MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

TEMA:

Integración de las Operaciones de Guerra Electrónica y Ciberdefensa en el ámbito para la Acción Militar Conjunta.

TÍTULO:

Las actividades ciberelectromagnéticas de la Acción Militar Conjunta bajo la concepción de Operaciones Multidominio.

Navarro, Claudio Alejandro

Año 2025

RESUMEN

El presente trabajo analiza la problemática de la integración de las actividades ciber-electromagnéticas en el nivel operacional, a partir del estudio de doctrinas y experiencias internacionales desarrolladas entre 2014 y 2024.

El objeto de estudio se centra en la convergencia entre la Guerra Electrónica y la Ciberdefensa en el marco de las Operaciones Multidominio, y el propósito principal es diseñar un marco conceptual y un modelo operativo que contribuyan a fortalecer la superioridad informacional y la interoperabilidad conjunta en la acción militar.

Desde el punto de vista teórico, la investigación se apoya en doctrinas y marcos conceptuales desarrollados por potencias militares que han avanzado en la integración ciber-electromagnética, así como en el enfoque contemporáneo de la guerra como fenómeno multidominio, en el cual la información y sus soportes se configuran como un centro de gravedad decisivo. Metodológicamente, se adopta un enfoque cualitativo, descriptivo y analítico, basado en el estudio de documentos doctrinarios y normativos, en el análisis comparado de experiencias operacionales recientes —con énfasis en los conflictos de Ucrania y Georgia— y en un diagnóstico preliminar de la situación argentina en materia de Guerra Electrónica y Ciberdefensa. La hipótesis de trabajo sostiene que la integración sinérgica de estas capacidades en un enfoque ciber-electromagnético concebido desde el nivel operacional mejora de manera significativa la capacidad de conducción, la resiliencia del sistema de mando y control y la eficacia de la acción militar conjunta.

Los resultados obtenidos permiten, en primer lugar, describir la evolución de la Guerra Electrónica y la Ciberdefensa hacia un enfoque integrado de actividades ciber-electromagnéticas y extraer principios doctrinarios y organizativos relevantes a partir de las experiencias internacionales estudiadas. En segundo lugar, el diagnóstico de la realidad nacional identifica avances y brechas en los planos doctrinario, organizativo, tecnológico y de recursos humanos. Finalmente, sobre esta base se propone un marco conceptual que concibe al ciberespacio y al espectro electromagnético como un entorno informacional único, y un modelo operativo para el nivel operacional argentino que

incorpora estructuras específicas ciber-electromagnéticas en los estados mayores, integra estas actividades en todo el ciclo de planeamiento y enfatiza la resiliencia informacional como condición para la maniobra en entornos multidominio, aportando lineamientos iniciales para orientar la modernización doctrinaria y la planificación conjunta en el ámbito nacional.

Palabras clave:

Guerra Electrónica – Ciberdefensa – Operaciones Multidominio – Nivel Operacional – Conflictos híbridos

ÍNDICE

RESUMEN 1

INTRODUCCIÓN 4

CAPÍTULO 1: MARCO CONCEPTUAL DE LAS ACTIVIDADES CIBER-ELECTROMAGNÉTICAS (CEMA) EN EL CONTEXTO DE LAS OPERACIONES MULTIDOMINIO 8

1.1 Evolución de la Guerra Electrónica y la Ciberdefensa 8

1.2 Relación entre el Ciberespacio y el Espectro Electromagnético..... 11

1.3 Importancia estratégica de la integración en Operaciones Multidominio 14

CAPÍTULO 2: ANÁLISIS COMPARATIVO DE DOCTRINAS INTERNACIONALES Y EXPERIENCIAS OPERACIONALES 18

2.1 Doctrinas de Estados Unidos y Reino Unido….....18

2.2 Estudio de casos prácticos: Conflictos en Ucrania y Georgia..... 23

2.3 Implicaciones para la planificación operativa en Argentina. 28

CAPÍTULO 3: DISEÑO DE UN MARCO OPERACIONAL PARA LA INTEGRACIÓN DE GE Y CD EN ARGENTINA 31

3.1 Diagnóstico de las Capacidades Ciber-Electromagnéticas en Argentina.....31

3.2 Propuesta de modelo operativo: Sincronización de capacidades GE y CD….33

3.3 Aplicación práctica: Escenarios hipotéticos y lecciones para el nivel operacional.....36

CONCLUSIONES.....40

BIBLIOGRAFÍA 44

INTRODUCCIÓN

La transformación del entorno estratégico internacional en las dos últimas décadas ha generado un cambio profundo y sostenido en la forma en que los Estados conciben, organizan y conducen el poder militar[1]. Este proceso no se limita a la incorporación de nuevas tecnologías, sino que implica una reconfiguración estructural de las dinámicas de seguridad, del rol de los actores internacionales y del modo en que se despliegan las capacidades nacionales frente a situaciones de competencia interestatal, amenazas híbridas y disputas de carácter multidominio. La velocidad con la que circula la información, la dependencia creciente de sistemas digitales y la expansión de infraestructuras críticas interconectadas han configurado un escenario operacional radicalmente distinto al que predominó durante el último tercio del siglo XX. En este nuevo contexto, la distinción entre paz, crisis y conflicto se ha vuelto difusa, y la frontera tradicional entre los ámbitos militar y civil es cada vez más permeable, lo que obliga a las fuerzas armadas a comprender y operar en un entorno donde la simultaneidad y la interdependencia son rasgos centrales.

El acelerado avance tecnológico ha traído consigo un crecimiento exponencial del volumen, diversidad y velocidad de circulación de datos, lo que ha convertido a la información en un recurso estratégico tan relevante como los medios físicos tradicionales.[2] Las decisiones operacionales dependen, cada vez más, de la calidad y disponibilidad de la información, de su protección frente a interferencias externas y de la capacidad de explotarla para generar ventajas asimétricas. La centralidad de los sistemas de mando y control basados en infraestructura digital, la adopción de plataformas con enlaces permanentes y el empleo de sensores distribuidos en múltiples escalas y dominios han reforzado la importancia del flujo informacional como un factor decisivo para la

[1]Diversos autores señalan que el entorno estratégico posterior a la Guerra Fría se caracteriza por la difusión de capacidades, la centralidad de la información y el uso sistemático de instrumentos no militares en la competencia entre Estados (Reale, 2023; Quintana, 2016).

[2] Diversos documentos doctrinarios recientes señalan que la línea entre paz, crisis y conflicto se ha vuelto difusa y que la competencia se desarrolla de manera continua en todos los dominios, con un fuerte énfasis en la dimensión informacional (U.S. Army Training and Doctrine Command, 2018; Joint Chiefs of Staff, 2018; Hillebrand, 2023; North Atlantic Treaty Organization, 2024).

conducción de operaciones. Esta realidad configura un ambiente operacional caracterizado por la simultaneidad, la multidimensionalidad y la superposición de tácticas convencionales, híbridas y cognitivas, lo que exige repensar las herramientas, los procesos y los principios mediante los cuales las fuerzas planifican y ejecutan sus misiones.

Dentro de este proceso de reconfiguración estratégica, los dominios ciberespacial y electromagnético han adquirido una relevancia que excede ampliamente el ámbito técnico o especializado. Ambos se consolidaron como componentes esenciales de la competencia y el conflicto contemporáneo, pues albergan las infraestructuras críticas que sostienen las capacidades militares, económicas, sociales y gubernamentales de los Estados. La creciente dependencia de redes digitales, sensores avanzados, sistemas automatizados y enlaces persistentes ha permitido mejorar la eficiencia operativa, la velocidad del ciclo de decisión y la capacidad de proyección, pero también introdujo vulnerabilidades que pueden ser explotadas por actores estatales o no estatales con medios relativamente modestos pero con objetivos determinados. En consecuencia, asegurar la disponibilidad, integridad y resiliencia del ciberespacio y del espectro electromagnético se ha convertido en un requisito indispensable para garantizar la continuidad del funcionamiento estratégico y la libertad de acción operacional.

La profunda interrelación entre ambos dominios se intensificó a medida que las tecnologías de la información y las comunicaciones se integraron de manera transversal en los sistemas militares. Esta interdependencia llevó a que la distinción tradicional entre Guerra Electrónica (GE) y Ciberdefensa (CD) comenzara a diluirse no por pérdida de identidad funcional, sino por la necesidad operacional de coordinar efectos simultáneos para asegurar la ventaja informacional. Las capacidades electrónicas orientadas al control del espectro, así como las capacidades cibernéticas orientadas a la seguridad, disponibilidad y explotación de la información, dejaron de ser funciones autónomas para convertirse en componentes esenciales de un mismo entramado conceptual. Esta evolución doctrinaria, tecnológica y organizacional dio origen al concepto de actividades ciber-electromagnéticas, una categoría integradora destinada a coordinar capacidades, procesos y estructuras bajo un enfoque común alineado con la conducción moderna de operaciones en todos los niveles.

Los desarrollos doctrinarios de las principales potencias militares evidencian con claridad esta tendencia. La necesidad de coordinar efectos electrónicos y cibernéticos se incorporó gradualmente en los modelos de planeamiento operacional, en las arquitecturas

institucionales y en los manuales o reglamentos que guían la conducción de operaciones multidominio. Dichos avances no responden únicamente a mejoras tecnológicas, sino a un diagnóstico compartido: la disputa contemporánea por la información y por el control funcional de los sistemas críticos constituye un factor determinante de la competencia estratégica. La formulación doctrinaria de actividades ciber-electromagnéticas, en consecuencia, refleja la madurez de un proceso conceptual que reconoce que la superioridad física carece de valor si no se acompaña de la superioridad informacional, entendida como la capacidad de percibir, decidir y actuar con mayor velocidad, precisión y coherencia que el adversario.

Desde una perspectiva operacional, esta evolución implica que las fuerzas militares deben contar con estructuras capaces de analizar el ambiente informacional, identificar vulnerabilidades y oportunidades en ambos dominios, y sincronizar efectos de manera coordinada. Esto requiere no solo capacidades técnicas adecuadas, sino también procesos conceptuales que permitan comprender la influencia recíproca entre fenómenos cibernéticos, electromagnéticos y físicos. La conducción moderna demanda planificadores con una visión integral del ambiente operacional, capaces de reconocer que las operaciones ciber-electromagnéticas no constituyen un apoyo secundario, sino una dimensión esencial de la maniobra general, y que la libertad de acción en el terreno está estrechamente vinculada al grado de control que se ejerza sobre la información en todas sus dimensiones.

En el ámbito nacional, la situación presenta características particulares. Las Fuerzas Armadas argentinas han reconocido la importancia creciente de estas capacidades y han iniciado diversas medidas orientadas a fortalecerlas, tanto en materia de formación, equipamiento, organización y actualización doctrinaria. Sin embargo, este proceso se encuentra aún en una fase de consolidación y enfrenta desafíos vinculados a la integración conjunta, la interoperabilidad, la disponibilidad de recursos tecnológicos avanzados y la necesidad de coordinar esfuerzos interinstitucionales. La fragmentación orgánica existente, la coexistencia de enfoques doctrinarios parciales y la ausencia de un modelo operativo unificado dificultan la adopción plena de un enfoque multidominio que permita explotar de manera eficiente las sinergias entre GE y CD. Esta situación, lejos de constituir un obstáculo insalvable, representa una oportunidad estratégica para orientar la modernización del instrumento militar de manera coherente y planificada.

Frente a este escenario, se vuelve imprescindible elaborar un marco conceptual que permita orientar la planificación, ejecución y evaluación de actividades ciber-

electromagnéticas en el nivel operacional, adaptado a las particularidades del entorno nacional y alineado con las tendencias internacionales, especialmente en el período 2014–2024. En este marco, el problema de investigación que orienta el presente Trabajo Final Integrador puede sintetizarse en la siguiente pregunta: ¿cómo deberían conceptualizarse e integrarse las actividades ciber-electromagnéticas en el nivel operacional argentino para contribuir de manera efectiva a la maniobra conjunta en operaciones multidominio?

El objetivo general de este trabajo es diseñar un marco conceptual y un modelo operativo ciber-electromagnético para el nivel operacional argentino, que contribuya a optimizar el empleo de recursos, fortalecer la interoperabilidad entre fuerzas, mejorar los mecanismos de coordinación y aportar criterios para la asignación de capacidades en operaciones conjuntas y combinadas. La hipótesis que orienta la investigación sostiene que la integración sistemática de la Guerra Electrónica y la Ciberdefensa en un enfoque CEMA específico para el nivel operacional incrementa de manera significativa la eficacia y coherencia de la maniobra, al ampliar la libertad de acción y la superioridad informacional frente a un adversario capaz de operar en múltiples dominios.

Metodológicamente, se adopta un enfoque cualitativo, descriptivo y analítico, basado en el análisis comparado de doctrinas y marcos conceptuales de potencias extranjeras, el estudio de casos recientes de empleo de capacidades ciber-electromagnéticas y el examen de documentos normativos y organizacionales del instrumento militar argentino en el período 2014–2024.

Sobre esta base, el trabajo se estructura en tres capítulos: el primero desarrolla el marco conceptual de las actividades ciber-electromagnéticas en el contexto de las operaciones multidominio; el segundo analiza doctrinas y experiencias operacionales internacionales relevantes, extrayendo implicancias para el nivel operacional; y el tercero presenta un diagnóstico preliminar de la situación nacional y propone un modelo operativo CEMA para el instrumento militar argentino, cuyas principales conclusiones se sintetizan en el cierre del trabajo.

CAPÍTULO 1

MARCO CONCEPTUAL DE LAS ACTIVIDADES CIBER-ELECTROMAGNÉTICAS (CEMA) EN EL CONTEXTO DE LAS OPERACIONES MULTIDOMINIO

El presente capítulo tiene por finalidad establecer el marco conceptual que sustenta la investigación. En particular, se busca explicar cómo evolucionaron la Guerra Electrónica (GE) y la Ciberdefensa (CD), cuál es la relación estructural entre el ciberespacio y el espectro electromagnético y por qué la integración de ambas capacidades, bajo el concepto de actividades ciber-electromagnéticas (CEMA),[3] adquiere un carácter estratégico en el contexto de las operaciones multidominio. (Aldea Gracia, 1988)

Este marco no constituye una revisión teórica desvinculada de la práctica, sino la base necesaria para comprender el problema central del trabajo: la integración de la GE y la CD en el nivel operacional de las Fuerzas Armadas argentinas. A partir de las definiciones, antecedentes y relaciones que aquí se establecen, los capítulos siguientes analizarán doctrinas y experiencias internacionales y avanzarán hacia la propuesta de un modelo operativo adaptado al entorno nacional.

1.1. Evolución de la Guerra Electrónica y la Ciberdefensa

La evolución de la Guerra Electrónica y de la Ciberdefensa representa uno de los procesos de transformación más significativos en la forma de concebir el empleo del poder militar desde mediados del siglo XX. Ambas disciplinas nacen de problemas concretos y coyunturales, pero el desarrollo tecnológico y doctrinario las va llevando desde un rol meramente técnico hacia un lugar central en la planificación y conducción de operaciones. En el fondo, lo que cambia no es solo la tecnología disponible, sino la manera en que las fuerzas armadas entienden el papel de la información en la guerra. (Trama & de Vergara, 2017)

En el caso de la Guerra Electrónica, sus raíces pueden rastrearse hasta los primeros años del siglo XX, cuando la radiotelegrafía comienza a utilizarse para coordinar fuerzas navales y terrestres. La posibilidad de interceptar mensajes, ubicar emisores y,

[3] En la doctrina estadounidense y británica, las actividades ciber-electromagnéticas se entienden como el empleo integrado de capacidades de Guerra Electrónica y operaciones en el ciberespacio para asegurar la libertad de acción propia y limitar la del adversario en el continuo que va desde las redes a las ondas de radio (Department of the Army, 2014; Department of the Air Force, 2023; UK Ministry of Defence, 2018).

eventualmente, interferir comunicaciones aparece tempranamente como una oportunidad y como una amenaza. Durante la Primera Guerra Mundial se desarrollan técnicas de escucha de radio, se realizan triangulaciones para localizar unidades enemigas y se adoptan medidas básicas para enmascarar o codificar mensajes. Aunque todavía de forma incipiente, el espectro empieza a percibirse como una dimensión en la que también se combate. (Aldea Gracia, 1988)

La Segunda Guerra Mundial profundiza y acelera este proceso. La introducción del radar para la defensa aérea del Reino Unido, la dirección de ataques aéreos sobre objetivos estratégicos, la guerra antisubmarina en el Atlántico y el empleo de ayudas electrónicas a la navegación convierten al espectro electromagnético en un componente decisivo del esfuerzo bélico. A ambos bandos se los obliga a desarrollar medios de detección y, en paralelo, contramedidas orientadas a degradar o engañar esos sistemas, consolidando la idea de que el control del espectro es un factor crítico para la supervivencia de plataformas y la eficacia de las operaciones. (Haig, 2015)

En este período comienza a consolidarse una tríada conceptual[4] que acompaña el desarrollo posterior de la GE: apoyo electrónico, ataque electrónico y protección electrónica. El apoyo electrónico se vincula a la búsqueda, interceptación, identificación y localización de emisiones enemigas con el objetivo de obtener información y elaborar un cuadro del ambiente electromagnético. El ataque electrónico comprende las acciones destinadas a degradar, negar o engañar el empleo del espectro por parte del adversario, ya sea mediante interferencia, saturación u otras técnicas; mientras que la protección electrónica abarca las medidas orientadas a preservar el uso del espectro por parte de las fuerzas propias, reduciendo su vulnerabilidad frente a las acciones enemigas. Esta estructura conceptual, adoptada luego por numerosos ejércitos, permite organizar funciones, asignar responsabilidades y doctrinar el empleo de medios electrónicos en un sentido más amplio y sistemático.

Con la Guerra Fría, el avance tecnológico y la carrera armamentista introducen nuevos elementos. Se generaliza el uso de radares tridimensionales de largo alcance, sistemas de defensa aérea integrados, misiles guiados por radar y enlaces de datos digitales. La densidad de emisiones en el espectro aumenta de manera notable y el

[4] La clasificación tradicional de la Guerra Electrónica distingue entre medidas de apoyo electrónico (ES), de ataque electrónico (EA) y de protección electrónica (EP), categorías que permiten organizar tanto los medios como las funciones asociadas a la detección, la interferencia y la protección frente a las emisiones enemigas (Aldea Gracia, 1988; Haig, 2015).

ambiente electromagnético se vuelve cada vez más complejo. En ese contexto, la GE se vuelve indispensable para la supervivencia de plataformas de combate, en especial en campañas aéreas planificadas contra sistemas de defensa sofisticados, donde el reconocimiento electrónico previo y la supresión de defensas forman parte nuclear del diseño operacional.

En paralelo, las fuerzas armadas comienzan a depender de redes de comunicaciones cada vez más complejas. Enlaces de HF, VHF y UHF, comunicaciones satelitales, sistemas de mensajería táctica y redes de datos convergen en arquitecturas integradas que sostienen la maniobra conjunta y combinada. La movilidad de las fuerzas, la dispersión de los teatros de operaciones y la necesidad de coordinar acciones en múltiples dominios refuerzan la dependencia del espectro electromagnético, de modo que la GE deja de ser una capacidad marginal para convertirse en uno de los pilares que condicionan la viabilidad de las operaciones de envergadura.

Mientras la GE se consolida, en otro plano comienza a gestarse la transformación que dará origen a la Ciberdefensa. Hacia finales del siglo XX, la informatización de los sistemas militares, gubernamentales y económicos se acelera. Los sistemas de mando y control basados en computadoras, las redes de datos, las bases de datos estratégicas, los sistemas de información geográfica y las aplicaciones de gestión logística se vuelven habituales, al tiempo que el ámbito civil desarrolla una infraestructura digital global interconectada de la que dependen, directa o indirectamente, los organismos de defensa. (Reale, 2023)

En un comienzo, la preocupación se centra en la seguridad informática clásica: evitar accesos no autorizados, proteger contraseñas, resguardar la integridad de los archivos y garantizar la continuidad de servicios. Con el tiempo, sin embargo, se hace evidente que las amenazas evolucionan hacia formas más sofisticadas, en las que actores estatales y no estatales utilizan herramientas cibernéticas con fines políticos, estratégicos o militares. Los incidentes dirigidos contra infraestructuras críticas y sistemas gubernamentales actúan como catalizadores para la elaboración de estrategias nacionales de ciberseguridad, la creación de estructuras permanentes de Ciberdefensa y el reconocimiento del ciberespacio como un ámbito que debe ser defendido de manera análoga a los dominios físicos. (Reale, 2023)

En el ámbito militar, este cambio se traduce en la creación de comandos específicos, centros de operaciones cibernéticas y doctrinas que reconocen al ciberespacio como un dominio de operaciones más, junto al terrestre, marítimo, aéreo y espacial. La protección

de redes, sistemas y datos críticos se convierte en una responsabilidad central de la defensa, en estrecha relación con otros organismos del Estado y con actores privados que administran infraestructuras esenciales.

La convergencia entre GE y CD se produce cuando los sistemas militares pasan a operar sobre arquitecturas integradas que dependen simultáneamente del espectro y del ciberespacio. Un centro de mando que gobierna enlaces de datos, radios definidas por software, redes de sensores y sistemas de información táctica es, en la práctica, un nodo ciber-electromagnético cuyas vulnerabilidades abarcan toda la cadena que conecta el dato con la decisión. Esta constatación lleva a distintas fuerzas armadas a introducir marcos conceptuales que integran Guerra Electrónica y operaciones en el ciberespacio bajo una misma lógica, dando lugar al concepto de actividades ciber-electromagnéticas. (Alaniz Miranda, 2018)

En este trabajo, la evolución de la GE y de la CD no se describe con intención enciclopédica, sino para mostrar cómo se pasó de funciones técnicas de apoyo a disciplinas que condicionan directamente la posibilidad de concebir y ejecutar operaciones modernas. Ese recorrido permite comprender por qué la integración de ambas capacidades en el nivel operacional se ha transformado en un desafío central, tanto para las grandes potencias como para países que, como la Argentina, se encuentran en procesos de modernización y adaptación doctrinaria. (Casale, 2022)

1.2. Relación entre el ciberespacio y el espectro electromagnético

La relación entre el ciberespacio y el espectro electromagnético es uno de los fundamentos conceptuales de las actividades ciber-electromagnéticas. Sin entender con claridad cómo se articulan estos dos ámbitos resulta difícil justificar la necesidad de integrarlos doctrinariamente y de crear estructuras específicas para gestionarlos en forma conjunta. Durante años, la tendencia fue abordarlos por separado: el ciberespacio se asociaba a computadoras, redes, software y datos, mientras que el espectro se vinculaba con ondas de radio, comunicaciones, radares y otros sistemas emisores. La evolución tecnológica, sin embargo, fue uniendo de manera cada vez más estrecha estas dos dimensiones. (Haig, 2015)

En términos sencillos, el ciberespacio puede definirse como el conjunto de infraestructuras físicas, sistemas lógicos y actores que hacen posible la creación, almacenamiento, procesamiento y transmisión de información digital, lo cual incluye tanto los medios militares como aquellos civiles de los que estos dependen directa o

indirectamente.[5] En el ámbito de la defensa, abarca los sistemas de mando y control, las redes tácticas y estratégicas, los sistemas de información de combate, las bases de datos logísticas y de inteligencia, y las plataformas de simulación.

El espectro electromagnético, por su parte, es el rango de frecuencias que se utilizan para transmitir señales en forma de ondas. Las comunicaciones de HF, VHF y UHF, los enlaces de microondas, las comunicaciones satelitales, los radares, las ayudas a la navegación y una parte creciente de los sistemas de vigilancia y reconocimiento emplean distintas porciones de ese espectro. En el nivel militar, el espectro se administra, se planifica y se protege, porque de su disponibilidad e integridad depende buena parte de la capacidad de coordinar fuerzas, detectar amenazas y sostener la maniobra. (Aldea Gracia, 1988)

La conexión entre ambos ámbitos se hace visible cuando se analiza el recorrido concreto de un flujo de información. Un reporte generado por un sensor puede ser digitalizado, transmitido por un enlace de radio, enrutado a través de una red de datos, procesado en un servidor y presentado en la pantalla de un operador como parte de un cuadro de situación. Cada una de esas etapas se apoya en distintos componentes físicos y lógicos, que incluyen tanto dispositivos informáticos como medios de transmisión espectrales. El mensaje que parece estar "en la red" atraviesa, en realidad, de manera sucesiva estructuras del ciberespacio y del espectro. (Haig, 2015)

La arquitectura de los sistemas militares modernos refuerza esta interdependencia. Las radios definidas por software permiten programar parámetros de frecuencia, modulación, cifrado y salto automático de canales mediante software; los enlaces de datos tácticos integran información de diferentes plataformas y la distribuyen en tiempo casi real a múltiples usuarios; los sistemas de mando y control combinan comunicaciones cableadas e inalámbricas, redes de área local y extendida, enlaces satelitales y sistemas de mensajería táctica. Los sensores avanzados, por su parte, utilizan el espectro para detectar pero requieren de redes digitales para transmitir los datos recogidos y para que estos puedan ser procesados y explotados por los niveles de conducción. (TRADOC, 2018)

[5] En varias doctrinas contemporáneas el ciberespacio se describe como un dominio global compuesto por redes de información interconectadas, infraestructuras físicas asociadas y los datos que circulan sobre ellas, lo que lo convierte en un entorno decisivo tanto para la defensa como para la competencia estratégica (Joint Chiefs of Staff, 2018; Department of the Air Force, 2023; North Atlantic Treaty Organization, 2024).

Esta situación genera una doble dependencia. Por un lado, el ciberespacio no puede funcionar sin el soporte físico y espectral que le proporciona conectividad: sin enlaces adecuados, las redes se fragmentan, los nodos quedan aislados y la información deja de circular. Por otro lado, el aprovechamiento pleno del espectro moderno requiere de sistemas digitales que administren frecuencias, filtren señales, procesen datos y permitan que las emisiones se integren en sistemas mayores. En la práctica, ciberespacio y espectro forman un continuo ciber-electromagnético sobre el cual se apoya el flujo informacional.

Las vulnerabilidades se distribuyen también a lo largo de ese continuo. Un ataque sobre un servidor crítico puede afectar la disponibilidad de servicios de comunicaciones, aun cuando las radios y antenas sigan operativas; un malware que comprometa un sistema de gestión de redes puede dejar sin control un conjunto de enlaces, provocar congestión o habilitar accesos no autorizados. Inversamente, una operación de interferencia o de engaño sobre determinados enlaces puede aislar nodos, impedir la actualización de datos, degradar la coordinación entre unidades o generar lagunas de información. En ambos casos, el efecto final se traduce en una alteración del proceso de conducción.

Desde la perspectiva de la maniobra, la interdependencia entre ciberespacio y espectro afecta directamente la capacidad de observar, decidir y actuar. La obtención de información sobre el ambiente, la transmisión de órdenes, la coordinación de fuegos y movimientos, la ejecución de apoyos logísticos, la interacción entre componentes y la articulación con otros organismos del Estado dependen de que el flujo informacional se mantenga dentro de ciertos umbrales. Cuando ese flujo se degrada o se interrumpe de manera significativa, la organización enfrenta mayores niveles de incertidumbre y riesgos elevados de tomar decisiones con información incompleta o desactualizada.

Esta realidad plantea desafíos doctrinarios y organizativos. Si se mantiene una estructura fragmentada, donde la seguridad de la información se gestiona en un área, las comunicaciones en otra y la Guerra Electrónica en otra, es probable que nadie tenga una visión completa del ambiente ciber-electromagnético. Las amenazas modernas, en cambio, tienden a explotar justamente esas grietas organizativas, encadenando acciones en el ciberespacio y en el espectro para producir efectos significativos sobre la disponibilidad y la confiabilidad de los sistemas críticos. (Casale, 2022)

También surgen desafíos en el plano estratégico. Las infraestructuras críticas que sostienen el funcionamiento de un país dependen de redes digitales y de servicios de telecomunicaciones: sistemas de energía, transporte, finanzas, salud y administración pública utilizan masivamente el ciberespacio y el espectro. La defensa de este entramado

no puede ser responsabilidad exclusiva de un único organismo, sino que requiere marcos normativos claros[6], coordinación entre distintos niveles del Estado, acuerdos de cooperación con el sector privado y, en algunos casos, arreglos internacionales que permitan gestionar incidentes con ramificaciones transfronterizas.

Para las fuerzas armadas, asumir la existencia de un continuo ciber-electromagnético implica concebir la defensa de la información como un esfuerzo compartido, que trasciende los límites tradicionales entre armas, servicios y organismos. Supone desarrollar capacidades de vigilancia del ambiente ciber-electromagnético, establecer procedimientos para detectar y responder a incidentes que afecten tanto redes como enlaces, y diseñar arquitecturas que integren redundancias, rutas alternativas y mecanismos de recuperación rápida. También exige formar cuadros capaces de entender que un problema que se manifiesta en un punto concreto del sistema puede tener su origen en otro nivel, y que por lo tanto requiere una mirada integral. (Department of the Army, 2014; JDN 1/18, 2018)

En el contexto de este trabajo final integrador, la relación entre ciberespacio y espectro no se aborda solo como un dato técnico, sino como el fundamento que justifica la necesidad de integrar Guerra Electrónica y Ciberdefensa en el nivel operacional. Solo a partir de este reconocimiento es posible avanzar hacia un enfoque CEMA coherente, que permita planificar y conducir operaciones en entornos multidominio donde la información y su soporte ciber-electromagnético se han convertido en uno de los principales factores de éxito o fracaso. (Casale, 2022)

1.3. Importancia estratégica de la integración en operaciones multidominio

La integración de las actividades ciber-electromagnéticas en el marco de las operaciones multidominio[7] reviste una importancia estratégica que deriva de la manera en que ha cambiado el carácter de la guerra. La confrontación contemporánea combina, desde el inicio, acciones en el plano terrestre, marítimo, aéreo, espacial, cibernético e

[6]En el caso argentino, entre esos marcos se destacan la Estrategia Nacional de Ciberseguridad aprobada en 2019, la Directiva de Política de Defensa Nacional de 2021 y los lineamientos de los Libros Blancos de la Defensa, que reconocen la importancia de proteger infraestructuras críticas y de articular esfuerzos civiles y militares en el ciberespacio (República Argentina, 2015; República Argentina, 2019; República Argentina, 2021; República Argentina, 2023).

[7] En la doctrina estadounidense, las operaciones multidominio se definen como el empleo integrado de capacidades en todos los dominios —tierra, mar, aire, espacio y ciberespacio— para crear dilemas simultáneos al adversario y desarticular la cohesión de su sistema de fuerzas (U.S. Army Training and Doctrine Command, 2018).

informacional. La frontera entre paz, crisis y conflicto armado se vuelve difusa y aparecen zonas grises[8] donde actores estatales y no estatales despliegan campañas de presión, desinformación, sabotaje o interferencia que no siempre alcanzan el umbral de la guerra declarada, pero que pueden producir efectos acumulativos significativos

Las operaciones multidominio surgen como respuesta a este tipo de escenarios, planteando la necesidad de coordinar de manera simultánea efectos físicos y no físicos en distintas dimensiones, de aprovechar las ventajas propias y de explotar las vulnerabilidades ajenas de forma integrada. Desde este punto de vista, las actividades ciber-electromagnéticas dejan de ser un recurso secundario y se convierten en un componente esencial para asegurar la coherencia de la maniobra, la continuidad del mando y la protección del sistema de fuerzas

En primer lugar, la integración CEMA es clave para preservar la libertad de acción en el nivel operacional. Esta libertad incluye la capacidad de planear y ejecutar una campaña, de adaptar el diseño operacional a la evolución de la situación y de coordinar a los componentes terrestre, naval, aéreo y, llegado el caso, espacial y cibernético. Comunicaciones interrumpidas, redes degradadas, sensores cegados o engañados y sistemas de mando y control parcialmente paralizados pueden obligar a un comandante a renunciar a cursos de acción, reducir su iniciativa o asumir riesgos elevados, restringiendo de hecho su libertad de acción.

En segundo lugar, las CEMA integradas permiten actuar de forma directa sobre el sistema de mando y control del adversario. La posibilidad de interferir comunicaciones críticas, degradar la calidad de la información que recibe, introducir demoras, aislar unidades clave o explotar vulnerabilidades para acceder a determinados sistemas puede afectar la cohesión y la eficacia de la fuerza contraria. Estos efectos, si se planifican y ejecutan de manera sincronizada con operaciones físicas, pueden facilitar la maniobra propia, abrir ventanas de oportunidad, reducir la capacidad de respuesta enemiga y, en algunos casos, evitar la necesidad de emplear medios más destructivos. (Alaniz Miranda, 2018)

En tercer lugar, la integración CEMA se relaciona con la superioridad informacional. Esta superioridad no se limita a disponer de más datos, sino a contar con

[8] El concepto de "zonas grises" alude a formas de presión que se sitúan por debajo del umbral del conflicto armado abierto —campañas de desinformación, coerción económica, sabotaje limitado— pero que buscan alterar el equilibrio estratégico a favor del actor que las impulsa (North Atlantic Treaty Organization, 2024; Quintana, 2016).

información pertinente, oportuna y confiable, y a gestionar esa información de manera que se traduzca en decisiones acertadas. En entornos donde la densidad de datos es muy alta, la calidad del procesamiento, la filtración, la presentación y la protección de la información se vuelven decisivas. La coordinación entre Guerra Electrónica y Ciberdefensa contribuye a asegurar que el flujo informacional propio se mantenga dentro de parámetros aceptables, a la vez que dificulta que el adversario alcance el mismo nivel de certeza.

En cuarto lugar, las actividades ciber-electromagnéticas integradas tienen un impacto directo en la disuasión. Un Estado que cuenta con capacidades creíbles para defender su propio entorno ciber-electromagnético, para detectar y atribuir ataques y para producir efectos selectivos sobre sistemas informacionales adversarios eleva el costo esperado de cualquier agresión en este ámbito. Esta capacidad de disuasión no se limita al período de guerra: en tiempos de paz y de tensión, la sola existencia de estructuras CEMA maduras puede influir en los cálculos de otros actores, desalentando determinadas acciones o incorporando un factor de incertidumbre respecto del resultado de operaciones hostiles en el ciberespacio o en el espectro. (Reale, 2023)

En quinto lugar, las CEMA integradas ofrecen herramientas valiosas para la gestión de crisis y para la respuesta graduada. No todas las agresiones o interferencias justifican una respuesta militar convencional. Contar con un abanico de opciones que incluyen medidas de protección reforzada, acciones de neutralización técnica, demostraciones de capacidad o respuestas proporcionadas en el entorno ciber-electromagnético permite gestionar escaladas de forma más flexible y ajustada a la política de defensa.

La integración CEMA plantea, asimismo, exigencias organizativas. Supone establecer estructuras en los niveles táctico, operacional y estratégico con responsabilidad clara sobre la planificación, coordinación y ejecución de actividades ciber-electromagnéticas; definir relaciones de comando y control; establecer procedimientos para la solicitud y asignación de efectos; articular canales de enlace con otros componentes y mecanismos de coordinación con organismos civiles responsables de la ciberseguridad y del espectro a nivel nacional. También demanda un esfuerzo sostenido de formación de cuadros, tanto técnicos como de conducción, capaces de comprender las implicancias operacionales de decisiones que, en apariencia, podrían considerarse puramente técnicas.

Por último, la integración de actividades ciber-electromagnéticas se vincula con la resiliencia del instrumento militar. En un entorno donde resulta razonable suponer que el

adversario logrará, al menos parcialmente, afectar redes, sistemas y enlaces, la cuestión central es si la organización está preparada para seguir operando bajo condiciones degradadas. Un enfoque CEMA maduro fomenta la adopción de arquitecturas con redundancias, la existencia de rutas alternativas de comunicación, el empleo de procedimientos manuales o simplificados cuando se pierde parte de la automatización y el entrenamiento específico para operar con niveles variables de información. (TRADOC, 2018)

En el caso argentino, la importancia estratégica de la integración de la GE y la CD se ve atravesada por condicionantes propios. La necesidad de modernizar equipamiento, la disponibilidad limitada de recursos, la coexistencia de marcos doctrinarios en proceso de actualización y la creciente dependencia de sistemas de información tanto en el ámbito militar como en el civil plantean desafíos particulares, pero también oportunidades para diseñar estructuras y procesos que incorporen desde el inicio la lógica CEMA. Los desarrollos doctrinarios conjuntos en materia de operaciones militares cibernéticas y los trabajos recientes sobre convergencia GE-CD en el nivel operacional ofrecen insumos valiosos para orientar este proceso.

El marco conceptual desarrollado en este capítulo tiene, por lo tanto, un doble propósito. Por un lado, ofrecer una visión clara y articulada de la evolución de la GE y la CD, de la relación entre ciberespacio y espectro y de la importancia de integrar ambas capacidades en el contexto de las operaciones multidominio. Por otro, sentar las bases para el análisis que se realizará en los capítulos siguientes, donde se examinarán doctrinas y experiencias de referencia en materia de actividades ciber-electromagnéticas y se abordará la situación argentina con el objetivo de proponer un modelo operativo que permita integrar de manera efectiva las capacidades ciber-electromagnéticas en el nivel operacional de las Fuerzas Armadas argentinas.

CAPÍTULO 2

ANÁLISIS COMPARATIVO DE DOCTRINAS INTERNACIONALES Y EXPERIENCIAS OPERACIONALES

El propósito de este capítulo es analizar cómo algunas de las principales potencias militares han conceptualizado e implementado la integración entre Guerra Electrónica (GE) y Ciberdefensa (CD), y cómo esa integración se ha puesto a prueba en conflictos recientes. Mientras el Capítulo 1 estableció el marco conceptual general de las actividades ciber-electromagnéticas (CEMA) y su lugar en las Operaciones Multidominio, el presente capítulo avanza hacia un terreno más concreto: las doctrinas de referencia y los casos prácticos que permiten observar la integración de GE y CD en contextos reales de empleo.

Este análisis se estructura en tres apartados. En primer lugar, se examinan las doctrinas de Estados Unidos y del Reino Unido, que constituyen marcos de referencia relevantes por su nivel de desarrollo y por la claridad con la que formulan la integración CEMA en el nivel operacional. En segundo término, se estudian dos casos prácticos: los conflictos en Ucrania y Georgia, donde la Federación Rusa ha empleado de manera combinada capacidades cibernéticas, electrónicas e informacionales como parte de campañas militares más amplias. Por último, se presenta una síntesis de implicaciones para la planificación operativa en Argentina, que servirá de base para el diseño del modelo operativo propuesto en el Capítulo 3.

De esta manera, el capítulo articula doctrina y práctica, con el objetivo de extraer lecciones útiles para el nivel operacional argentino sin caer en una simple trasposición de modelos ajenos, sino identificando aquellos elementos que pueden ser adaptados a las particularidades del instrumento militar nacional.

2.1 Doctrinas de Estados Unidos y Reino Unido

Estados Unidos y el Reino Unido han sido, en la última década, dos de los actores que más avanzaron en la elaboración de marcos doctrinarios explícitos para integrar la Guerra Electrónica y la Ciberdefensa en un enfoque común de actividades ciber-electromagnéticas. Ambos países parten de un diagnóstico similar: el ciberespacio y el espectro electromagnético ya no pueden ser tratados como ámbitos separados, reservados a especialistas, sino como partes de un mismo entorno informacional que sostiene la conducción de las operaciones en todos los dominios, lo que se refleja en manuales y notas doctrinarias específicas sobre CEMA.

En el caso de Estados Unidos, este proceso tiene un recorrido largo, que comienza con el reconocimiento del ciberespacio como dominio de operaciones, la creación del U.S. Cyber Command y la consolidación de comandos específicos de ciberdefensa en cada fuerza armada. En paralelo, el Ejército de Tierra fue redefiniendo el lugar de la Guerra Electrónica, que pasó de ser considerada un apoyo técnico de nicho a ser tratada como un componente esencial del sistema C4ISR y de la maniobra informacional. La síntesis de ese trayecto se expresa de manera clara en el manual FM 3-38, dedicado a las actividades ciber-electromagnéticas, donde se establece que GE, operaciones en el ciberespacio y otras funciones afines deben planificarse como un esfuerzo unificado al servicio de la maniobra.

El FM 3-38 no se limita a describir capacidades o medios, sino que define la finalidad de las CEMA en términos operacionales: contribuir a que la fuerza propia alcance y sostenga la superioridad informacional, apoyando la maniobra en todos los niveles de conducción. Para ello, la doctrina indica que las CEMA deben incorporarse desde las etapas iniciales del ciclo de planeamiento, empezando por el análisis del ambiente operacional. Se espera que las células CEMA identifiquen redes críticas, dependencias del adversario respecto del espectro, puntos de vulnerabilidad en los sistemas de mando y control y posibles objetivos informacionales cuyo tratamiento pueda modificar la relación de fuerzas sin necesidad de recurrir de inmediato a fuegos cinéticos

En esa lógica, el nivel operacional ocupa un lugar central. Las actividades ciber-electromagnéticas no se conciben como intervenciones puntuales en apoyo a una unidad táctica aislada, sino como parte de un diseño de campaña que abarca varios ejes, fases y componentes. El manual remarca que las decisiones sobre dónde, cuándo y con qué intensidad emplear capacidades de Guerra Electrónica u operaciones en el ciberespacio deben derivarse del concepto de la operación, de los centros de gravedad identificados[9] y de los objetivos que el comandante pretende alcanzar en cada fase. Esto supone que las CEMA no se agregan al final, como un "plus tecnológico", sino que forman parte de la arquitectura de la maniobra desde el momento en que se formulan los cursos de acción.

Organizativamente, esta concepción se traduce en la creación de secciones CEMA insertas en los estados mayores de cuerpos de ejército, divisiones e incluso brigadas. Estas

[9] En la doctrina operacional, el centro de gravedad se entiende como la fuente principal de fuerza, cohesión o libertad de acción del adversario o de la propia fuerza, cuya afectación o preservación condiciona el resultado de la campaña. Ubicar las CEMA en función de esos centros de gravedad evita emplearlas de manera dispersa o meramente oportunista.

secciones mantienen un vínculo estrecho con las áreas de inteligencia, operaciones, comunicaciones y protección de la fuerza, y funcionan como el punto de convergencia para todo lo relacionado con el espectro y el ciberespacio. Su tarea no es solo ejecutar pedidos de interferencia o brindar protección cibernética, sino también asesorar al comandante, traduciendo las necesidades operacionales en requerimientos ciber-electromagnéticos concretos y, a la inversa, explicando las limitaciones técnicas en términos de riesgo táctico u operacional.

En varios escalones se experimentó además con equipos CEMA desplegables, capaces de acompañar a las unidades de maniobra en el terreno. La lógica es similar a la de otros apoyos de combate: así como las unidades de artillería o ingenieros deben estar en condiciones de proporcionar efectos donde se los necesita, las capacidades ciber-electromagnéticas tienen que poder generar interferencia, protección o explotación en el tiempo y lugar oportunos. Este enfoque refuerza la idea de que las CEMA deben operar con la misma flexibilidad y capacidad de adaptación que los fuegos, el movimiento o la logística, lo que exige personal entrenado, procedimientos claros y una integración real con el resto de las funciones de combate.

Al mismo tiempo, la doctrina estadounidense vincula el desarrollo de las CEMA con el concepto más amplio de Operaciones Multidominio. La perspectiva de "campo de batalla multidominio" concibe al ciberespacio y al espectro como espacios de maniobra que pueden ser explotados para generar ventanas de oportunidad en otros dominios, lo que se refleja también en conceptos funcionales para operaciones en el ciberespacio y el espectro electromagnético (U.S. Army TRADOC, 2018)[10].

Bloquear temporalmente el sistema de navegación de un adversario, degradar la capacidad de enlace de sus drones o manipular información clave en sus redes de mando y control son ejemplos de cómo las actividades ciber-electromagnéticas pueden crear condiciones favorables para una ofensiva terrestre, un golpe aéreo o una operación aeronaval. El FM 3-38 insiste en que la planificación debe considerar estos encadenamientos de efectos y no tratar las CEMA como líneas de acción desconectadas del resto del esfuerzo.

[10] TRADOC Pamphlet 525-3-1 destaca que el control del espectro electromagnético y la protección del ciberespacio forman parte de una misma competencia por la superioridad de la información, en la que la Guerra Electrónica y la Ciberdefensa deben concebirse como componentes de un mismo esfuerzo (U.S. Army Training and Doctrine Command, 2018).

El Reino Unido recorre un camino convergente, aunque enmarcado en una tradición doctrinaria conjunta más marcada. En su caso, las actividades ciber-electromagnéticas se integran desde el inicio en un enfoque que habla de "maniobra en el entorno de la información". La Joint Doctrine Note 1/18 es uno de los documentos donde se explicita este concepto. Allí se entiende el entorno de la información como un espacio donde se cruzan el ciberespacio, el espectro electromagnético, las percepciones públicas, la legitimidad política y la narrativa estratégica (UK Ministry of Defence, 2018). La Guerra Electrónica y la Ciberdefensa se ubican dentro de esa maniobra más amplia, no como fines en sí mismos, sino como herramientas para proteger la capacidad de decidir y actuar de la propia fuerza y para influir en la voluntad y en la capacidad de respuesta del adversario.

La doctrina británica hace especial hincapié en el carácter conjunto de las CEMA. A diferencia de modelos más centrados en una fuerza específica, como el Ejército de Tierra, el Reino Unido insiste en que la superioridad informacional solo puede sostenerse mediante la acción coordinada de los componentes terrestre, naval, aéreo y de las estructuras de apoyo estratégico. Esto se refleja en la organización: se crean equipos y células CEMA en los estados mayores conjuntos, con la misión de asesorar al comandante, elaborar productos de evaluación del entorno ciber-electromagnético, proponer objetivos informacionales y articular medidas de protección para el sistema de mando y control.

Estos equipos no trabajan en forma aislada, sino en interacción permanente con otras capacidades que el Reino Unido agrupa bajo el paraguas de "information manoeuvre": operaciones de información, operaciones psicológicas, operaciones en redes sociales, acciones de comunicación estratégica y otras herramientas destinadas a modelar el entorno informacional. La Guerra Electrónica y la Ciberdefensa, en ese contexto, se ocupan principalmente de garantizar que la fuerza propia pueda seguir recibiendo, procesando y transmitiendo información confiable, mientras que, al mismo tiempo, degradan o alteran la información de la que depende el adversario. Se trata, nuevamente, de un enfoque orientado a efectos, donde el criterio de evaluación no es solo técnico, sino operacional.

En el nivel operacional, la doctrina británica prevé que las CEMA se incorporen formalmente al ciclo de planeamiento conjunto. Desde las primeras etapas, los planificadores deben considerar qué riesgos ciber-electromagnéticos enfrenta la fuerza, qué dependencias tienen los distintos componentes respecto de sistemas específicos, qué

infraestructuras de información son críticas y qué opciones existen para afectar de manera selectiva las capacidades adversarias. Al igual que en el caso estadounidense, la premisa es que estas decisiones no pueden dejarse para el final del proceso ni quedar relegadas a un diálogo técnico entre especialistas. Deben formar parte del diseño de la campaña y tener un lugar explícito en las órdenes y directivas operacionales.

Más allá de las diferencias institucionales, históricas o terminológicas, las doctrinas de Estados Unidos y el Reino Unido presentan varios puntos en común que resultan particularmente relevantes para el propósito de este. En primer lugar, ambas comparten la convicción de que la Guerra Electrónica y la Ciberdefensa forman parte de un mismo esfuerzo orientado a asegurar la superioridad informacional de la fuerza propia. Esto implica que ya no se las concibe como funciones separadas, sino como componentes de una categoría funcional integrada, capaz de actuar sobre un continuo ciber-electromagnético que sostiene el flujo de información necesario para la conducción.

En segundo lugar, existe coincidencia en que el nivel operacional es el espacio privilegiado para integrar estas capacidades. Es en ese nivel donde se diseñan las campañas, se secuencian las operaciones, se asignan esfuerzos principales y se articulan los apoyos entre componentes. Ubicar a las CEMA en ese plano significa reconocer que su empleo o su ausencia pueden modificar el curso de una campaña del mismo modo que lo hacen los fuegos o las reservas estratégicas. La presencia de secciones CEMA en los estados mayores operacionales, con voz efectiva en el planeamiento y en la conducción, es una respuesta organizativa concreta a esa convicción doctrinaria.

En tercer lugar, tanto Estados Unidos como el Reino Unido subrayan la importancia de contar con estructuras estables, doctrinariamente respaldadas y dotadas de personal especializado que tenga una doble competencia: por un lado, el dominio técnico de las capacidades ciber-electromagnéticas; por otro, la comprensión de la lógica de la maniobra y de las necesidades de la conducción en distintos niveles. Ese perfil mixto es clave para que las CEMA no queden encerradas en un lenguaje puramente técnico, incomprensible para los comandantes, pero tampoco se trivialicen en formulaciones generales que no se traducen en acciones concretas.

Finalmente, las doctrinas de ambos países coinciden en un cambio de criterio a la hora de evaluar el valor de las actividades ciber-electromagnéticas. El énfasis ya no está puesto exclusivamente en indicadores como el número de redes protegidas, la cantidad de ataques detectados o el volumen de interferencia emitido, sino en la contribución efectiva de las CEMA al logro de los objetivos de la campaña. Esta mirada orientada a

efectos aporta un criterio valioso para, en el caso argentino, pensar cómo debería medirse el aporte de GE y CD en el nivel operacional.

En conjunto, las doctrinas de Estados Unidos y del Reino Unido ofrecen una imagen clara del rumbo que siguen las fuerzas armadas que han decidido integrar plenamente las actividades ciber-electromagnéticas en su concepción de la guerra moderna. No se trata solamente de incorporar equipamiento avanzado o de crear nuevas oficinas en los organigramas, sino de ordenar el pensamiento militar en torno a la idea de que la información y su soporte ciber-electromagnético son componentes estructurales del diseño operacional. En el apartado siguiente, este marco doctrinario será puesto en relación con experiencias concretas de empleo en conflictos recientes, particularmente en Ucrania y en el entorno del Cáucaso, con el propósito de identificar cómo estos principios se materializan en campañas reales y qué lecciones pueden extraerse para la planificación operativa en Argentina.

2.2 Estudio de casos prácticos: Conflictos en Ucrania y Georgia

Las doctrinas adquieren verdadero sentido cuando se contrastan con la práctica. Los conflictos en Ucrania y Georgia constituyen, en este sentido, laboratorios empíricos en los que puede observarse cómo la integración de capacidades ciber-electromagnéticas se convierte en una herramienta concreta al servicio de campañas militares, y cómo la ausencia de una preparación adecuada en esta dimensión genera vulnerabilidades críticas que impactan de manera directa en la conducción y en los resultados de las operaciones.

El caso de Ucrania, especialmente a partir de 2014[11], ofrece un ejemplo extendido en el tiempo de empleo combinado de capacidades ciber-electromagnéticas y operaciones convencionales, donde se registran ataques cibernéticos, campañas de desinformación y empleo intensivo de Guerra Electrónica en apoyo de la acción militar rusa (Baezner, 2018). Con la anexión de Crimea y el inicio del conflicto en el Donbás, la Federación Rusa despliega un conjunto articulado de acciones que incluye operaciones cibernéticas contra organismos estatales ucranianos, campañas de desinformación orientadas a la población y a audiencias externas, empleo intensivo de Guerra Electrónica en zonas clave y operaciones militares en el terreno. Los ataques informáticos se dirigen, en una primera

[11] Entre 2014 y 2022, Ucrania registró múltiples campañas de intrusión y sabotaje contra redes gubernamentales, infraestructuras críticas y medios de comunicación, que incluyeron el apagón eléctrico de 2015 y ataques coordinados contra bancos y organismos estatales (Baezner & Robin, 2017; Baezner, 2018).

etapa, contra sitios gubernamentales, medios de comunicación y servicios públicos, con el objetivo de desorganizar la capacidad de comunicación oficial, generar incertidumbre y erosionar la confianza en las instituciones. Paralelamente, se observan intrusiones en redes administrativas y en sistemas de apoyo a la toma de decisiones, lo que pone de manifiesto la intención de explorar y, cuando resulta posible, explotar vulnerabilidades en la infraestructura digital ucraniana, tanto en el plano gubernamental como en sectores vinculados a servicios esenciales (Baezner, 2018).

En este contexto, la Guerra Electrónica adquiere un rol relevante como complemento y potenciador de las acciones cibernéticas. Se registran interferencias sobre comunicaciones tácticas, intentos de degradar sistemas de posicionamiento global, acciones orientadas a neutralizar o limitar el empleo de drones para observación y corrección de fuegos, así como perturbaciones sobre sensores asociados a sistemas de vigilancia terrestre y aérea. La integración de estos esfuerzos con acciones convencionales permite a la Federación Rusa mejorar su conciencia situacional en determinados sectores, dificultar la coordinación de las fuerzas ucranianas y, en algunos casos, aislar posiciones clave del flujo de información que sostiene el mando y control.

La invasión a gran escala iniciada en 2022 intensifica e ilumina con mayor claridad estos patrones. Antes del comienzo de las operaciones terrestres, diversos informes dan cuenta de nuevas oleadas de ataques cibernéticos contra ministerios, bancos y empresas de servicios críticos, así como de intentos de comprometer sistemas de comunicaciones y plataformas digitales utilizadas para la coordinación gubernamental y la gestión de servicios esenciales. En paralelo, se emplean capacidades de Guerra Electrónica de mayor alcance y sofisticación, capaces de interferir comunicaciones tácticas en franjas amplias del frente, perturbar enlaces satelitales y degradar la calidad de los sistemas de navegación y posicionamiento empleados por plataformas terrestres y aéreas. En varios sectores se reportan dificultades para mantener enlaces estables, para operar con normalidad medios aéreos no tripulados utilizados para observación, reconocimiento y corrección de fuegos y para sostener en forma continua ciertos canales críticos de mando y control.

A nivel operacional, estas acciones se inscriben en una lógica de “preparación del campo de batalla ciber-electromagnético”. Mediante la combinación de ataques cibernéticos, interferencia de comunicaciones y desinformación, se busca reducir la capacidad de Ucrania para coordinar la defensa, retrasar sus tiempos de reacción y generar un ambiente de confusión que favorezca las maniobras iniciales de las fuerzas rusas. El empleo de sistemas de Guerra Electrónica de largo alcance, junto con capacidades de

inteligencia de señales, permite además a la Federación Rusa obtener información sobre patrones de emisión, identificar nodos de comunicaciones relevantes y ajustar sus acciones en función del comportamiento ucraniano, lo que refuerza la dimensión informacional de la campaña.

Frente a este escenario, la respuesta ucraniana se caracteriza por una combinación de refuerzo externo en materia de Ciberdefensa, innovación en el uso de medios comerciales adaptados al empleo militar y organización de estructuras dedicadas a la coordinación ciber-electromagnética. Ucrania recurre a acuerdos de cooperación con actores estatales y privados para fortalecer la protección de sus redes, introduce rápidamente soluciones basadas en infraestructuras civiles, como servicios de comunicaciones satelitales comerciales y redes de datos no originalmente diseñadas para uso militar, y diversifica los medios de comunicación disponibles en el teatro de operaciones.

Paralelamente, incorpora de manera masiva drones comerciales modificados para funciones de observación, ataque y corrección de fuego, y adapta su doctrina de empleo para aprovechar la disponibilidad de estos medios en múltiples escalones. Al mismo tiempo, se desarrollan capacidades organizativas destinadas a identificar prioridades, gestionar incidentes cibernéticos y coordinar la defensa del entorno informacional con la conducción de las operaciones. La creación de estructuras dedicadas a la Ciberdefensa y a la gestión de incidentes, el vínculo permanente con organizaciones internacionales y con empresas del sector tecnológico y la incorporación de especialistas civiles al esfuerzo de defensa digital dan cuenta de un proceso de adaptación que trasciende el plano estrictamente militar.

En este contexto, la resiliencia informacional[12], entendida como la capacidad de continuar operando bajo condiciones de degradación ciber-electromagnética, emerge como un factor central que, en muchos momentos del conflicto, compensa parcialmente la asimetría material existente entre las fuerzas (Baezner, 2018). Esta resiliencia no es producto exclusivo del equipamiento disponible, sino de una combinación de decisiones doctrinarias, organizativas y técnicas: aceptar la coexistencia de sistemas de alta tecnología con soluciones simples pero robustas, planificar con la expectativa de sufrir interrupciones en las comunicaciones, entrenar para operar con información incompleta

[12]La resiliencia informacional combina medidas técnicas (redundancia, respaldo de datos, segmentación de redes) con dimensiones organizativas y societales, como la alfabetización mediática y la coordinación público-privada frente a campañas de desinformación (Osorio Lalinde et al., 2017; Moyano, 2020).

y prever mecanismos de mando alternativos cuando los sistemas principales se vean afectados.

El caso de Georgia[13], aunque anterior en el tiempo, resulta igualmente ilustrativo para comprender la integración de actividades ciber-electromagnéticas en campañas de orientación ofensiva. Durante el conflicto de agosto de 2008, las operaciones militares se ven precedidas y acompañadas por una serie de acciones en el ciberespacio y en el espectro electromagnético. Diversos análisis señalan la ejecución de ataques informáticos contra sitios gubernamentales georgianos, medios de comunicación y servicios en línea, con el objetivo de saturar y desorganizar los canales oficiales de información, dificultar la comunicación del gobierno con su población y obstaculizar la proyección de la narrativa georgiana hacia la comunidad internacional (Tikk et al., 2008). Los ataques incluyen denegación de servicio contra portales oficiales, alteración o bloqueo de contenidos y afectación de la disponibilidad de servicios críticos de información, lo que limita la capacidad del gobierno para informar en tiempo real y para articular pedidos de apoyo político y diplomático.

En paralelo, se observan acciones de Guerra Electrónica orientadas a interferir comunicaciones militares, degradar la coordinación entre unidades georgianas y dificultar la transmisión de órdenes y la difusión de información sobre la situación en el terreno. Las comunicaciones tácticas y algunos enlaces de mando y control se ven afectados por interferencias y perturbaciones que obligan a recurrir a medios alternativos menos eficientes. La combinación de operaciones rápidas de fuerzas convencionales, acciones cibernéticas simultáneas y empleo de GE contribuye a limitar la capacidad de reacción de Georgia, reduce su margen para reorganizar fuerzas, complica la ejecución de maniobras coordinadas y dificulta la presentación oportuna de información hacia organismos internacionales y aliados potenciales.

Aunque el conflicto georgiano es anterior al período 2014–2024, sus características lo convierten en un antecedente directo de los patrones que se observan posteriormente en Ucrania. En ambos casos se aprecia una lógica de empleo integrada, donde las actividades ciber-electromagnéticas se emplean como parte constitutiva de la estrategia general y no como intervenciones improvisadas (Tikk et al., 2008). Las acciones en el

[13] Durante el conflicto de 2008 en Georgia, los ataques distribuidos de denegación de servicio y las intrusiones contra sitios gubernamentales y medios de comunicación acompañaron las operaciones militares rusas, anticipando patrones de empleo combinado de instrumentos cibernéticos y cinéticos (Tikk et al., 2008).

ciberespacio y en el espectro se diseñan para debilitar la cohesión del adversario, desorganizar su conducción, limitar su capacidad de comunicar y, en última instancia, influir en la percepción de la comunidad internacional sobre el desarrollo y la legitimidad de las operaciones. La secuencia que combina afectación del entorno informacional, presión diplomática y empleo de fuerzas convencionales se repite, con adaptaciones, en ambos casos, lo que sugiere la existencia de un patrón doctrinario más amplio en el empleo ofensivo de capacidades ciber-electromagnéticas.

Desde la perspectiva del nivel operacional, estos casos permiten extraer varias observaciones de interés. En primer lugar, muestran que un actor que dispone de capacidades ciber-electromagnéticas integradas puede emplearlas para preparar el terreno antes del inicio de las operaciones militares abiertas, generando condiciones favorables en términos de desorganización, sorpresa y confusión.

En segundo lugar, estos conflictos evidencian que la ausencia de una preparación suficiente en materia de Ciberdefensa y Guerra Electrónica se traduce rápidamente en pérdida de iniciativa, en dificultades severas para coordinar fuerzas y en un deterioro acelerado de la capacidad de mando y control. Georgia, con un tiempo de reacción reducido y con capacidades limitadas para proteger su entorno informacional, se vio superada en poco tiempo en la dimensión ciber-electromagnética y careció de margen para recuperar la iniciativa, mientras que Ucrania, aunque sufrió impactos importantes, fue capaz de adaptarse y reforzar sus arquitecturas de comunicación.

En tercer lugar, ambos ejemplos ponen de manifiesto la centralidad de la resiliencia informacional como criterio de planeamiento. No se trata solamente de contar con capacidades de ataque o de interferencia, sino de asegurar que el sistema propio de mando y control pueda continuar funcionando bajo presión, aun cuando partes de la infraestructura se vean comprometidas.

Finalmente, estos casos muestran que las actividades ciber-electromagnéticas tienen una dimensión política que no puede ignorarse en el nivel operacional. El impacto de los ataques cibernéticos y de las campañas de desinformación no se limita al campo de batalla. Afecta la percepción de la población, la voluntad de resistencia, la confianza en las autoridades y la imagen internacional del conflicto. La interacción entre operaciones militares, acciones ciber-electromagnéticas y batallas narrativas convierte al entorno informacional en un espacio donde se dirimen no solo cuestiones tácticas, sino también la legitimidad y la interpretación de los hechos.

Estas experiencias no pueden extrapolarse de manera automática al caso argentino, ya que responden a realidades geopolíticas, tecnológicas y doctrinarias distintas. Sin embargo, ofrecen un material valioso para pensar qué papel deberían desempeñar las actividades ciber-electromagnéticas en la planificación operativa nacional y qué riesgos supone ignorar o subestimar esta dimensión en un contexto internacional donde el empleo de capacidades ciber-electromagnéticas se ha convertido en una práctica habitual tanto en crisis como en conflictos abiertos.

2.3 Implicaciones para la planificación operativa en Argentina

El análisis de las doctrinas de Estados Unidos y del Reino Unido, así como de los casos de Ucrania y Georgia, permite extraer una serie de implicaciones concretas para la planificación operativa en Argentina. Estas implicaciones no constituyen todavía un modelo acabado, pero sí señalan líneas de acción que deberán ser consideradas al momento de diseñar el marco conceptual y el modelo operativo que se desarrollará en el Capítulo 3.

Una primera implicación se refiere a la necesidad de reconocer explícitamente a las actividades ciber-electromagnéticas como un componente esencial de la planificación en el nivel operacional, y no como un apoyo técnico marginal, en línea con lo que ya plantean doctrinas como FM 3-38 y la JDN 1/18. Para la realidad argentina, esto implica revisar cómo se integran actualmente GE y CD en los procesos de planeamiento operacional conjunto y hasta qué punto se las considera desde el inicio del ciclo de planificación.

En segundo lugar, las experiencias estudiadas muestran que la existencia de estructuras específicas CEMA dentro de los estados mayores es un factor decisivo para que este reconocimiento doctrinario se materialice en decisiones operativas concretas. Tanto en Estados Unidos como en el Reino Unido, las actividades ciber-electromagnéticas disponen de espacios propios en la organización del estado mayor, con vínculos formales y permanentes con las áreas de inteligencia, operaciones, comunicaciones y protección de la fuerza.

Una tercera implicación se vincula con la formación de cuadros y con la cultura organizacional. Los casos de Ucrania y Georgia ponen en evidencia que la comprensión del entorno ciber-electromagnético no puede quedar confinada a especialistas técnicos. Es necesario que los oficiales que participan en el planeamiento operacional posean un conocimiento básico pero sólido de qué puede y qué no puede lograrse mediante las CEMA, cuáles son los tiempos de preparación requeridos, qué dependencias existen con

otros subsistemas y qué riesgos implica el empleo de estos medios en términos de escalada, atribución y posibles efectos colaterales (Baezner, 2018).

En cuarto lugar, los conflictos analizados señalan la importancia de planificar no solo la generación de efectos ciber-electromagnéticos sobre el adversario, sino también la resiliencia del propio sistema de mando y control. Tanto en Georgia como en Ucrania queda claro que la capacidad de seguir conduciendo operaciones cuando las comunicaciones se ven perturbadas o cuando parte de la infraestructura digital resulta comprometida es un factor decisivo para sostener la iniciativa.

Una quinta implicación tiene que ver con la necesidad de adoptar una lógica de empleo orientada a efectos en la evaluación y en la planificación de las actividades ciber-electromagnéticas. Las doctrinas y experiencias internacionales sugieren que las CEMA deben medirse menos por indicadores puramente técnicos y más por su contribución a objetivos operacionales concretos, como la conservación de la iniciativa, la sincronización de esfuerzos y la protección de sistemas críticos.

En sexto lugar, tanto las doctrinas como los casos analizados muestran que las actividades ciber-electromagnéticas tienen una dimensión conjunta e interinstitucional difícil de soslayar. En la práctica, el entorno informacional se apoya sobre infraestructuras compartidas entre el ámbito militar, el sector civil y otros organismos del Estado. Asimismo, muchas de las capacidades necesarias para la Ciberdefensa y para el empleo de herramientas avanzadas en el espectro se encuentran parcial o totalmente fuera del ámbito orgánico de las fuerzas armadas, lo que exige prever mecanismos de coordinación con organismos públicos y actores privados responsables de infraestructuras críticas (Baezner, 2018).

Por último, una implicación transversal se relaciona con la necesidad de adecuar los marcos doctrinarios nacionales a estas exigencias. Las doctrinas analizadas muestran que la integración de Guerra Electrónica y Ciberdefensa bajo un enfoque ciber-electromagnético no se produce de manera espontánea, sino que requiere definiciones claras sobre conceptos, funciones, responsabilidades y niveles de conducción.

Estas implicaciones no agotan el problema, pero delinean un conjunto de requisitos mínimos que cualquier propuesta de modelo operativo CEMA para el nivel operacional argentino deberá contemplar. De manera sintética, se requiere: reconocer a las actividades ciber-electromagnéticas como componente esencial de la planificación, crear o fortalecer estructuras específicas en los estados mayores operacionales, formar cuadros capaces de comprender y emplear estas capacidades, planificar la resiliencia informacional como

parte integral de la maniobra, adoptar un enfoque orientado a efectos y articular los esfuerzos militares con otros actores estatales y privados vinculados al entorno informacional. El Capítulo 3 retomará estos elementos y los pondrá en relación con las capacidades, limitaciones y marcos doctrinarios existentes en el país, con el fin de diseñar un modelo conceptual y operativo que permita integrar de manera efectiva la Guerra Electrónica y la Ciberdefensa en la planificación y conducción de operaciones en un entorno multidominio.

CAPÍTULO 3

PROPUESTA DE MARCO CONCEPTUAL Y MODELO OPERATIVO CIBER-ELECTROMAGNÉTICO PARA EL NIVEL OPERACIONAL ARGENTINO

3.1 Diagnóstico preliminar de la situación argentina en materia ciber-electromagnética

El recorrido conceptual del Capítulo 1 y el análisis comparado del Capítulo 2 permiten enfocar ahora la mirada sobre la realidad argentina. El propósito de este apartado no es presentar un inventario exhaustivo de medios, normas y procedimientos, sino identificar aquellos rasgos estructurales que condicionan la posibilidad de integrar de manera efectiva la Guerra Electrónica (GE) y la Ciberdefensa (CD) en el nivel operacional. Se trata de un diagnóstico preliminar que sirve como punto de partida para la propuesta de marco conceptual y modelo operativo que se expondrá en las secciones siguientes.

En términos generales, puede afirmarse que las Fuerzas Armadas argentinas han reconocido la importancia creciente de las capacidades vinculadas al ciberespacio y al espectro electromagnético. En los últimos años se han impulsado procesos de actualización doctrinaria, se han creado o fortalecido estructuras vinculadas a la Ciberdefensa y a la Guerra Electrónica, se han incorporado nuevos medios y se ha promovido la formación de especialistas, tanto en el plano conjunto como en el específico de cada fuerza. Sin embargo, este desarrollo todavía se encuentra en una fase de consolidación y presenta brechas significativas cuando se lo observa desde la óptica de las actividades ciber-electromagnéticas (CEMA) en el nivel operacional.

En primer lugar, el plano doctrinario muestra avances parciales pero aún fragmentados. Existen referencias a la Ciberdefensa, a la seguridad de la información y al empleo del espectro electromagnético en documentos conjuntos y específicos, así como en reglamentos y manuales de nivel operacional y táctico. No obstante, la integración de GE y CD bajo un marco conceptual explícito de actividades ciber-electromagnéticas todavía no se encuentra plenamente desarrollada. Esto se traduce en la coexistencia de enfoques que abordan el ciberespacio y el espectro como problemas separados, con definiciones, responsabilidades y procedimientos que no siempre convergen en una lógica única orientada a la superioridad informacional.

En segundo término, el plano organizativo presenta una realidad similar. Se han establecido organismos dedicados a la Ciberdefensa y se mantienen estructuras responsables de la Guerra Electrónica en las distintas fuerzas, pero la articulación de estos elementos en el nivel operacional conjunto no siempre es clara. La existencia de competencias distribuidas, líneas de dependencia diferenciadas y culturas organizacionales propias de cada fuerza dificulta, en la práctica, la constitución de un esfuerzo ciber-electromagnético integrado en el marco de campañas y operaciones conjuntas. En muchos casos, las capacidades se concentran en niveles estratégicos o en ámbitos específicos, sin una traducción directa en órganos de estado mayor que, en el nivel operacional, asuman la responsabilidad de planificar, coordinar y evaluar las CEMA como parte del diseño de la maniobra.

A ello se suma el desafío tecnológico. La modernización de equipamiento en materia de comunicaciones, sistemas de mando y control, sensores y medios de GE y CD avanza en un contexto de recursos limitados, con ciclos de incorporación más lentos que los de las potencias analizadas en el Capítulo 2. Esta realidad no impide desarrollar capacidades relevantes, pero obliga a priorizar, a buscar soluciones tecnológicas escalables y a combinar medios de distinta generación en una misma arquitectura operacional. Al mismo tiempo, la fuerte dependencia de infraestructuras civiles para servicios esenciales de comunicaciones y datos introduce un grado adicional de complejidad, ya que una parte significativa del entorno ciber-electromagnético en el que operan las fuerzas armadas se encuentra fuera de su control orgánico directo (Eissa & Albarracín Keticoglu, 2020).

Otro aspecto central del diagnóstico se vincula con los recursos humanos y la cultura institucional. La creación de especialistas en Ciberdefensa y Guerra Electrónica ha progresado, pero la cantidad de personal con formación específica sigue siendo limitada en relación con la amplitud de tareas que demanda el entorno actual. Además, como se observó en los casos de Ucrania y Georgia, la integración efectiva de CEMA en el nivel operacional no depende solo de los expertos técnicos, sino también de la capacidad de los cuadros de mando y de los oficiales de estado mayor para comprender la dimensión ciber-electromagnética, incorporar sus efectos en el planeamiento y conducir operaciones en entornos informacionalmente degradados. En este punto, la formación de los cuadros argentinos todavía muestra un énfasis mayor en los dominios físicos tradicionales que en el ciberespacial y el espectral, lo que puede dificultar la incorporación plena de estas variables en la concepción de la maniobra (Rutz, 2019).

Finalmente, debe señalarse que el entorno ciber-electromagnético en el que se inserta el instrumento militar argentino no es autónomo, sino que forma parte de un ecosistema nacional más amplio. Infraestructuras críticas, redes de comunicaciones, centros de datos, proveedores de servicios tecnológicos y organismos responsables de la ciberseguridad civil participan de manera directa o indirecta en la configuración de las condiciones en las que las fuerzas armadas deberán operar. Esto implica que la resiliencia y la seguridad del entorno informacional relevante para la defensa no dependen exclusivamente de decisiones y capacidades militares, sino también de la coordinación interinstitucional y de la existencia de marcos normativos y acuerdos de cooperación adecuados[14].

En síntesis, el diagnóstico preliminar sugiere que, si bien existen capacidades y avances significativos en materia de Ciberdefensa y Guerra Electrónica, persisten desafíos doctrinarios, organizativos, tecnológicos y de recursos humanos que dificultan la adopción plena de un enfoque integrado de actividades ciber-electromagnéticas en el nivel operacional. La realidad argentina presenta, por lo tanto, un escenario dual: por un lado, limitaciones que deben ser reconocidas con realismo y, por otro, oportunidades para aprovechar de manera inteligente los recursos disponibles y para orientar la modernización doctrinaria y organizativa hacia un modelo que responda a las exigencias de las operaciones multidominio.

Sobre esta base, los apartados siguientes propondrán un marco conceptual y un modelo operativo CEMA adaptados a esta realidad, inspirados en las tendencias internacionales analizadas, pero construidos a partir de las necesidades y condicionantes propios del instrumento militar nacional.

3.2 Marco conceptual propuesto para la integración de Guerra Electrónica y Ciberdefensa en el nivel operacional argentino

La formulación de un marco conceptual específico para la integración de la Guerra Electrónica y la Ciberdefensa en el nivel operacional argentino constituye un paso necesario para superar la fragmentación doctrinaria y organizativa identificada en el diagnóstico. El objetivo de este marco conceptual no es reemplazar las definiciones

[14]La creación del Comando Conjunto de Ciberdefensa, la aprobación de la Estrategia Nacional de Ciberseguridad y su actualización reciente, así como diversos acuerdos de cooperación internacional, apuntan precisamente a articular ese ecosistema nacional en torno a objetivos comunes de protección y respuesta ante incidentes (Estado Mayor Conjunto de las Fuerzas Armadas, s.f.; República Argentina, 2019; República Argentina, 2023).

existentes, sino ofrecer una estructura de ideas que permita articularlas bajo una lógica común, centrada en la idea de que el ciberespacio y el espectro electromagnético conforman, en la práctica, un entorno informacional único cuya protección y explotación resultan indispensables para la maniobra.

En primer lugar, el marco conceptual propuesto asume que las actividades ciber-electromagnéticas constituyen un esfuerzo integrado orientado a asegurar la superioridad informacional en apoyo a las operaciones en todos los dominios. Desde esta perspectiva, la GE y la CD no se conciben como sistemas de apoyo aislados, sino como componentes de una misma función operacional cuya finalidad es garantizar la disponibilidad, integridad y confidencialidad de la información propia, al tiempo que se degrada, niega o explota la información adversaria. Esta función se vincula directamente con la capacidad del comandante para ejercer el mando y el control, para coordinar esfuerzos y para conservar la iniciativa frente a un oponente que también busca operar sobre el entorno informacional.

En segundo término, el marco conceptual propone entender el ciberespacio y el espectro electromagnético como un continuo técnico y operacional[15]. El ciberespacio no puede operar sin el soporte físico del espectro, y el empleo militar moderno del espectro depende, casi en su totalidad, de sistemas digitales que pertenecen al ciberespacio. En consecuencia, las acciones diseñadas para proteger o atacar uno de estos ámbitos tendrán, de manera casi inevitable, efectos en el otro. Desde la óptica del nivel operacional, esto significa que resulta artificial planificar por un lado "operaciones cibernéticas" y por otro "acciones de GE", sin una instancia integradora que las conciba como manifestaciones específicas de una misma lógica de empleo.

La tercera idea central del marco conceptual es que las actividades ciber-electromagnéticas deben ser planificadas y conducidas con el mismo rigor que cualquier otra función operacional. Esto implica definir objetivos ciber-electromagnéticos coherentes con el concepto de la operación, identificar centros de gravedad informacionales, establecer prioridades, asignar recursos, diseñar medidas de coordinación y evaluar resultados. En esta lógica, las CEMA no se limitan a "apagar incendios" o a responder a incidentes imprevistos, sino que forman parte del diseño deliberado de la maniobra, con un antes (preparación y modelado del entorno), un durante

[15] El tratamiento conjunto del ciberespacio y del espectro electromagnético se propone cada vez más como un enfoque superador frente a visiones que fragmentan la gestión de redes, comunicaciones y Guerra Electrónica en compartimentos estancos (Casarino & Ortíz, 2019; Trama & de Vergara, 2017).

(apoyo directo a la ejecución de la operación) y un después (evaluación de efectos y lecciones aprendidas).

En cuarto lugar, el marco conceptual propuesto subraya la necesidad de considerar la resiliencia informacional como un objetivo explícito de las actividades ciber-electromagnéticas. Proteger redes, sistemas y enlaces no significa solamente evitar intrusiones o interferencias, sino también estar en condiciones de seguir operando cuando, pese a todas las medidas, se produzcan impactos en el entorno ciber-electromagnético. Esto implica concebir las CEMA no solo como un conjunto de acciones de protección y ataque, sino también como una herramienta para diseñar arquitecturas de mando y control que incorporen redundancias, rutas alternativas, soluciones híbridas y procedimientos simplificados capaces de sostener la maniobra bajo condiciones de degradación.

Una quinta dimensión del marco conceptual remite a la articulación entre actividades ciber-electromagnéticas y otras funciones, como inteligencia, comunicaciones, operaciones de información, protección de la fuerza y logística. En la práctica, las CEMA dependen de la inteligencia para identificar vulnerabilidades y objetivos, necesitan de las comunicaciones para coordinar sus propios medios, influyen sobre la eficacia de las operaciones de información y contribuyen a la protección de fuerzas y de infraestructuras críticas. Por lo tanto, el marco conceptual propone concebir a las actividades ciber-electromagnéticas como un factor transversal que debe integrarse de manera orgánica en los procesos y estructuras que ya gestionan estas funciones, evitando duplicidades y competencias superpuestas.

Finalmente, el marco conceptual incorpora la dimensión conjunta e interinstitucional como una característica constitutiva de las actividades ciber-electromagnéticas en la realidad argentina. Dado que las infraestructuras y capacidades relevantes se distribuyen entre distintas fuerzas, organismos del Estado y actores civiles, resulta imprescindible que cualquier abordaje CEMA contemple la coordinación con estructuras de nivel estratégico y con entidades externas al ámbito estrictamente militar. En el nivel operacional, esto se traduce en la necesidad de disponer de mecanismos de enlace, protocolos de intercambio de información y procedimientos de actuación coordinada ante incidentes que afecten al entorno informacional en el que se desarrollan las operaciones.

En conjunto, este marco conceptual proporciona las bases para la construcción de un modelo operativo CEMA para el nivel operacional argentino. Al definir la finalidad, el ámbito, la lógica de empleo, la relación con otras funciones y la dimensión conjunta e

interinstitucional de las actividades ciber-electromagnéticas, establece los parámetros dentro de los cuales podrán diseñarse estructuras, procesos y procedimientos concretos que materialicen esta integración en la práctica.

3.3 Propuesta de modelo operativo ciber-electromagnético para el nivel operacional argentino

Sobre la base del diagnóstico preliminar y del marco conceptual propuesto, este apartado presenta una propuesta de modelo operativo ciber-electromagnético para el nivel operacional argentino. Se trata de un esquema de referencia que busca ser coherente con las tendencias internacionales analizadas, pero adaptado a las particularidades del instrumento militar nacional, al contexto de recursos disponibles y a la necesidad de avanzar de manera gradual en la integración de la Guerra Electrónica y la Ciberdefensa.

En términos generales, el modelo operativo se articula alrededor de cuatro ejes principales: la organización de una estructura CEMA en los estados mayores operacionales, la integración de las actividades ciber-electromagnéticas en el ciclo de planeamiento, el diseño de un esquema básico de funciones y responsabilidades y la incorporación de la resiliencia informacional como criterio transversal de la maniobra.

El primer eje es organizativo. El modelo propone la creación, o el fortalecimiento cuando existan antecedentes, de una célula o sección CEMA en los estados mayores del nivel operacional conjunto, con reflejos proporcionalmente más reducidos en estados mayores específicos que participen en campañas u operaciones determinadas. Esta estructura CEMA debería estar integrada por personal con formación en Guerra Electrónica y Ciberdefensa, pero también por oficiales con experiencia en operaciones e inteligencia, de modo que se garantice una comprensión compartida del vínculo entre actividades ciber-electromagnéticas y maniobra general.

Esta célula CEMA tendría, entre otras, las siguientes funciones básicas: analizar el entorno ciber-electromagnético del teatro de operaciones, identificar vulnerabilidades y oportunidades informacionales, proponer objetivos CEMA en coherencia con el concepto de la operación, coordinar el empleo de capacidades de GE y CD asignadas al nivel operacional, asesorar al comandante sobre riesgos y limitaciones y contribuir a la planificación de la resiliencia del sistema de mando y control. Para ello, debería mantener vínculos formales y permanentes con las áreas de inteligencia, comunicaciones, operaciones, protección y logística, así como con los organismos responsables de Ciberdefensa y Guerra Electrónica en los niveles superior y específico.

El segundo eje del modelo se refiere a la integración de las actividades ciber-electromagnéticas en el ciclo de planeamiento operacional. El modelo propone que, desde las fases iniciales de la apreciación de la situación, la célula CEMA participe en la identificación de factores informacionales clave del teatro: infraestructuras críticas, dependencias del adversario y propias respecto de redes y sistemas, posibles puntos de quiebre en el entorno ciber-electromagnético y riesgos de afectación de servicios esenciales. Sobre esa base, durante la elaboración de cursos de acción, debería evaluar para cada opción cuáles son las exigencias y vulnerabilidades CEMA asociadas, proponiendo medidas de protección y oportunidades para el empleo ofensivo de capacidades ciber-electromagnéticas.

En la fase de decisión, el modelo contempla que el concepto de la operación incluya, de manera explícita, una concepción CEMA que indique qué efectos se persiguen sobre el entorno informacional y cómo se coordinarán los esfuerzos de GE y CD con otras funciones. Durante la ejecución, la célula CEMA debería participar en la conducción, monitoreando el comportamiento del entorno ciber-electromagnético, proponiendo ajustes y coordinando respuestas ante incidentes que afecten al mando y control, a las comunicaciones o a las infraestructuras críticas. Finalmente, en la fase de evaluación, tendría la responsabilidad de contribuir a las lecciones aprendidas, identificando aciertos y deficiencias en el empleo de las actividades ciber-electromagnéticas.

El tercer eje del modelo se vincula con la definición de funciones y responsabilidades básicas en materia CEMA. Sin pretender agotar el detalle, el modelo distingue tres grandes líneas de esfuerzo: protección, explotación y ataque. La protección comprende todas las medidas destinadas a asegurar la continuidad y seguridad de las redes, sistemas y enlaces propios, incluyendo coordinación con organismos de Ciberdefensa y con proveedores de servicios críticos cuando corresponda. La explotación abarca el uso de capacidades ciber-electromagnéticas para obtener información sobre el adversario, identificar patrones de emisión, detectar vulnerabilidades y alimentar los procesos de inteligencia. El ataque incluye el empleo de GE y de herramientas cibernéticas para degradar, negar o manipular las capacidades informacionales del adversario, siempre dentro del marco normativo vigente y de las directivas superiores.

En el nivel operacional argentino, estas funciones no necesariamente implican disponer de capacidades orgánicas sofisticadas en todos los campos, pero sí contar con la capacidad de solicitar, coordinar y orientar el empleo de los medios disponibles en otros escalones o ámbitos. El modelo, por lo tanto, concibe la célula CEMA operacional como

un “gestor de efectos” más que como un mero operador técnico, responsable de traducir necesidades operacionales en requerimientos ciber-electromagnéticos y de integrar las respuestas recibidas en la maniobra general.

El cuarto eje, transversal a los anteriores, es la incorporación de la resiliencia informacional como criterio central del modelo. Esto se traduce en la exigencia de que cada campaña u operación planificada considere, desde su diseño, escenarios de degradación ciber-electromagnética. La célula CEMA, en coordinación con comunicaciones, operaciones y logística, debería proponer esquemas de redundancia, medios alternativos de enlace, prioridades de protección de sistemas, procedimientos para operar con información parcial y protocolos para la continuidad del mando en caso de afectar nodos críticos. El objetivo no es eliminar el riesgo, algo imposible, sino reducir la probabilidad de colapso funcional frente a ataques o incidentes en el entorno informacional.

Por último, el modelo reconoce que la realidad argentina requiere una implementación gradual y realista. La creación de estructuras CEMA en el nivel operacional, la integración de estas actividades en el planeamiento y la consolidación de una cultura organizacional que valore la dimensión ciber-electromagnética demandarán tiempo, recursos y ajustes sucesivos. En esta perspectiva, el modelo operativo propuesto debe entenderse como una hoja de ruta flexible, susceptible de adaptarse a la evolución doctrinaria, tecnológica y organizativa del instrumento militar nacional, pero lo suficientemente clara como para orientar decisiones concretas en el corto y mediano plazo.

En conjunto, el marco conceptual y el modelo operativo CEMA propuestos en este capítulo buscan responder a la pregunta central de la investigación: cómo integrar de manera efectiva la Guerra Electrónica y la Ciberdefensa en el nivel operacional argentino, en un contexto de operaciones multidominio y de creciente disputa por el entorno informacional. Las conclusiones generales, retomarán los principales aportes de este recorrido y señalarán posibles líneas de desarrollo futuro para fortalecer las capacidades nacionales en este campo.

Desde la perspectiva de la Acción Militar Conjunta argentina, el modelo operativo propuesto se apoya en algunos principios que orientan el empleo de las actividades ciber-electromagnéticas en el nivel operacional. En primer lugar, la protección y el empleo ofensivo en el continuo ciber-electromagnético deben vincularse explícitamente con los centros de gravedad, las capacidades críticas y las vulnerabilidades del adversario y de la

propia fuerza, evitando tratamientos genéricos o desligados de la maniobra. En segundo lugar, la integración CEMA exige una participación temprana de la célula especializada en el ciclo de planeamiento, de manera que sus aportes influyan en la definición de cursos de acción y no se limiten a ajustes tardíos de carácter técnico. En tercer lugar, la unidad de concepción en materia CEMA debe combinarse con una ejecución descentralizada, que permita a los comandantes subordinados disponer de márgenes de acción dentro de un marco de coordinación y control de efectos.

En cuarto lugar, el modelo operativo considera imprescindible articular de manera sistemática el nivel operacional con los organismos de nivel estratégico responsables de la Ciberdefensa, así como con los actores civiles que gestionan infraestructuras críticas relevantes para la conducción de las operaciones. Esta articulación apunta a superar la fragmentación entre ámbitos técnico–especializados y el planeamiento conjunto, y a asegurar que las decisiones sobre el empleo de capacidades CEMA contemplen tanto las restricciones jurídicas como las eventuales implicancias sobre servicios esenciales para la población. En conjunto, estos principios buscan traducir la noción de continuo ciber-electromagnético en prácticas concretas de conducción en el teatro de operaciones.

CONCLUSIONES GENERALES

El presente Trabajo Final Integrador se propuso responder cómo deben planificarse e integrarse las actividades ciber-electromagnéticas bajo la concepción de Operaciones Multidominio para mejorar la coordinación y la efectividad de la acción militar conjunta, particularmente en el nivel operacional de las Fuerzas Armadas argentinas. Para ello se definió como objetivo general analizar el empleo y la evolución de la Guerra Electrónica (GE) y la Ciberdefensa (CD) en el período 2014–2024, y elaborar un marco conceptual y un modelo operativo que permitan su integración en el nivel operacional, orientados a fortalecer la superioridad informacional y la interoperabilidad conjunta. Este objetivo se operacionalizó mediante tres objetivos específicos: describir la evolución doctrinaria de la GE y la CD y su convergencia en el concepto de actividades ciber-electromagnéticas (CEMA); analizar doctrinas y experiencias operacionales internacionales relevantes, con énfasis en Estados Unidos, Reino Unido y los conflictos de Ucrania y Georgia; y desarrollar, sobre la base de un diagnóstico preliminar de la situación argentina, un marco conceptual y un modelo operativo CEMA adaptados al nivel operacional nacional. La hipótesis sostuvo que la integración sinérgica de GE y CD en un enfoque ciber-electromagnético, concebido y gestionado desde el nivel operacional en el marco de las Operaciones Multidominio, contribuye de manera significativa a mejorar la interoperabilidad, optimizar la respuesta frente a amenazas complejas y aumentar la eficacia operativa del instrumento militar argentino.

En relación con el primer objetivo específico, el análisis de la evolución de la Guerra Electrónica y la Ciberdefensa permitió demostrar que ambas disciplinas han transitado desde enfoques técnicos relativamente aislados hacia una concepción integrada, en la que el ciberespacio y el espectro electromagnético se entienden como partes de un mismo entorno informacional. La creciente digitalización de los sistemas de mando y control, comunicaciones, sensores y apoyos críticos generó una interdependencia estructural entre estos dominios, haciendo insuficiente la separación rígida entre “lo electrónico” y “lo cibernético”. A partir de este proceso, la noción de actividades ciber-electromagnéticas surge como categoría que sintetiza esta convergencia y la orienta a la obtención de superioridad informacional y a la protección de la libertad

de acción en todos los dominios. Puede concluirse, por lo tanto, que el trabajo cumplió con el propósito de describir y fundamentar la evolución de GE y CD hacia un enfoque CEMA, mostrando que esta integración responde a transformaciones profundas en el carácter de la guerra y no solo a la incorporación de nuevas tecnologías.

En cuanto al segundo objetivo específico, el estudio de las doctrinas de Estados Unidos y del Reino Unido, junto con el análisis de los conflictos en Ucrania y Georgia, permitió identificar tendencias claras en la forma en que las potencias militares más avanzadas conciben e implementan la integración ciber-electromagnética. En el plano doctrinario, se observa la decisión de tratar las CEMA como un esfuerzo integrado que debe planificarse desde el nivel operacional, con estructuras específicas en los estados mayores, participación temprana en el ciclo de planeamiento y una lógica de empleo orientada a efectos concretos sobre el sistema de mando y control propio y adversario. En el plano operacional, los casos de Ucrania y Georgia muestran que el empleo combinado de operaciones cibernéticas, Guerra Electrónica, campañas de desinformación y maniobra convencional puede modificar de manera significativa la relación de fuerzas, tanto en el campo de batalla como en la dimensión política y cognitiva. Al mismo tiempo, evidencian que la falta de preparación suficiente en materia CEMA se traduce rápidamente en pérdida de iniciativa, degradación acelerada del mando y control y dificultades para sostener la cohesión interna y la narrativa estratégica. De ello se concluye que el objetivo de analizar doctrinas y experiencias internacionales para extraer criterios útiles para el diseño de un modelo adaptado a la realidad argentina ha sido alcanzado, en la medida en que se identificaron principios, estructuras y prácticas transferibles, aunque requieran adaptaciones al contexto nacional.

Respecto del tercer objetivo específico, el diagnóstico preliminar de la situación argentina en materia ciber-electromagnética permitió reconocer la existencia de avances relevantes, pero también de brechas significativas. Se constató que las Fuerzas Armadas argentinas han incorporado progresivamente la importancia del ciberespacio y del espectro, a través de la creación y fortalecimiento de estructuras de Ciberdefensa y Guerra Electrónica, de la actualización de algunos documentos doctrinarios y de la formación de especialistas. Sin embargo, también se identificó una fragmentación doctrinaria y organizativa que dificulta la articulación estable de capacidades CEMA en el nivel operacional conjunto, la dispersión de competencias entre distintos organismos, limitaciones tecnológicas y de recursos humanos y una fuerte dependencia de infraestructuras civiles para servicios críticos de comunicaciones y datos. Sobre esta base,

el trabajo propuso un marco conceptual que concibe al ciberespacio y al espectro como un entorno informacional único, que entiende las actividades ciber-electromagnéticas como una función transversal destinada a asegurar superioridad informacional y resiliencia del mando y control, y que enfatiza su integración con inteligencia, comunicaciones, operaciones de información, protección de la fuerza y logística. A partir de ese marco se diseñó un modelo operativo CEMA para el nivel operacional argentino, centrado en la organización de células o secciones CEMA en los estados mayores operacionales, en su participación sistemática a lo largo de todo el ciclo de planeamiento, en la gestión de líneas de esfuerzo en protección, explotación y ataque, y en la incorporación explícita de la resiliencia informacional como criterio de diseño de campañas y operaciones. De este modo, puede afirmarse que el objetivo de elaborar una propuesta conceptual y operativa adaptada al contexto argentino se encuentra cumplido.

Considerando el conjunto de los resultados obtenidos, la hipótesis de trabajo se confirma en sus líneas principales. El análisis realizado sugiere que la integración sinérgica de la Guerra Electrónica y la Ciberdefensa bajo un enfoque ciber-electromagnético, concebido y gestionado desde el nivel operacional en el marco de las Operaciones Multidominio, constituye una vía eficaz para mejorar la interoperabilidad entre componentes, optimizar la respuesta frente a amenazas complejas y aumentar la eficacia operativa del instrumento militar. La experiencia internacional muestra que los actores que han desarrollado estructuras CEMA en el nivel operacional, con una lógica de empleo orientada a efectos y con atención prioritaria a la resiliencia informacional, han incrementado su capacidad para preservar la libertad de acción y adaptarse a entornos de alta complejidad. La propuesta de marco conceptual y de modelo operativo elaborada en este trabajo indica que es posible trasladar esos principios al caso argentino mediante un esquema gradual, que combina realismo respecto de los recursos disponibles con una orientación clara hacia la integración ciber-electromagnética como componente estructural de la maniobra.

Al mismo tiempo, es necesario reconocer las limitaciones del estudio. El análisis se basó en fuentes abiertas y documentación de dominio público, lo que condiciona el nivel de detalle alcanzable en relación con capacidades, procedimientos y estructuras de alta sensibilidad. La rápida evolución tecnológica en el campo ciber-electromagnético obliga, además, a considerar las conclusiones como una fotografía de un momento determinado, que requerirá revisiones periódicas a medida que se incorporen nuevos sistemas y se modifiquen las condiciones del entorno estratégico. Finalmente, el modelo operativo

propuesto tiene un carácter general y necesita ser contrastado con ejercicios concretos, experiencias de adiestramiento y evaluaciones de Estado Mayor que permitan validar, ajustar o reformular sus componentes en función de la práctica.

Estas limitaciones abren, a la vez, líneas de desarrollo futuro. Entre ellas se destacan la conveniencia de realizar estudios centrados en ejercicios conjuntos nacionales en los que se incorporen de manera explícita actividades ciber-electromagnéticas; la necesidad de profundizar la definición de perfiles y requerimientos de capacitación de los cuadros de estado mayor en materia CEMA; la importancia de analizar en mayor detalle el marco normativo aplicable al empleo de estas capacidades en paz, crisis y conflicto; y la oportunidad de explorar alternativas tecnológicas escalables que fortalezcan la resiliencia informacional del instrumento militar. En síntesis, el trabajo permite concluir que la integración de la Guerra Electrónica y la Ciberdefensa bajo un enfoque ciber-electromagnético, articulada en un modelo operativo adecuado al nivel operacional argentino, no solo es coherente con las tendencias doctrinarias internacionales, sino que constituye una necesidad para preparar a las Fuerzas Armadas frente a un entorno estratégico en el que la disputa por la información y por los soportes que la hacen posible se ha convertido en un rasgo permanente de la competencia y del conflicto contemporáneo.

BIBLIOGRAFÍA

Alaniz Miranda, O. (2018). Las actividades ciberelectromagnéticas: Un combate invisible. Escenarios actuales, 23(2), 15–24.

Aldea Gracia, P. L. (1988). Aspectos conjuntos de la guerra electrónica. Boletín de Información, (208).

Baezner, M., & Robin, P. (2017). Cyber and information warfare in the Ukrainian conflict (Hotspot Analysis). Center for Security Studies (CSS), ETH Zürich.

Casale, C. G. (2022). Convergencia de las operaciones de guerra electrónica y ciberdefensa para su empleo dentro de un teatro [Trabajo final integrador, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas].

Casarino, P. G., & Ortíz, J. U. (2019). La ciberdefensa y la ciberinteligencia militar. Visión Conjunta, 11(21), 43–52.

Ciberdefensa: El desafío de las nuevas generaciones. (2018, 9 noviembre). Argentina.gob.ar. https://www.argentina.gob.ar/noticias/ciberdefensa-el-desafio-de-las-nuevas-generaciones

Department of the Air Force. (2023). Air Force doctrine publication 3-12: Cyberspace operations. Department of the Air Force.

Department of the Army. (2014). Cyber electromagnetic activities (Field Manual FM 3-38). Headquarters, Department of the Army.

Eissa, S. G., & Albarracín Keticoglu, A. (2020). La ciberdefensa en su laberinto: Cambio de rumbo en la concepción de ciberdefensa durante la gestión de Mauricio Macri (2015–2019). Defensa Nacional, (5).

Estado Mayor Conjunto de las Fuerzas Armadas. (s.f.). Comando Conjunto de Ciberdefensa. Argentina.gob.ar. https://www.argentina.gob.ar/estado-mayor-conjunto/comando-conjunto-de-ciberdefensa

Estado Mayor Conjunto de las Fuerzas Armadas. (s.f.). Función del Comando Conjunto de Ciberdefensa. Argentina.gob.ar. https://www.argentina.gob.ar/historia-del-comando-conjunto-de-ciberdefensa/funcion-del-comando-conjunto-de-ciberdefensa

Gago, E. A. (2017). El enfoque argentino sobre ciberseguridad y ciberdefensa [Trabajo final de licenciatura, Escuela Superior de Guerra “Tte. Grl. Luis María Campos”].

Haig, Z. (2015). Electronic warfare in cyberspace. Security and Defence Quarterly, 7(2), 22–35.

Hillebrand, G. D. (Ed.). (2023). Strategic cyberspace operations primer. U.S. Army War College, Center for Strategic Leadership.

Joint Chiefs of Staff. (2018). Joint publication 3-12: Cyberspace operations. U.S. Department of Defense.

Moyano, T. R. (2020). La República Argentina y sus esfuerzos en ciberdefensa: El compromiso con las buenas prácticas como parte de su ideario. Visión Conjunta, 12(22), 50–63.

North Atlantic Treaty Organization. (2024, July 30). Cyber defence. NATO. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

Osorio Lalinde, A., Lorduy López, G., Amaya Henao, L. M., & Arenas Méndez, T. (2017). Ciberseguridad y ciberdefensa: Pilares fundamentales de la seguridad y defensa nacional. Revista de las Fuerzas Armadas, (241).

Reale, J. (2023). Los desafíos de la ciberguerra y la importancia de fortalecer la inteligencia estratégica militar en la Argentina. Revista de la Escuela Nacional de Inteligencia, (2), 69–98.

República Argentina. Jefatura de Gabinete de Ministros, Secretaría de Gobierno de Modernización. (2019, 24 mayo). Estrategia Nacional de Ciberseguridad (Resolución 829/2019). Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528

República Argentina. Jefatura de Gabinete de Ministros. (2023, 5 septiembre). Se aprobó la Segunda Estrategia Nacional de Ciberseguridad. Argentina.gob.ar. https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad

República Argentina. Ministerio de Defensa. (2015). Libro blanco de la defensa 2015. Ministerio de Defensa.

República Argentina. Ministerio de Defensa. (2023). Libro blanco de la defensa 2023. Ministerio de Defensa.

República Argentina. Poder Ejecutivo Nacional. (2021, 14 julio). Decreto 457/2021: Directiva de Política de Defensa Nacional. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/246990/20210719

Rutz, G. (2019). Ciberdefensa y formación de posgrado en Argentina: Indagaciones preliminares para un aporte al desafío ciber de la defensa nacional. Defensa Nacional, (3).

Trama, G. A., & de Vergara, E. A. (2017). Operaciones militares cibernéticas: Planeamiento y ejecución en el nivel operacional. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Tikk, E., Kaska, K., Rünnimeri, A., Kert, M., Talihärm, A., & Vihul, L. (2008). *Cyber attacks against Georgia: Legal lessons identified*. Cooperative Cyber Defence Centre of Excellence.

UK Ministry of Defence. (2018). Cyber and electromagnetic activities (Joint Doctrine Note 1/18). Development, Concepts and Doctrine Centre.

U.S. Army Training and Doctrine Command. (2018). The U.S. Army in multi-domain operations 2028 (TRADOC Pamphlet 525-3-1). U.S. Army Training and Doctrine Command.