de los escenarios potenciales que se le puede presentar a un estado – nación es recibir ataques cibernéticos y por incapacidad tecnológica y/o de gestión, terminar adjudicando los desastres ocasionados por dichos ataques a accidentes impredecibles.

Ante el cambio radical del ambiente operacional provocado por la confluencia de la tecnología de las redes y de equipos de comunicaciones, sumados a los constantes avances en materia de tecnología alámbrica, inalámbrica y el creciente efecto que producen las redes sociales lo que provoca un cambio en la sociedad, hace imperante que las fuerzas armadas se equipen y capaciten para

poder enfrentar las diferentes amenazas que surgen de esta permanente evolución. La múltiple cantidad de agentes (estados-nación o no combatientes) que aprovechan y explotan esta revolución tecnológica, mediante ataques cibernéticos o realizando operaciones de guerra electrónica, se constituyen en una seria amenaza a la Infraestructura Crítica (IC) de los estados. Es por todo esto que llegamos al interrogante principal de esta investigación ¿Cómo la integración de las operaciones de ciberdefensa y guerra electrónica pueden contribuir de manera exitosa al logro de objetivos operacionales?

Capítulo I

Análisis de las capacidades y tácticas y el impacto de la Guerra Electrónica en la Acción Militar Conjunta

El presente capítulo intenta analizar el uso de la Guerra Electrónica dentro las operaciones militares conjuntas, destacando su importancia como una capacidad clave para lograr y retener la supremacía en el espectro electromagnético. En un entorno operacional que es, sin duda, más complejo y tecnológico, la Guerra Electrónica se establece como un elemento vital para asegurar la libertad de acción, proteger las comunicaciones propias y afectar las del enemigo. A lo largo del desarrollo, se analizarán minuciosamente las tres acciones centrales de la Guerra Electrónica; concretamente, el Ataque Electrónico, la Protección Electrónica, y el Apoyo de Guerra Electrónica. Cada una de ellas, serán abordadas de manera que se determine su función específica y cuál es su contribución al éxito de la maniobra conjunta.

Sección I

Conceptos fundamentales de la Guerra Electrónica

Con el inicio del uso militar de las emisiones radioeléctricas nace lo que conocemos como Guerra Electrónica. Los primeros indicios de su aparición datan de la Primer Guerra Mundial (1914-1918) cuando se conocieron los primeros intentos de interceptación de emisiones enemigas. Se sabe que las tropas alemanas obtuvieron grandes ventajas al interceptar las emisiones de comunicaciones de las tropas rusas en Tannenberg. Ya para la 2da Guerra Mundial (1939-1945) este tipo de operación evolucionó notablemente, haciendo un uso más extenso del espectro electromagnético. Es en esta guerra en donde aparece el radar y comienza un crecimiento exponencial de este tipo de operación llegando a ser decisivo para alcanzar la victoria en las operaciones militares. Ya para el final de la guerra surgen los bloqueadores de radar y de comunicaciones y junto a ellos aparecen los primeros receptores de contramedidas que juntos inciden directamente en la planificación de las operaciones.

En la actualidad, el espectro electromagnético es considerado como el

campo de batalla más crítico, por sobre el terrestre, naval, aéreo o espacial. Llegando a ser sumamente determinante en el desenlace de los conflictos sin que se efectúe el primer disparo físico. Como se mencionó anteriormente desde su empleo masivo en la Segunda Guerra Mundial, la Guerra Electrónica (GE) ha evolucionado de manera tal que ha llegado a convertirse en una pieza fundamental para alcanzar la superioridad en el enfrentamiento de los conflictos modernos, buscando, mediante operaciones específicas, reducir las capacidades de los sistemas electrónicos del enemigo, protegerse de las operaciones de GE del oponente para mantener en operaciones los sistemas electrónicos propios y asegurar su efectivo empleo en las operaciones militares.

> "La Guerra Electrónica es un elemento importante de los Sistemas de Comando, Control, Comunicaciones, Inteligencia e Informática (C3I2) y provee: 1. Alerta contra emisiones hostiles; 2. Ocultamiento contra emisiones hostiles; 3. Interferencia de Sistemas hostiles; 4. Apoyo a las operaciones de engaño; 5. Apoyo a la detección, clasificación y lanzamiento transhorizonte." (Procedimiento para las Operaciones de Guerra Electrónica; RO -2-030, pags. 1.01-2).

Lo expresado anteriormente, extraído de la doctrina específica en materia de Comunicaciones y Guerra Electrónica de la Armada de la República Argentina marcan un lineamiento general en concordancia con las doctrinas de otras fuerzas armadas en la que encontramos con exactitud la finalidad de este tipo de operaciones. Al respecto una publicación conjunta del año 2012 de los Estados Unidos de Norteamérica nos menciona que:

> "El término guerra electrónica se refiere a acciones militares que involucran uso de energía electromagnética y energía dirigida para controlar el espectro electromagnético o atacar al enemigo. La GE consta de tres divisiones: ataque electrónico (AE), Protección Electrónica (PE) y Apoyo de Guerra Electrónica (AGE).
>
> La guerra electrónica puede afectar negativamente a las fuerzas amigas cuando no se integran y coordinan adecuadamente. La misma se emplea para crear efectos decisivos e independientes o para apoyar operaciones militares generando varios niveles de control, detección, negación, engaño, perturbación, degradación, explotación, protección y destrucción." (JCS, 2012).

En referencia a las operaciones de Guerra Electrónica, Herrera (2017) concluyó que las mismas deben ser planeadas y ejecutadas en forma conjunta integrando una celda independiente para asegurar el comando y control, la defensa aérea, el engaño, las operaciones de ciberdefensa, las comunicaciones, las operaciones en el espacio, las operaciones de inteligencia y las operaciones de información.

Chiavaro (2018) agrega que la Guerra Electrónica (GE) forma parte integral inherente de las tácticas y procedimientos que se ejecutan en el nivel operacional. La GE constituye una herramienta para generar las condiciones favorables a la ejecución de las operaciones militares decisivas.

Sección II

Actividades de Guerra Electrónica

Para continuar con el desarrollo del primer capítulo es necesario avanzar con algunas definiciones que son esenciales para comprender este tipo de operaciones que utilizan el espectro electromagnético para la concreción de los objetivos militares, sea este, el control del espectro electromagnético o atacar al enemigo. Entonces podemos mencionar que la GE constituye un componente muy importante dentro del marco de las operaciones militares conjuntas, ya que permite el control y la explotación del espectro electromagnético como un factor decisivo en el combate moderno. Las fuerzas que logran superioridad en este dominio obtienen una ventaja operacional concreta, afectando la capacidad de mando, control, detección y respuesta del oponente. Como mencionáramos anteriormente, de acuerdo con la doctrina conjunta del Departamento de Defensa de los Estados Unidos, la GE comprende tres funciones principales: Ataque Electrónico (AE), Protección Electrónica (PE) y Apoyo de Guerra Electrónica (AGE) (JCS, 2012).

Ataque Electrónico (AE)

Odierno (2014) nos define el Ataque Electrónico como el empleo de energía electromagnética, dirigida, con el propósito de degradar, neutralizar o destruir las capacidades en el espectro electromagnético del enemigo. Esta función abarca la interferencia de comunicaciones y no comunicaciones, entendiendo a

estas últimas como todas aquellas emisiones electromagnéticas que no tienen como fin transmitir información entre personas o entre sistemas de mando y control pero que al ser emisiones dentro del espectro electromagnético siguen siendo detectables y en consecuencia pueden ser interferidas. Como ejemplo de emisiones de no comunicaciones podemos mencionar emisiones de radar, sistemas de guiado y telemetría de misiles o artillería y sensores en general altímetros, transpondedores, etcétera. Su empleo en el nivel operacional impacta directamente sobre el nivel táctico, donde el AE busca negar el uso efectivo del espectro electromagnético al enemigo mediante la negación del uso de los sistemas de comunicaciones, sistemas de armas y el sistema de Comando, Control, Comunicaciones, Inteligencia e Informática (C3I2) reduciendo así su capacidad de reacción. En un ambiente conjunto, su aplicación requiere una coordinación precisa con las operaciones de maniobra y fuego, maximizando la sinergia entre efectos cinéticos y no cinéticos.

Protección Electrónica (PE)

La Protección Electrónica, por su parte, busca garantizar la integridad de los sistemas propios frente a las acciones electromagnéticas del enemigo.

> "Consiste en todas aquellas acciones realizadas para proteger al personal, instalaciones, equipamientos de cualquier efecto producido por el uso del espectro electromagnético por parte de la propia fuerza o enemigo que degrade, neutralice, o destruya la capacidad de combate propio." (Guerra Electrónica para la Acción Militar Conjunta; PC 13-50, 2012, pág. 31)

Este tipo de actividad incluye diferentes tareas, de las cuales podemos mencionar la gestión del Espectro Electromagnético (EEM), la aplicación de contramedidas de interferencia, el diseño de equipos resistentes a perturbaciones y la implementación de doctrinas de empleo seguras (EMCFFAA, 2012). En las operaciones conjuntas, la PE adquiere un carácter proactivo, integrando la planificación de frecuencias y la compatibilidad electromagnética como elementos críticos para sostener la continuidad operativa.

Apoyo de Guerra Electrónica (AGE)

Finalmente, el Apoyo de Guerra Electrónica constituye la base informativa

sobre la cual se desarrollan tanto el ataque como la protección electrónica. El reglamento conjunto nos define esta actividad como:

> "La división de la Guerra Electrónica que incluye acciones conducidas por o bajo el control directo del Comandante Operacional para obtener información de la energía presente en el medio ambiente, mediante la búsqueda, interceptación, escucha, localización, análisis, identificación, evaluación y registro de las características de las emisiones detectadas, intencionales o no, con el fin de realizar un inmediato reconocimiento y seguimiento de amenazas como así la planificación y conducción de futuras operaciones. Además de ser utilizada para producir Inteligencia de Emisiones, detectar amenazas para atacarlas electrónicamente o destruirlas y producir inteligencia." (Guerra Electrónica para la Acción Militar Conjunta; PC 13-50, 2012, pág. 17)

Su objetivo es proporcionar información para producir inteligencia de señales (SIGINT) y de esta manera facilitar la toma de decisiones. Chiavaro (2018) nos menciona que este proceso permite elaborar un cuadro situacional del espectro, identificando patrones de empleo enemigo y facilitando la planificación de futuras operaciones. En el ámbito conjunto, el AE se convierte en una herramienta de apoyo directo para el mando, al proveer información en tiempo real que contribuye a anticipar las intenciones del enemigo.

De esta forma, la Guerra Electrónica consolida su rol como una capacidad decisiva en la conducción de operaciones conjuntas, donde la gestión del espectro electromagnético, la coordinación interagencial y el dominio técnico de los medios empleados se constituyen en factores determinantes para la obtención de la superioridad operacional.

Sección III

Importancia de la Guerra Electrónica en la Acción Militar Conjunta

Como se mencionó en el comienzo de este capítulo las operaciones militares se desarrollan en un entorno operativo extremadamente complejo en donde la GE adquiere un rol fundamental para el logro de los objetivos militares. Concentrándonos en los dominios no físicos la importancia de este tipo de actividades alcanza niveles decisivos teniendo en cuenta que resulta necesaria la

coordinación y ejecución en forma conjunta por los medios de las tres Fuerzas Armadas.

Con el fin de alcanzar todo su potencial, la Guerra Electrónica debe estar integrada con otros aspectos de las operaciones militares conjuntas y esta integración requiere de un planeamiento cuidadoso como nos menciona (EMCFFAA, 2012), destacando que la GE conjunta debe ser planificada y dirigida en forma centralizada y ejecutada de manera descentralizada. Con respecto al proceso de planificación de la Guerra Electrónica Conjunta se deberían tomar ciertas acciones para integrar el planeamiento conjunto, entre otras podemos mencionar, la determinación del tipo, la duración, ubicación geográfica prevista durante la operación, el estudio de la magnitud de las operaciones y estimar la cantidad y experiencia del personal.

Este tipo de planificación es sumamente importante para que las capacidades de GE se utilicen mediante correctos niveles de control y protección en el EEM y evitar de esta manera afectar involuntariamente a la propia fuerza.

Conclusiones parciales del Capítulo I

La Guerra Electrónica (GE), sin duda, se está afianzando como un elemento crucial y vital, en el desarrollo de operaciones militares conjuntas. Esto, por supuesto, debido a sus facultades que son decisivas para el dominio del espectro electromagnético. Un análisis detallado de la doctrina nos conduce a la conclusión de que una integración efectiva, dentro de la planificación y ejecución conjuntas, es fundamental para lograr la superioridad en el ámbito operacional. Los documentos doctrinales, aquellos en que se basa este análisis, convergen en la idea de que el control del espectro electromagnético actúa como un potente multiplicador del poder de combate. Su gestión, por lo tanto, debe ser ejecutada desde los más altos niveles de la conducción, hasta el nivel táctico.

Las tres actividades que conforman la GE: Ataque Electrónico (AE), Protección Electrónica (PE) y Apoyo de Guerra Electrónica (AGE) deben entenderse como capacidades complementarias que, integradas en un mismo sistema, permiten generar efectos sinérgicos en todos los niveles de la conducción. El EA ofrece la posibilidad de negar o degradar la capacidad enemiga de mando y

control; la PE garantiza la preservación de los sistemas propios frente a la acción del enemigo; y el AGE brinda la información necesaria para anticipar, planificar y ejecutar con precisión los efectos que se desean alcanzar en el EEM.

Aun así, la GE, implementada en el ámbito conjunto, enfrenta grandes retos, principalmente en el área de la tecnología y estructural. La necesidad imperiosa de equipamiento especializado, junto a la exigencia de personal altamente instruido, sumado a la intrincada gestión del EEM, establece restricciones que podrían, de hecho, mermar su efectividad. Estas limitaciones dejan claro la necesidad imperativa de un órgano rector para la Guerra Electrónica, brindando soporte a la conducción operativa, una propuesta expuesta por Marrupe Pereyra (2014); este enfoque favorece la interoperabilidad, la coherencia en la doctrina y, la centralización de la planificación. El impacto de la Guerra Electrónica (GE) en las operaciones militares conjuntas demuestra una habilidad primordial, la de obtener superioridad informativa sobre el enemigo. Esto minimiza la incertidumbre y expande el margen de maniobra para el comandante, traduciéndose en aumentar su libertad de acción. En los ambientes actuales en donde se destacan los grandes avances tecnológicos el correcto empleo de la GE permite neutralizar las fortalezas del enemigo sin recurrir necesariamente al empleo de fuegos letales. En consecuencia, la evolución constante de la GE nos indica que son actividades indispensables para sostener la iniciativa propia resguardando a su vez la seguridad de las fuerzas amigas. Su desarrollo, modernización y doctrina deben ser considerados prioridades dentro de la planificación de la defensa nacional.

Capítulo II

La Ciberdefensa, estrategias y tecnología. Evaluando la efectividad en la protección de las infraestructuras críticas.

Este capítulo tiene por objetivo analizar el ciberespacio como uno de los dominios de las operaciones militares, identificando sus características y alcances en el contexto de la acción militar conjunta. En la actualidad, donde la información se ha convertido en un activo clave para el logro de los objetivos militares, el control del ciberespacio cobra una importancia crucial tanto para la defensa como para la proyección del poder de combate. Entender su funcionamiento es clave para saber cómo evoluciona la guerra y su influencia en las tácticas actuales. A lo largo de este capítulo se nombrarán las capacidades y las distintas clases de operaciones cibernéticas, distinguiendo las acciones ofensivas, defensivas y de apoyo, además de su vinculación con los objetivos operacionales. También se analizará la integración del ciberespacio dentro del planeamiento y la conducción militar conjunta, resaltando la importancia de sincronizar sus efectos con los de otros dominios, en especial el dominio electromagnético.

Sección I

Conceptualización del Ciberespacio en el ámbito militar

A lo largo de los siglos, las innovaciones tecnológicas influyeron de manera directa y elocuente en la forma en la que se libran las guerras y en sus resultados. Por lo tanto, los conflictos armados son los que provocan de manera indefectible cambios en las doctrinas de seguridad y defensa de los diferentes Estados. El contexto actual presenta nuevas amenazas que en el pasado no existían, aunque también presenta oportunidades que antes hubieran sido imposibles. Los conflictos de hoy en día requieren de estrategias y de políticas coherentes con una era en donde predomina el aspecto científico y tecnológico por sobre los demás, en la que se combatirá en diversas dimensiones al mismo tiempo frente a un enemigo con capacidades similares. Es así como llegamos a las Operaciones Multidominio (MDO) que son una respuesta a esta realidad, permitiendo conseguir una superioridad frente a un enemigo a partir del control, coordinación y conexión entre las dimensiones de combate clásicas, añadiendo el dominio electromagnético y el dominio cibernético (Alonso, 2023).

Allá por el año 2015 el Subsecretario de Defensa de los Estados Unidos de Norteamérica Bob Work en el US Army War College, describió los problemas que crearía la guerra del siglo XXI y las soluciones que requeriría.

> Este concepto debería permitir al ejército de los Estados Unidos luchar y ganar, después de irrumpir en el teatro y romper defensas de Anti Acceso / Negación de Área (A2/AD) del enemigo. Según sus palabras, el campo de batalla se había expandido. La combinación de municiones guiadas de largo alcance y de la guerra informativa eran las variables críticas para el éxito militar en la guerra del siglo XXI. Afirmó que la guerra informativa era la combinación de guerra cibernética, electrónica, operaciones de información, engaño y negación que el enemigo emplearía para interrumpir nuestra función de mando y control y obtener ventaja en el ciclo de decisión.
>
> El hecho de que el Sr. Work destacara batalla aeroterrestre proporcionó un punto de partida para que se empezase a pensar en la idea de sinergia entre dominios, de tal manera que cada uno mejoraría la efectividad y compensaría las vulnerabilidades de los demás. En su implementación ideal, sería la fuerza conjunta la que actuaría de manera óptima, como una sola fuerza. (León, 2023)

En este entorno cada vez más complejo sumado a una constante evolución tecnológica en donde se destacan los avances informáticos, entre otros, es cuando toma vital importancia el dominio cibernético. Dominio en donde se libra la guerra cibernética que como nos menciona (Trama, 2017) difiere fundamentalmente del conflicto armado tradicional pues a diferencia de la conducción de la guerra en el pasado, los oponentes pueden librarla de manera rápida, económica, anónima y devastadora, desde lugares apartados del globo.

Esta revolución tecnológica en constante crecimiento enmarcada en un mundo totalmente digitalizado ofrece grandes ventajas, pero también importantes riesgos que deben ser atacados con eficacia para tratar de reducir al máximo problemas de seguridad y defensa.

Los cambios producidos en el ciberespacio suelen estar impulsados por la investigación y el desarrollo de la industria privada, lo que lo hace dinámico y en constante crecimiento a medida que las capacidades de la tecnología se expanden y evolucionan.

Paez (2014) nos menciona que dado el alcance global que tiene el ciberespacio, un comando conjunto de ciberdefensa encuentra su ámbito de aplicación en la información y las infraestructuras críticas que tengan algún impacto sobre la fuerza desplegada en un teatro de operaciones. Las tareas y capacidades que se asocian a un comando conjunto de ciberdefensa deben buscar garantizar el libre acceso, establecer un ámbito seguro y obtener y mantener la superioridad en el ciberespacio durante las operaciones para que el comandante operacional mantenga su comando y control y conduzca a sus fuerzas en la campaña.

Ahora bien, estas operaciones que mencionamos anteriormente se pueden describir como el empleo de las capacidades ciberespaciales cuyo propósito principal es alcanzar objetivos en o a través el ciberespacio, estas operaciones, se pueden dividir en tres grandes grupos: operaciones ofensivas, operaciones defensivas y operaciones de la red de información del Departamento de Defensa.

Capacidades y tipos de operaciones cibernéticas

El ciberespacio se ha convertido en un campo de batalla más, esto obligó a crear nuevas destrezas militares centradas en actuar dentro y fuera de él. Las operaciones cibernéticas, son aquellas maniobras programadas y llevadas a cabo, para alcanzar objetivos militares tácticos, operacionales y estratégicos, aprovechando los recursos digitales, los sistemas informáticos, y las redes de comunicaciones. En la doctrina establecida por el Departamento del Ejército de los Estados Unidos, estas capacidades se estructuran en tres categorías principales: operaciones ofensivas, defensivas y de apoyo (Odierno, 2014).

Así mismo, el Ministerio de Defensa de Gran Bretaña en su Nota de Doctrina Conjunta 1/18 nos menciona que las operaciones cibernéticas se pueden dividir en: operaciones cibernéticas ofensivas, operaciones cibernéticas defensivas, ciberinteligencia, vigilancia y reconocimiento y por último operaciones cibernéticas de preparación del entorno.

Las operaciones ofensivas buscan proyectar poder en el ciberespacio, degradando, interrumpiendo o destruyendo capacidades enemigas a través de ataques dirigidos contra sus sistemas de información o infraestructura crítica

(Scott, 2018). Por su parte, las operaciones defensivas se orientan a proteger la integridad, disponibilidad y confidencialidad de los sistemas propios, anticipando y neutralizando intentos de intrusión o explotación del adversario. Finalmente, las operaciones de apoyo incluyen las actividades de reconocimiento, vigilancia y análisis digital que proporcionan información esencial para la toma de decisiones.

En el contexto de la acción militar conjunta, estas capacidades se articulan dentro de un marco doctrinario que busca sincronizar los efectos cibernéticos con otras dimensiones del combate, como la Guerra Electrónica, la inteligencia y las operaciones de información. La eficacia de su empleo depende tanto de la integración tecnológica como del planeamiento conjunto, factores que determinan la posibilidad de obtener y mantener la superioridad en este dominio durante el desarrollo de las operaciones.

Sección II

Integración del ciberespacio con la Acción Militar Conjunta

El reconocimiento del ciberespacio como dominio operacional ha modificado la estructura tradicional de la conducción militar, lo que lleva necesariamente a que se integre dentro del planeamiento y la ejecución de manera conjunta. En este escenario, las operaciones cibernéticas ya no son un componente aislado, sino que son capaces de afectar a todos los otros dominios que influyen en el ambiente operacional. Su influencia en todos los niveles de maniobra es evidente y son inevitables las coordinaciones con otras operaciones militares como la Guerra Electrónica, la Inteligencia y las Operaciones de Información. Esta integración busca generar efectos sincronizados y sostenidos que contribuyan a alcanzar los objetivos de la acción militar conjunta.

> Dada la dependencia del Ejército del Ciberespacio, así como del Espectro Electromagnético, los comandantes integran plenamente las actividades cibernéticas/electromagnéticas dentro de la operación general. Estas actividades emplean un enfoque de armas combinadas para las operaciones en un dominio ciberespacial en disputa y un espectro electromagnético congestionado. Las actividades cibernéticas/electromagnéticas aprovechan, retienen y explotan ventajas en el ciberespacio y el espectro electromagnético. El resultado permite a las fuerzas del Ejército conservar la libertad de acción mientras se niega la libertad de acción a

enemigos y adversarios, permitiendo así la operación general. (Soesanto, 2021).

Doctrina británica de los últimos años hace hincapié en la necesidad de incluir las Actividades Cibernéticas y Electromagnéticas (CEMA) en la planificación de nivel operacional. Esto, usando estructuras de coordinación a medida, asegurando la coherencia en los efectos cibernéticos y electromagnéticos. El documento del Reino Unido (Defence, 2018) sugiere que integrar efectivamente las capacidades CEMA demanda un entendimiento unificado del campo de batalla. Además, requiere un control centralizado para las operaciones, permitiendo una ejecución descentralizada según la decisión que adopte el comandante. Siguiendo esta línea, (Odierno, 2014) y (JCS, 2012), del Departamento de Defensa de los Estados Unidos de Norteamérica, definen la importancia de organizar las operaciones cibernéticas dentro de planes conjuntos, promoviendo la interoperabilidad técnica y doctrinal.

Considerando reglamentaciones conjuntas del Ejército Argentino como (EMCFFAA, 2012) podemos encontrar que se establece la necesidad de coordinar las capacidades de Guerra Electrónica con las del dominio Cibernético. Favoreciendo de esta manera la formación de órganos de planeamiento integrados, liderados por el Estado Mayor Conjunto. Tal convergencia, que todavía se encuentra en desarrollo, es un paso fundamental para lograr una conducción integral del multidominio en donde el Ciberespacio y el Espectro Electromagnético se unen siendo instrumentos fundamentales para controlar, negar, explotar la información.

Impacto del ciberespacio en la conducción operacional moderna

El empleo del ciberespacio dentro del diseño operacional amplía el campo de acción del comandante, permitiéndole anticipar, condicionar y modificar la conducta del adversario mediante efectos no cinéticos, de alcance global y con impacto inmediato (Encina, 2019).

La inclusión de este dominio como un plano más en el que se puede librar la batalla ha alterado, como se mencionó anteriormente en este mismo capítulo, la visión clásica de la conducción militar. Resultando en un ámbito donde la información la rapidez y la interconexión dictan el curso de las maniobras

militares. En este nuevo contexto, las operaciones ya no se limitan a los efectos físicos, sino que se extienden al plano virtual, donde la capacidad de influir, negar o explotar información se convierte en un factor decisivo para la obtención de la superioridad operacional.

Las operaciones en el ciberespacio son, por naturaleza, conjuntas, y amplían la capacidad del comandante para proyectar poder, influir sobre los adversarios y moldear el entorno operacional sin las limitaciones de la geografía física (Scott, 2018).

El impacto del ciberespacio en la conducción operacional se manifiesta en múltiples dimensiones. Desde el punto de vista doctrinario, obliga a revisar los principios de la maniobra y de la concentración del esfuerzo, integrando el concepto de efectos simultáneos en todos los dominios. Desde la perspectiva de la organización, se necesita establecer áreas conjuntas para que la planificación y ejecución de las operaciones cibernéticas se puedan realizar de manera coordinada entre todos los integrantes de las Fuerzas Armadas (Ejército, Armada y Fuerza Aérea). Finalmente, en el plano estratégico, redefine el equilibrio entre la acción militar y los instrumentos del poder nacional, al permitir la proyección de fuerza sin presencia física y con consecuencias globales.

El florecimiento de disputas actuales mediante el aumento de tensiones recientes exhibe que el ciberespacio incide directamente en la toma de decisiones, la conexión entre agencias y el sostenimiento del esfuerzo operacional. La experiencia del conflicto Rusia-Ucrania, muestra con certeza cómo las operaciones cibernéticas complementan y, a su vez, influyen sobre las maniobras convencionales, desencadenando efectos que van más allá del simple campo de batalla físico, tal cual lo conocemos. Por ende, el ciberespacio se reafirma como una herramienta crucial en la dirección moderna; aquí la aptitud para maniobrar, resguardar y subsistir en este dominio se transforma en un requisito obligatorio para la acción militar conjunta actual.

Conclusiones Parciales del Capítulo II

El ciberespacio, que emerge como un novedoso campo de batalla en las operaciones militares, cada vez gana más importancia, impactando en todos los niveles de la conducción militar. La hegemonía en esta área exige el forjamiento de capacidades ofensivas, defensivas y de soporte, todas entrelazadas en una doctrina conjunta lo que es esencial para garantizar la supremacía en la obtención de la información frente a la del adversario sin, a su vez, comprometer la propia libertad de acción.

La integración del ciberespacio en la acción militar conjunta, a su vez, exige una convergencia coordinada entre sus múltiples componentes. Sincronizar los medios, garantizar la interoperabilidad, junto con la utilización combinada de las capacidades cibernéticas y electromagnéticas; estos son factores cruciales para alcanzar la eficiencia operativa.

Finalmente, las operaciones en el ciberespacio redefinen la naturaleza del conflicto, extendiendo sus efectos más allá del terreno físico. Su impacto en el ritmo de acción, la maniobra estratégica, y la formulación de decisiones constata que el ciberdominio ya no se observa como apoyo complementario, sino como un factor crucial en la dirección moderna de las operaciones militares.

Capítulo III

Integración y diferencia entre la Guerra Electrónica y la Ciberdefensa en el Ámbito Operacional Conjunto

El presente capítulo tiene por objetivo analizar la relación que existente entre la Guerra Electrónica y la Ciberdefensa en el nivel operacional conjunto, identificando los puntos donde convergen ambas capacidades y como eso fortalece la efectividad del instrumento militar. En este ambiente operacional muy influenciado por la tecnología y en donde es cada vez mas difícil hacer frente a la expansión de los dominios de conflicto, es clave entender cómo la integración de estas capacidades ayuda a potenciar la acción militar conjunta garantizando la superioridad en la obtención de la información ante las amenazas híbridas. A lo largo del capítulo, exploraremos los pilares doctrinales claves detrás de la conexión estratégica entre la Guerra Electrónica y la Ciberdefensa, usando las perspectivas estadounidenses, británicas y nacionales como base. Analizaremos las fortalezas compartidas de estos campos, y como se entrelazan en la planificación conjunta, además de los obstáculos para su implementación en el campo de batalla.

Sección I

Capacidades complementarias y áreas de convergencia operativa

La integración entre la Guerra Electrónica (GE) y la Ciberdefensa es uno de los pilares del accionar militar de hoy en día. Ambas capacidades, aunque trabajan en dominios distintos, comparten un mismo propósito: garantizar la superioridad de la información por sobre la del enemigo y la libertad de acción del comandante en todos los niveles de la conducción. Como lo hemos desarrollado anteriormente en este trabajo de investigación la GE actúa sobre el espectro electromagnético, mientras que la Ciberdefensa lo hace sobre las redes y sistemas digitales. Sin embargo, el punto de contacto entre ambas se da en la necesidad de dominar el flujo de información, detectar, negar o explotar las capacidades del adversario, y proteger las propias infraestructuras críticas del sistema de fuerzas.

Con respecto a la conducción de la GE encontramos en doctrina del Ejército Argentino que:

> "En tiempo de paz, será responsabilidad del nivel estratégico militar, desde el ámbito conjunto, la conducción de las acciones de guerra electrónica, para evitar incidentes e implicancias de orden internacional, lograr la confluencia de esfuerzos, incrementar el intercambio de información, disminuir costos, determinar acciones y procedimientos, y definir la protección electrónica que deberán poseer los sistemas de comunicaciones y el tipo o características de los sistemas de armas y los equipos que ejecutarán las tareas de apoyo de guerra electrónica (AGE) y de ataque electrónico (AE) para el apoyo a las operaciones tácticas." (DGOD, 2017).

En la doctrina que utilizamos para el desarrollo de este trabajo encontramos que la Guerra Electrónica se la puede dividir en tres acciones fundamentales: Ataque Electrónico (AE), Protección Electrónica (PE) y Apoyo de Guerra Electrónica (AGE). El Ataque Electrónico consiste usar la energía electromagnética para atacar instalaciones / equipamiento del adversario la cual busca degradar, neutralizar o destruir el empleo del espectro por parte del enemigo. La Protección Electrónica tiene como finalidad preservar el uso propio del espectro ante las acciones del oponente, incorporando técnicas de resistencia, contramedidas y gestión eficiente de frecuencias. Por su parte, el Apoyo Electrónico se orienta en la búsqueda, identificación y localización, entre otras, de emisiones electromagnéticas para contribuir al reconocimiento y seguimiento de amenazas presentes en el Espectro Electromagnético y proporcionar la información necesaria para la planificación y conducción de futuras operaciones. Estas acciones realizan un aporte directo al proceso de toma de decisiones, aportando información crítica para la maniobra.

Paralelamente, la Ciberdefensa se organiza en tres áreas funcionales comparables. Estas son: Operaciones Cibernéticas Ofensivas, Operaciones Cibernéticas Defensivas y Operaciones de Apoyo en el Ciberespacio. Las Operaciones Cibernéticas Ofensivas tratan de afectar las redes y sistemas del enemigo, buscando disuadirlo o neutralizarlo; las Operaciones Cibernéticas Defensivas se concentran en resguardar activamente los propios sistemas; mientras que las Operaciones de Apoyo en el Ciberespacio trabajan para garantizar la integridad y disponibilidad de las redes de información del aparato militar (Scott, 2018). Dentro de este planteamiento, la manera en que se utilizan es similar a la de la Guerra Electrónica: se pretende impedir el uso del entorno al

adversario, mantener la operatividad propia y aprovechar la información disponible para tomar decisiones. Esta conexión funcional ayuda a desentrañar un área donde convergen operaciones entre Guerra Electrónica (GE) y Ciberdefensa. Cada una demanda un entendimiento profundo del ámbito electromagnético y cibernético, eso también incluye el empleo de sensores, software para detectar, además de técnicas de interferencia y resguardos activos. En cuanto a lo operacional, esta unión abre el camino a planificar actos conjuntos en el espectro y las redes, a la par que se sincronizan efectos aumentando así la eficiencia de las acciones combinadas. La doctrina del ejército de los Estados Unidos de Norteamérica define este enfoque bajo el concepto de Cyber-Electromagnetic Activities (CEMA), allí la coordinación de los dos dominios propicia un beneficio significativo en la contienda informativa (Odierno, 2014).

Desde la óptica nacional, la lección que aprendimos de las doctrinas nos indica que urge una articulación similar. De Vergara (2016), insiste en ello, que integrar la Guerra Electrónica con la Ciberdefensa, en el ámbito operacional conjunto, es clave para encarar situaciones intrincadas, donde la tecnología nos une, y a su vez, expone nuestras infraestructuras más importantes. Este punto de vista lo refuerza Marrupe (2014) quien subraya la relevancia de idear una entidad líder en Guerra Electrónica, que trabaje con las estructuras de Ciberdefensa, para tener una dirección unificada sobre el espectro y el ciberespacio, en su conjunto.

Sección II

Integración de la GE y la Ciberdefensa en la planificación y conducción conjunta

La moderna conducción de las operaciones conjuntas exige, sin duda, una integración real de todas las capacidades que ofrecen las Fuerzas Armadas, sobre todo en aquellas que impactan en los dominios no convencionales, como el ciberespacio y el espectro electromagnético. La Guerra Electrónica (GE), junto a la Ciberdefensa, se deben ver como piezas que van juntas en el plan operacional, logrando efectos combinados que ayudan a la maniobra y garantizan la ventaja de la información. La unión entre estas áreas no solo implica que los medios funcionen simultáneamente, sino que necesitan de una unidad de mando que permita sincronizar acciones y evitar interferencias mutuas en el desarrollo de las operaciones.

Desde una perspectiva doctrinal, la planificación conjunta precisa incluir la Guerra Electrónica (GE) y la Ciberdefensa desde el mero comienzo del proceso de conducción. La doctrina británica y estadounidense lo dejan sumamente en claro en sus manuales (CEMA), que es ahí donde se manifiesta la urgente necesidad de integrar operaciones cibernéticas, guerra electrónica, y la administración del espectro en la planificación operacional. Según estos reglamentos de países integrantes de la Organización del Tratado del Atlántico Norte (OTAN), las Actividades Cibernéticas Electromagnéticas (CEMA) actúan como órganos de asesoramiento del comandante, asegurando la coordinación de los efectos cibernéticos y electromagnéticos a lo largo de todas las fases de la operación.

A nivel nacional (EMCFFAA, 2012) subraya, la importancia de integrar la Guerra Electrónica, en el planeamiento conjunto, marcando su intervención desde el análisis del ambiente operacional hasta la ejecución de la operación. Este reglamento, realmente, fundamenta una integración, paso a paso, con las nuevas capacidades que surgen del espacio cibernético impulsando una conducción, que tenga en cuenta el dominio de la información en su totalidad. Por otro lado, (DGOD, 2017) destaca, que es indispensable la coordinación en el mando, sobre las áreas de comunicaciones, informática y guerra electrónica, identificando la interrelación técnica entre esos subsistemas. Lo que nos conduce a que su aplicación práctica, a nivel operacional, permite observar una arquitectura de mando que se alinea con un enfoque conjunto.

La doctrina analizada ofrece igualmente ejemplos valiosos para guiar este desarrollo. El documento británico (Defence, 2018) destaca que una integración eficaz de las capacidades CEMA depende de tres pilares: un entendimiento común del entorno operacional, un mando centralizado, y una ejecución que descentralizada. Esta visión pretende que los efectos tanto en el ciberespacio como en el espectro electromagnético sean coherentes con la intención del comandante, así se evitan solapamientos, y se fomenta la sincronización de las maniobras.

A nivel operacional, la coordinación GE–Ciberdefensa debe concretarse a través de un sistema de planeamiento que tenga en cuenta tres puntos claves: el análisis integral del ámbito informacional, la identificación de objetivos comunes

y la distribución flexible de recursos, técnicos y humanos. Esa integración, no sólo optimiza la eficiencia al emplear recursos, sino que aumenta la habilidad de reaccionar contra amenazas híbridas. Especialmente en situaciones donde el límite entre el espacio cibernético y el electromagnético es confuso. Tal como nos manifiesta De Vergara (2017), el cambio del campo de batalla requiere estructuras de mando que permitan el control simultáneo sobre estos dos dominios. El fin es resguardar la libertad de acción del comandante y garantizar la continuidad de las operaciones conjuntas.

En este sentido, la planificación combinada entre Guerra Electrónica y Ciberdefensa no es solo un juntar de capacidades de distintos dominios, sino lo que se busca es lograr una sinergia para producir efectos e influir de esta manera la percepción, decisión, y capacidades del oponente. El reto está en crear procedimientos estandarizados, con buena interoperabilidad y doctrinas firmes para que haya cohesión en el funcionamiento de las fuerzas conjuntas, con ejecución flexible, tanto en escenarios nacionales como, así también, en operaciones con fuerzas aliadas.

Impacto de la sinergia GE–Ciberdefensa en la acción militar conjunta

Como hemos venido desarrollando, la conjunción entre la Guerra Electrónica (GE) y la Ciberdefensa marca un gran cambio en cómo debemos entender y conducir la acción militar conjunta. La cohesión entre estos dominios nos facilita la obtención de efectos en simultáneo sobre el espectro electromagnético y el ciberespacio, abriendo el campo en donde se realizan las operaciones y ofreciendo al comandante una herramienta más flexible y versátil para el combate actual. Integrar estas actividades nos permite trabajar de manera coordinada sobre la información, los sistemas y las comunicaciones del enemigo, cuidando nuestros recursos. Así, la sinergia GE–Ciberdefensa se consolida como un multiplicador del poder de combate, posibilitando el cambio del ritmo de combate, el alcance y la fuerza de las operaciones en conjunto.

En la actualidad la coordinación entre GE y Ciberdefensa se manifiesta en tres sectores bien diferenciados y que producen un gran impacto. Hablamos del plano de la toma de decisiones, del plano de la organización y por último el plano netamente de la técnica. En la dimensión de la toma de decisiones, disponer de

toda la información procesada en tiempo real mediante el AGE y el monitoreo cibernético brinda al comandante una visión más completa, algo que le permite prever movimientos del enemigo y adaptar su plan con datos válidos. Con respecto a la organización, la integración de los equipos de GE y Ciberdefensa en los puestos comando ayuda a tomar decisiones de manera descentralizadas, así como la utilización de diferentes capacidades de forma rápida según cambie el rumbo de la operación. Finalmente, técnicamente la compatibilidad de sensores, software y sistemas para la administración del espectro facilita responder antes las interferencias, intrusiones o ataques híbridos, reforzando la resiliencia del sistema de comunicaciones y mando.

En línea con lo anteriormente expresado el manual del Departamento del Cuartel General del Ejército de los Estados Unidos "Cyber Electromagnetic Activities." (2014) nos dice que:

> "Las actividades CEMA integran y sincronizan las operaciones en el ciberespacio, la guerra electrónica y las operaciones de gestión del espectro para apoyar las operaciones terrestres unificadas.
>
> Los comandantes emplean las actividades CEMA para coordinar, integrar y sincronizar efectos a través de los dominios cibernético y electromagnético, con el fin de crear múltiples dilemas para el enemigo y proteger las capacidades propias." (Odierno, 2014).

La verdadera ventaja del trabajo integrado entre estos dominios está en la posibilidad de producir efectos sincronizados, que no solo buscan mermar las capacidades del enemigo, sino que también buscan proteger las de nuestra fuerza. En este contexto, la Guerra Electrónica y la Ciberdefensa, al operar juntas, logran mantener el ciclo para la toma de decisiones mediante la Observación, Orientación para finalmente Decidir y Actuar (ODDA) a nuestro favor, incluso bajo condiciones de denegación o saturación del espectro. De esta manera se logra maximizar el flujo de información y a su vez disminuir los tiempos de decisión, provocando una aceleración en la velocidad operativa, un factor clave en el combate de hoy.

Desde una perspectiva nacional basada en doctrina específica del Ejército Argentino como doctrina conjunta y publicaciones militares, subrayan, que la

articulación de ambas disciplinas es lo que verdaderamente fortalece la capacidad del instrumento militar para operar de forma sostenida, en entornos en donde prima lo técnico. Estos documentos señalan la necesidad crucial de desarrollar doctrinas procedimientos y medios que aseguren el control del entorno de la información afianzando así la autonomía de decisión y, la integridad del sistema de fuerzas. A la vez, autores como Marrupe (2014) y Vergara (2016) hacen hincapié en que, la integración de órganos directores especializados permitiría una conducción más coherente y eficiente, eliminando superposiciones funcionales y por último asegurando una unidad de propósito en la gestión del espectro y las redes.

Conclusiones Parciales del Capítulo III

La integración entre los dominios de Guerra Electrónica y de Ciberdefensa, se afianzó como una necesidad operativa para hacer frente a uno de los escenarios más desfavorables que se pueden presentar que son los ataques cibernéticos dentro de un escenario bélico en constante cambio, sumada a una dependencia tecnológica en crecimiento. Lejos de ser vistas como actividades de funcionamiento estanco, estas se complementan para asegurar la libertad de acción y mantener la superioridad en la gestión de información para la Fuerza en todos los niveles de la conducción.

La doctrina analizada en este capítulo nos deja una enseñanza sumamente importante, la integración entre los dominios del ciberespacio y de la guerra electrónica nos permite aumentar el impacto en las operaciones militares modernas. Esta combinación hace posible coordinar efectos cuasi en tiempo real, afectando los sistemas del enemigo, su información, comunicaciones y su proceso de toma de decisiones. Por otro lado, el trabajo combinado de estos dominios nos permite asegurar el normal funcionamiento de nuestro propio sistema defensivo, con medidas de protección y detección, todo bajo la centralización de comando.

Desde una visión nacional, los documentos de doctrina que fueron analizados en el presente capítulo nos muestran la necesidad de continuar trabajando hacia un modelo de planeamiento conjunto entre las Fuerzas Armadas, que abarque de manera integral estos dominios emergentes. Estableciendo estructuras de coordinación permanentes, normalizando los procedimientos, y

garantizando la interoperabilidad entre los diversos componentes que emergen como requisitos de gran importancia para reforzar un sistema de defensa preparado ante las exigencias de los conflictos del siglo XXI.

La sinergia GE–Ciberdefensa redefine la acción militar conjunta al introducir una nueva lógica de conducción basada en la información como centro de gravedad. Su incorporación en la planificación y posterior ejecución en el campo de combate permitirá a las Fuerzas Armadas no solo actuar con mayor flexibilidad y precisión, sino también anticipar, prevenir, conjurar, proteger y dominar los espacios donde hoy se decide la superioridad estratégica: el ciberespacio y el espectro electromagnético.

CONCLUSIONES

El estudio propuesto a lo largo de este Trabajo Final Integrador revela un progreso continuado en la comprensión de la doctrina en la acción militar conjunta. La Guerra Electrónica y la Ciberdefensa, que emergieron de manera separada, han dejado de ser capacidades complementarias, para consolidarse en herramientas fundamentales que determinan la eficacia del sistema de defensa en el combate moderno. El control sobre la información, en todas sus facetas, se consolida como el nuevo centro de gravedad en los conflictos actuales. Esto define el ritmo de las operaciones militares y la toma de decisiones por parte del comandante.

La confluencia del Espectro Electromagnético y el Ciberespacio se constituye como el núcleo fundamental de la conducción en las operaciones de multidominio. Combinar las actividades de Guerra Electrónica y Ciberdefensa, permite a las Fuerzas Armadas planificar efectos integrados, operando de manera simultánea y manteniéndose a lo largo del tiempo, lo cual mejora la capacidad de maniobra y debilita la exposición frente a las amenazas híbridas. Tal sinergia, cimentada en un mando cohesionado y estructuras de coordinación constantes, muestra el avance obligatorio hacia una doctrina conjunta que responda a la evolución tecnológica y operacional del siglo XXI.

Desde una óptica nacional el análisis de la doctrina tanto específica como conjunta y trabajos de investigación anteriores evidencian una imperiosa exigencia de reforzar el planeamiento conjunto, además de impulsar el desarrollo de capacidades propias y consolidar un marco normativo que unifique los esfuerzos en los dominios cibernético y electromagnético. La constitución de un órgano rector con la responsabilidad de articular la planificación, el adiestramiento y la gestión de estas destrezas permitiría acrecentar la resiliencia del instrumento militar asegurando una reacción eficaz ante amenazas complejas.

Por último, la integración de las actividades de Guerra Electrónica y la Ciberdefensa marcan una transformación elemental en la forma de entender la

acción militar conjunta. Esta conjunción no solo reconfigura la forma de ejecutar las operaciones militares, sino que también necesariamente modifica la manera de planificar y de gestionar la defensa nacional. La información pasa a ser el eje central para la toma de decisiones requiriendo de una coordinación entre las fuerzas, como requisito indispensable. Urge desarrollar capacidades conjuntas en lo doctrinario técnico y humano, una necesidad estratégica para que Argentina conserve la iniciativa y responda eficientemente a las amenazas del panorama bélico actual.

Bibliografía

Reglamentos

Comando de Operaciones Navales; Armada Argentina. (1998). *Procedimiento para las Operaciones de Guerra Electrónica*; RO-2-030. Buenos Aires.

DGOD. (2017). *ROD – 05 – 01 "Conceptos Básicos sobre los Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza".* Buenos Aires: Ejército Argentino.

EMCFFAA. (2012). *Guerra Electrónica para la Acción Militar Conjunta; PC 13 – 50.* Buenos Aires.

Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina. (2021). *Seguridad de la Información*; PC 22-01. Buenos Aires.

Publicaciones / Tesis

Alaniz Miranda, O. (2023). *Las actividades electromagnéticas: un enemigo invisible.* Centro de estudios e investigaciones militares de Chile. Santiago de Chile, Chile: Escenarios Actuales.

Alonso, J. (2023). *Operaciones Multidominio*. El nuevo carácter de la guerra. Madrid, Ministerio de Defensa.

Casarino, P. G. (2019). *La Ciberdefensa y la Ciberinteligencia Militar.* Buenos Aires, Argentina: Vision Conjunta Nro 21.

Chiavaro, G. D. (2018). *La influencia de la Guerra Electrónica en el diseño operacional.* Buenos Aires: Trabajo Final Integrador. Escuela de Guerra Conjunta de las Fuerzas Armadas.

EMCO, B. I. (2023). *Conceptos generales sobre la concepción estratégica de "Capas, Restricción de Áreas y de Operaciones Multidominio".* Buenos Aires: EMCFFAA.

Feickert, A. (2021). *Defense Primer: Army Multi-Domain Operations (MDO).* Congressional Research Service.

Gutiérrez de León, B. (2023). *Las Operaciones Multidominio*. Los motores de cambio de la seguridad y la defensa. Zaragoza, Ministerio de Defensa.

Herrera, A. O. (2017). *Diseño y planificación de las actividades de Guerra Electrónica en el Ambiente Operacional.* Buenos Aires: Trabajo Final Integrador. Escuela de Guerra Conjunta de las Fuarzas Armadas.

Hoffman, F. (2007). *Conflict in the 21th Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute for Policy Studies.

JCS. (2012). *Electronic Warfare*. Joint Publication 3-13. 1.

Lind, W. S. (2005). *Comprendiendo la Guerra de Cuarta Generación.* Military Review.

Marrupe Pereyra, A. I. (2014). *Diseño de un órgano director de guerra electrónica en apoyo al comando de nivel operacional.* Buenos Aires: Trabajo Final Integrador. Escuela de Guerra Conjunta de las Fuerzas Armadas.

Meza, M. S. (2012). *El Espectro Electromagnético.* Lima: Revista Big Bang Fautiniano.

Paez, E. P. (2014). *La Guerra Cibernética en el Nivel Operacional.* Buenos Aires, Argentina: Trabajo Final Intregrador. Estado Mayor Conjunto de las Fuerzas Armadas.

Odierno, R. T. (2014). *FM 3-38 Cyber Electromagnetic Activities.*Washington. Department of de Army.

Scott, K. D. (2018). *Cyberspace Operations.* Joint Publication 3-12

Soesanto, E. (2021). *A Digital Army: Synergies on the Battlefield and the Development of Cyber Electromagnetic Activities (CEMA)*. Zurich: Center for Security Studies (CSS).

Steingartner, W. (2021). *Cyber Threats and Cyber Deception in Hybrid Warfare.* Acta Polytechnica Hungarica.

Trama, G. A. (2017). *Operaciones Cibernéticas. Su naturaleza, propósito y conducción.* Buenos Aires, Argentina: Vision Conjunta Nro 17.

Defence, U. M. (2018). *Cyber and Electromagnetic Activities.* Joint Doctrine Note 1/18.

Uzal, R. (2012). *Guerra Cibernética: ¿Un desafio para la Defensa Nacional?* Buenos Aires, Argentina: Vision Conjunta Nro 7.

De Vergara, E. (2017). *Operaciones Militares Cibernéticas: Planeamiento y ejecución en el Nivel Operacional.* Buenos Aires: Visión Conjunta.

Wilson, C. (2007). *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.* Congressional Research Service.