TRABAJO FINAL INTEGRADOR

TEMA:

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

TÍTULO:

Convergencia de las Operaciones de Guerra Electrónica y Ciberdefensa para su empleo dentro de un Teatro.

AUTOR: MAYOR (EA) CARLOS GERARDO CASALE

TUTOR: CORONEL (EA) LUIS PABLO GUIMPEL

Año 2022

RESUMEN

Los adelantos tecnológicos surgidos de las distintas revoluciones industriales dieron nacimiento a las Nuevas Tecnologías de la Información y la Comunicación (TICS) que tuvieron un fuerte impacto en la revolución de asuntos militares y su consecuente influencia en el campo de combate moderno ya que permitieron apoyar y complementar las operaciones tradicionales mediante la ejecución de operaciones militares con cada vez mayor influencia y capacidad de determinación en el curso de los conflictos.

La presente investigación alude a la integración entre las Operaciones de Ciberdefensa y las Operaciones de Guerra Electrónica en el ámbito del nivel operacional de las Fuerzas Armadas (FFAA). En este sentido, se contempla principalmente la doctrina actual de algunos países miembros de la Organización del Tratado del Atlántico Norte (OTAN) y, excepcionalmente, algunos países de América del Sur, para determinar cómo vinculan ambas operaciones y cómo las llevan a cabo.

En los países como Estados Unidos, Reino Unido, España o Alemania, miembros de la OTAN, la vinculación, su planificación y/o ejecución, así como la forma en que estructuran la organización entre ambos tipos de operaciones se encuentra inserta en la doctrina con el nombre de *Cyber and Electromagnetic Activities* (CEMA), por sus siglas en inglés, desde hace años. Asimismo poseen la experiencia real de haberlas podido desarrollar en conflictos, de forma que ambas se complementen pudiendo perfeccionar las técnicas de su concreción.

En América del Sur, algunas fuerzas armadas, también han abordado este tema incorporando las actividades ciberelectromagnéticas dentro de su vocabulario.

En el plano local, en el ámbito conjunto como específico, existe doctrina y elementos de planeamiento que abordan la temática planteada pero de manera separada; contemplan ambos tipos de operaciones pero no como complementarias entre sí o bajo un mismo elemento de planificación y ejecución.

De acuerdo a lo descripto hasta el momento en los párrafos previos, éste trabajo de investigación propone como objetivo general describir la vinculación entre ambos tipos de operaciones en el nivel operacional para determinar los beneficios de implementarlo en el plano local conjunto.

Como interrogante surge ¿cómo la convergencia entre las operaciones de ciberdefensa y guerra electrónica bajo un único elemento de comando facilita su ejecución en el nivel operacional?

Palabras claves: Operaciones, Electrónica, Ciberdefensa, Integración, Ciberespacio.

ÍNDICE

RESUMEN i
ÍNDICE ii
INTRODUCCIÓN 1
CAPITULO 1 9
CONVERGENCIA ENTRE OPERACIONES DE CIBERDEFENSA Y GUERRA ELECTRÓNICA EN PAÍSES DE LA OTAN 9
Conceptos generales 9
Convergencia de ambas operaciones en las FFAA de la República Federal de Alemania 10
Convergencia de ambas operaciones en las FFAA de España 12
Convergencia de ambas operaciones en las FFAA del Reino Unido de Gran Bretaña 14
Convergencia de ambas operaciones en las FFAA de los Estados Unidos de América 19
CAPÍTULO II 23
SITUACIÓN NACIONAL ACTUAL PARA EL DESARROLLO DE OPERACIONES DE CIBERDEFENSA Y GUERRA ELECTRÓNICA 23
Conceptos generales 23
Estructura Nacional Actual 23
CONCLUSIONES FINALES 28
BIBLIOGRAFÍA 31

INTRODUCCIÓN

La influencia de la tecnología en el desarrollo de operaciones militares ha ido en aumento junto con su evolución a través de nuevos y mejores medios. Esto ha llevado a la aparición de nuevas formas de llevar a cabo operaciones en los distintos dominios que componen el ambiente operacional y la configuración de nuevos dominios.

Este es el caso del Ciberespacio, dominio creado íntegramente por el hombre, donde se desarrollan las Operaciones de Ciberdefensa destinadas a proteger la Infraestructura Crítica del Sistema de Defensa Nacional y aquellas de nivel nacional que sean asignadas a las fuerzas armadas como Objetivos de Valor Estratégico, así como asegurar el empleo del propio Ciberespacio y negarlo al enemigo.

Relacionado con los adelantos tecnológicos que revolucionaron los asuntos militares, pero cronológicamente previo a la Ciberdefensa, aparecen en el ámbito de las comunicaciones e informática las operaciones de Guerra Electrónica junto con los medios que permiten llevarlas a cabo. Estas buscan el control del espectro electromagnético asegurando el propio empleo y negándolo al enemigo; afectando el empleo eficiente de aquellos equipos militares que lo emplean.

Ambos tipos de operaciones buscan afectar el comando y control del oponente para dificultar su accionar coordinado y ordenado, contribuyendo a su dislocamiento sistémico.

En relación a lo descripto en los párrafos precedentes, la presente investigación tiene la intención de identificar y plasmar la convergencia existente entre las operaciones de ciberdefensa y guerra electrónica realizando un análisis descriptivo y explicativo sobre algunos miembros de la OTAN en materia de organización y ejecución, en el marco conjunto, de dicho tipo de operaciones y su aplicación en el ámbito nacional dentro de un teatro de operaciones (TO).

Desde hace años, la constante evolución tecnológica ha ido incidiendo en forma creciente en el desarrollo de los conflictos armados. Introduciendo cada vez más y mayores medios tecnológicos que permiten el desarrollo de operaciones que complementan o permiten el desarrollo de las operaciones tradicionales con menor pérdida del recurso humano. El empleo de estos medios se da en todos los niveles de la conducción, desde el táctico hasta el estratégico pasando por el operacional.

Gracias a los inventos y descubrimientos de hombres como Hertz, con la producción de ondas electromagnéticas y la medición de la longitud de onda, o Marconi, con la primera transmisión de radio, se logró el empleo del espectro electromagnético a través del cual se propaga la energía electromagnética, que con el correr del tiempo se empleó para las

comunicaciones por voz y datos mediante equipos especializados que irradian este tipo de energía.

Es a partir de la Segunda Guerra Mundial "que adquiere mayor relevancia el uso de las comunicaciones radioeléctricas, dándole importancia al empleo del espectro electromagnético. Se presume que mediante el uso de los medios electrónicos, durante este conflicto, se dio inicio a lo que hoy denominamos guerra electrónica" (Rojas 2014, p 3).

Posteriormente, en los conflictos armados, uno de los objetivos fue el control de este dominio para asegurar el propio empleo e impedir el del enemigo permitiendo el comando y control en el desarrollo de las operaciones.

De acuerdo a lo expresado en el trabajo de Diseño y Planificación de las actividades de Guerra Electrónica en el ambiente operacional (Herrera, 2017) el empleo de componentes electrónicos en los distintos sistemas, comando y control-armas, que operan dentro del campo de combate han dado una ventaja cualitativa a quien lo posea; pero paralelamente se desarrollaban dispositivos de guerra electrónica que protegían o neutralizaban los del oponente. Resalta la importancia para un comandante contar con un sistema que le permita, en tiempo real, el control de las operaciones mediante la impartición de órdenes sin ser afectadas por la acción del enemigo. Hasta los signa como un factor determinante a tener en cuenta dentro del planeamiento y ejecución de las acciones.

Este tipo de operaciones deben realizarse previamente y durante el desarrollo del conflicto en todos los ambientes conocidos (tierra, aire, mar y espacio) para permitir el diligenciamiento de la información entre todas las fuerzas que operan dentro del teatro de operaciones.

Según el Coronel Zsolt Haig (2017) afirma que "la guerra electrónica juega un rol muy importante en cualquier operación militar, en el nivel que sea" (p 3). Las fuerzas armadas realizan e integran este tipo de operaciones a las tradicionales para interrumpir y/o aumentar el tiempo de reacción en la toma de decisiones del enemigo. También aporta a la propia fuerza información sobre los sistemas electromagnéticos del enemigo, otorgando al comandante un conocimiento más detallado de las capacidades que puede desarrollar éste.

Según el reglamento de Guerra Electrónica para las Acción Militar Conjunta, PC 13-50 (Estado Mayor Conjunto, 2012), actualmente los equipos electromagnéticos se emplean con mayor continuidad en los conflictos militares para cumplir tareas o actividades de inteligencia, comunicaciones, navegación, procesamiento o almacenamiento de información. Esto marca una dependencia de las operaciones de este tipo de equipamiento. Su utilización, genera un ambiente denominado ambiente electromagnético.

Las operaciones que se ejecutan en este ambiente a través de los medios que operan en él son las operaciones de guerra electrónica que buscan generar efectos que contribuyan al cumplimiento de los objetivos.

Las operaciones de guerra electrónica no solo deben estar en capacidad de controlar las comunicaciones que desarrolla el enemigo para restringirlas o negarlas, sino también poder direccionarlas al empleo de medios que puedan ser controlados o monitoreados por las tropas técnicas específicas. Los medios que ejecutan este tipo de operaciones son empleados con el fin de lograr un efecto determinado sobre el enemigo. En relación a esto dependerá la selección de la capacidad a emplear.

El PC 13–50 (Estado Mayor Conjunto, 2012) contempla como clasificación de las Tareas de guerra electrónica, el Apoyo de Guerra Electrónica dirigidas a la obtención de información mediante una serie de actividades con el fin de proporcionar bases para planificar y conducir operaciones; el Ataque Electrónico con el fin de degradar, neutralizar o destruir la capacidad del enemigo; y la Protección Electrónica que son el conjunto de acciones destinadas a proteger personal y medios mediante la neutralización de los efectos que puedan causar las operaciones del enemigo.

En el libro Guerra Electrónica Martínez (2013) asegura que la guerra ha evolucionado y como consecuencia de ello, en las guerras de cuarta generación se ha incrementado el empleo de la guerra electrónica y el rol que desempeña dentro de estos conflictos, los que se caracterizan por la asimetría. Resalta que en la doctrina de Estados Unidos para el empleo de los medios de la defensa nacional, establece prioridades para comenzar las operaciones dentro de un teatro. Una de ellas ante todo es alcanzar el dominio del espectro electromagnético para asegurar el propio empleo beneficiando a las propias fuerzas. Esto para proteger y asegurar los sistemas de comando y control entre los distintos niveles, la explotación de los sensores y distintos sistemas de armas para que puedan cumplir con sus objetivos impuestos limitando la influencia que pueda tener el adversario.

La función principal que permitirá el control del espectro, es el transporte de información, es por esto que la guerra electrónica es un componente crítico dentro del teatro de operaciones para la conducción de las fuerzas que en él se actúen.

En relación con los antecedentes de la ciberdefensa los avances en la tecnología, citados previamente, producidos por el hombre han influido en todos los ámbitos de las personas incluidas las acciones que se desarrollan dentro del campo de combate. Estos avances relacionados al empleo de computadoras, redes, satélites, enrutadores, todo aquel dispositivo de conexión y la transferencia de información a través de ellos; han dado origen al ciberespacio

con nuevas y complejas amenazas. Estos adelantos han producido una transformación permanente en las fuerzas armadas debiendo adaptarse a escenarios cada vez más complejos. La adaptación ha incluido al ciberespacio contemplado como un nuevo, el quinto, dominio el cual no tiene fronteras físicas dentro del ámbito de las operaciones. Esta transformación trajo consigo una revolución de los asuntos militares.

Brett (2014) señala que en el ciberespacio se integran las operaciones terrestres, marítimas y espaciales para alcanzar objetivos de la campaña.

Collantes (2012) enuncia que con el surgimiento del ciberespacio como una nueva dimensión en la que se materializan diferentes amenazas que han ido modificando el escenario tradicional en el ámbito de la defensa, que solo consideraba los dominios tradicionales y lo señala cómo un dominio más intangible que el resto. Es por esto que las naciones han creado elementos especializados en la defensa de éste.

Relacionado a que no existe una única definición de ciberdefensa, ya que cada estado y/u organización han realizado la suya propia.

La Junta Interamericana de Defensa (2020) conceptualiza al ciberespacio como en ámbito en el cual se llevan a cabo las actividades de ciberdefensa, resaltando la importancia de tener una clara y precisa idea de su naturaleza y particularidades.

La ciberdefensa pasó a ser un aspecto fundamental en la conducción y ejecución de las operaciones militares actuales. La libertad de acción que se logre en el empleo y control del ciberespacio dependerá de las capacidades que se puedan desarrollar para brindar la protección necesaria para lograr defenderse de las operaciones que realice la voluntad en oposición (Lacroix 2020).

De acuerdo a lo expresado en el reglamento de terminología conjunta se entiende como ciberdefensa al “Conjunto de acciones desarrolladas en el ciberespacio de interés del sistema de defensa para prevenir y/o contrarrestar toda amenaza o agresión cibernética” (Estado Mayor Conjunto 2015, p 42).

Según el artículo La Ciberdefensa y sus efectos en el campo de Batalla (infodefensa.com, 2017) se refiere a la ciberdefensa y sus efectos en el campo de batalla, en relación al ciberespacio considera que es importante tenerlo en desde el punto de vista conjunto, porque se ha hecho un dominio crítico para el desarrollo de las operaciones militares como una extensión del campo de batalla. Y con respecto a la ciberdefensa aclara que debe asegurar el dominio y garantizar el libre acceso al ciberespacio para permitir la conducción eficiente y eficaz de las operaciones militares.

En el presente, tanto el empleo del espectro electromagnético para el desarrollo de operaciones de guerra electrónica, cómo el del ciberespacio para operaciones de ciberdefensa son esenciales en el desarrollo de los conflictos modernos. Las fuerzas armadas emplean redes informáticas que transmiten por ondas, sensores para obtener la ubicación del enemigo, equipos radioeléctricos para establecer las comunicaciones y equipos de bloqueo de señales que logran interrumpir las comunicaciones. Todos estos medios pueden ser afectados mediante procedimientos informáticos o electrónicos o una combinación de ambos. Por lo descripto previamente es que existe una importante interdependencia entre ambos tipos de operaciones, en donde es necesario poseer conocimientos o técnicas de empleo de ambas.

De Vergara (2017) concluye que las actividades ciberelectromagnéticas permiten sincronizar las operaciones en el ciberespacio, las de guerra electrónica y la gestión del espectro electromagnético, con la finalidad de crear o combinar efectos que posibiliten superar las diferencias entre operaciones defensivas y ofensivas.

Según establece el artículo de Martínez (elradar.es, 2020) ambos tipos de operaciones se basan en el empleo de la tecnología de la información y comunicación (TICS) pero han aparecido y se han evolucionado en forma separada. Salvando las diferencias doctrinarias, tecnológicas. Expresa que la guerra electrónica siempre fue relacionada con el empleo y control del espectro electromagnético, mientras que la ciberdefensa se asocia con la defensa y ataque de los sistemas informáticos mediante sus redes. Pero a partir de los últimos años, esto fue cambiando a raíz de los cambios en las características de los conflictos y la convergencia y empleo de equipos tecnológicos con finalidades similares. Se atribuye que esta convergencia entre ambos ámbitos operativos se dio luego del conflicto en el Donbass en el año 2014 en donde las limitaciones operativas de la OTAN, concretándose en el reglamento FM 3–38 del Ejército de los Estado Unidos.

De acuerdo a lo expresado por el Coronel Zslot (2017) ambos dominios no son lo mismo pero existe una convergencia entre los dos. En donde un rasgo del ciberespacio es que los sistemas de información y comunicación en red que operan en él una de las formas de operación es mediante el uso del espectro electromagnético. Una de las características del ciberespacio es que no puede existir sin poder explotar la existencia del espectro electromagnético, sin ella muchas tecnologías de la información y la comunicación no podrían conectarse entre sí solo dependiendo de conexiones físicas. Dentro del campo de batalla actual, una gran cantidad de sistemas de red (los de configuración móvil) emplean energía electromagnética para realizar la transmisión, almacenamiento y recopilación de datos e información. Los agrupa como parte del entorno de la información, definido como el espacio físico y virtual en donde la información

es recibida, procesada y transmitida. Existe una superposición entre ambos en donde el resultado es la multiplicidad de efectos. Algunos denominan al entorno operacional donde se desarrollan las actividades electromagnéticas como Cyber.

Este tipo de actividades han sido reconocidas y empleadas por el ejército de los Estados Unidos de Norteamérica desde el año 2014. Como parte de su doctrina posee un reglamento específico, el FM 3–38, en el que se desarrolla todos los aspectos relacionados a este tipo de actividades. De acuerdo a este documento, la conceptualiza como "aquellas actividades que tienen como objetivo aprovechar, retener y explotar una ventaja sobre el enemigo o adversario en el ciberespacio y en el espectro electromagnético, mientras que simultáneamente, niegan o degradan el empleo de los mismos por parte del enemigo y buscan proteger los sistemas de comando propios" (p. 1–1).

En el Reino Unido de Gran Bretaña, dentro de su doctrina, el Centro de Desarrollo de Conceptos y Doctrina del Ministerio de Defensa, en la segunda edición del "Cyber Primer" o "Cartilla Cibernética" por sus siglas en inglés (2016) en el capítulo 3, especifica las funciones cibernéticas y analiza los tipos de operaciones militares cibernéticas y la relación de estas y otras operaciones militares. Dentro de este documento explica cómo debe tomarse la relación entre lo ciber y electromagnético denominándolo como actividades ciberelectromagnéticas. Subraya que vinculando ambas se puede generar los efectos deseados en mayor medida y especifica que para agilizar la coordinación entre ambas se debe crear el Grupo Conjunto de CEMA (JCG, por sus siglas en inglés).

En función de lo descripto hasta el momento es que la presente investigación trata de mostrar la importancia, en la acción militar conjunta (AMC), qué beneficios proporciona contar con un elemento que vincule la conducción y planificación de ambos tipos de operaciones, permitiendo reducir los tiempos de ejecución y optimizar el funcionamiento del sistema.

Esto da lugar al interrogante o el problema a resolver que es ¿cómo la convergencia entre las operaciones de ciberdefensa y guerra electrónica bajo un único elemento de comando facilita su ejecución en el nivel operacional?

Para delimitar el alcance que se propone en éste trabajo, cabe aclarar que solo se enfocará en el nivel operacional el cual tiene la particularidad de ser aquel en el que las tres FFAA operan de manera conjunta. Busca obtener un punto de vista objetivo en cuanto a la relación existente entre las operaciones de ciberdefensa y las de guerra electrónica, cómo se vinculan y su aplicación en este nivel de la conducción.

Para el desarrollo de ello se empleará doctrina disponible, con clasificación de seguridad pública, principalmente de países miembros de la OTAN, documentos y artículos

extraídos de internet. Asimismo, se analizará, en base a la experiencia que adquirieron los miembros del Tratado del Atlántico Norte, cómo logran esa vinculación, las bondades que brinda y la estructura responsable de concretarlas. En la actualidad, dentro del ámbito local, no se posee doctrina específica del tema en cuestión en el nivel conjunto.

No se analizarán aspectos técnicos ni tecnológicos referidos al desarrollo de estas operaciones, ya que estos se encuentran fuera del objetivo de trabajo.

Para el desarrollo del trabajo sólo se limitará a los aspectos que refieren a este tipo de operaciones en conflictos convencionales como dicta el plexo normativo vigente para el empleo de las Fuerzas Armadas.

Desde el aspecto teórico, la presente investigación busca plasmar cómo se vinculan las operaciones de guerra electrónica y las de ciberdefensa en su ejecución dentro del nivel operacional, establecer las bases para que ambos tipo de operaciones sean planificadas y conducidas por un solo elemento de comando en el nivel operacional obteniendo las bondades de converger ambos tipos de operaciones.

Debido a la falta de doctrina local vigente en las FFAA argentinas, el tema puede ser considerado de interés. Es una contribución positiva que puede ser tenida en cuenta y servir como base al momento de contemplar la conformación de un comando de teatro de operaciones como también un elemento que posea las capacidades para planificar y/o desarrollar en forma simultánea este tipo de operaciones, pudiendo ser aplicado en el ámbito conjunto o específico de cada instrumento de la defensa nacional.

La presente investigación presenta como su objetivo general describir la vinculación e integración de las operaciones de Guerra Electrónica y Ciberdefensa en el marco conjunto del nivel operacional en países miembros de la OTAN y América del Sur para determinar los beneficios e implementación en el plano local.

Para arribar al objetivo general se hará por medio de objetivos específicos o particulares que permitan corroborar el mismo. En primer lugar se buscará analizar el plexo doctrinario público vigente de países integrantes de la OTAN para lograr la convergencia de ambos tipos de operaciones. En segunda instancia se tratará de describir/analizar en el ámbito conjunto nacional, en el nivel operacional, la estructura actual para el desarrollo de las acciones de Ciberdefensa y Guerra Electrónica.

Para el desarrollo de la presente investigación se ha trabajado con la hipótesis de que la integración entre las operaciones de Guerra Electrónica y las de Ciberdefensa bajo un único comando es aplicable a la estructura organizacional nacional para su desarrollo en el nivel

operacional dentro de un conflicto convencional para sincronizar su planeamiento y ejecución con la finalidad de un mejor aprovechamiento de los medios.

Esta investigación se basó en el empleo de un diseño descriptivo mediante el análisis de información proveniente de distintas fuentes abiertas de otros países y del ámbito nacional. Con el desarrollo de cada capítulo, que responde a objetivos particulares, y sus respectivas conclusiones parciales, darán lugar a conclusiones finales de carácter general que permitan responder al objetivo general planteado en la investigación.

En cuanto al diseño de la investigación, el método a emplear será de carácter explicativo, en el que se empleará como técnica de validación el análisis bibliográfico, documental y lógico para describir el problema y establecer la relación entre los distintos conceptos necesarios para dar respuesta a los interrogantes.

En lo que respecta al análisis doctrinario, para no vulnerar medidas de seguridad, se enfocará en aquella que es de libre acceso pudiendo, si es necesario, hacer mención de la existencia o desarrollo de proyectos vinculados a la temática en cuestión.

La estructura de esta investigación está conformada en dos capítulos, para ir de lo general a lo particular, primero analizando el estado actual de este tipo de operaciones en el nivel internacional y luego en lo que respecta al ámbito local.

CAPÍTULO 1

CONVERGENCIA ENTRE OPERACIONES DE CIBERDEFENSA Y GUERRA ELECTRÓNICA EN PAÍSES DE LA OTAN

Conceptos generales

El presente capítulo tiene como objetivo particular analizar y desarrollar la convergencia entre las Operaciones de Ciberdefensa y Guerra Electrónica, basado en la información de acceso público disponible, en el marco de las FFAA de países que integran la OTAN que cuentan con vasta experiencia con años de aplicación en el nivel Táctico y Operacional. Estos países han sido foco de análisis por haber incorporado este tipo de operaciones dentro de la organización militar para su planeamiento y ejecución.

El enfoque que propone el análisis está orientado hacia dos aspectos que son fundamentales, en principio, como se clasifican este tipo de operaciones militare en el nivel conjunto operacional desde la perspectiva de su tipificación y ordenamiento, en los países expuestos como de interés, y en segundo orden, como está estructurado el sistema para concretarlas desde su planeamiento hasta su ejecución.

El espectro electromagnético y el ciberespacio como parte del entorno específico de la información son fundamentales para el desarrollo de operaciones militares, por lo que se deben abordar de similar manera a la par de los dominios tradicionales de la guerra. Estos conflictos modernos se ganaran mediante el empleo de todos los dominios.

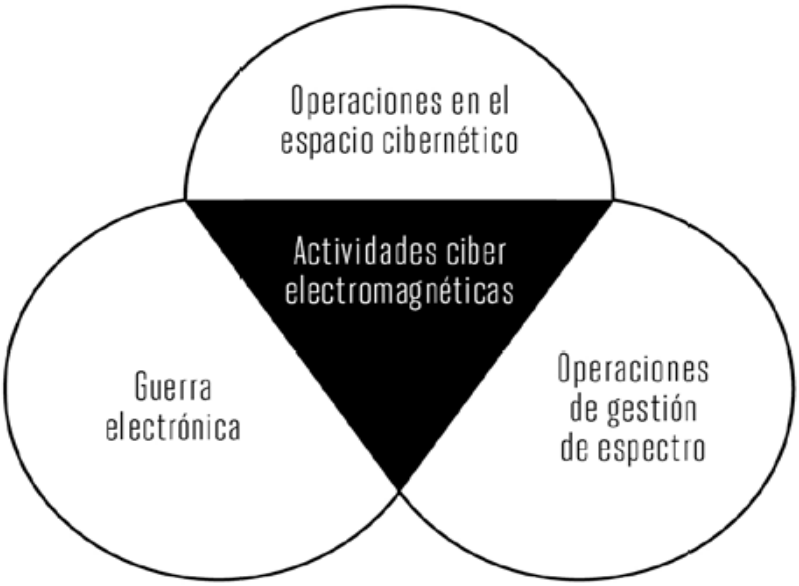
Como se abordó en la introducción del presente trabajo, la necesidad de coordinar las operaciones militares que se llevan a cabo en el ciberespacio y en el espectro electromagnético dieron lugar al concepto de actividades cibernéticas y electromagnéticas (CEMA, pos sus siglas en inglés). En la actualidad en los países miembro de la OTAN han reconocido la importancia de las actividades cibernéticas y electromagnéticas. Coinciden en que existe una vinculación y complementación entre ambos tipos de Operaciones, principalmente por la cercanía o superposición de los ambientes en donde desarrollan sus actividades.

Actualmente solo en la doctrina de Estados Unidos (EEUU) y el Reino Unido de Gran Bretaña (RUGB) se ha desarrollado el concepto de CEMA, mientras que si nos referimos a doctrina combinada o específica de los demás miembros de esta organización, la estandarización de este término se encuentra bastante rezagado o inexistente actualmente.

Pero la descripción de estas actividades, como se verá más adelante, será desde la óptica de las FFAA británicas ya que es cronológicamente más reciente y amigable para su entendimiento.

Figura 1

Convergencia de las Operaciones ciber, guerra electrónica y de gestión del espacio.



Nota. Detalle de la convergencia de las Operaciones. Fuente: De Vergara y Trama (2017). Operaciones Militares Cibernéticas (p. 228)

Según De Vergara y Trama (2017) se refieren a las CEMA como la sincronización y coordinación de actividades, de variada actitud, por medio del ciberespacio y el espectro electromagnético. Esto permite obtener una simultaneidad de efectos o combinación de los mismos dentro de ambos dominios. El contar con esta capacidad permite afectar los distintos subsistemas que componen la estructura del enemigo y afectar su funcionamiento cohesionado.

La existencia del ciberespacio depende de que haya un componente electrónico y electromagnético; este último brinda una existencia física al espacio cibernético en donde su relación nace a partir de cómo la información digital se transporta a través del espacio (De Vergara y Trama, 2017).

Para continuar con el desarrollo del presente capítulo, se describe cómo se estructura en cada caso particular y de qué forma integran ambos tipos de operaciones.

Convergencia de ambas operaciones en las FFAA de la República Federal de Alemania

En primer orden se abordará a las Fuerzas Armadas de la República Federal de Alemania. Los elementos de defensa no cuentan con término específico para referirse a la integración de este tipo de operaciones, sin embargo dentro de su estructura organizacional como se podrá observar ya se encuentran integradas bajo un único elemento de comando y dentro de una organización particular.

En el mes de abril de 2016 la ministra de defensa en ese momento, Úrsula Von Der Leyen, pone en marcha un proceso de reestructuración de las FFAA de Alemania. Esto llevó a la creación de una nueva rama militar, el Comando Cibernético y del espacio de la Información (Kdo CIR) que entró en servicio en abril de 2017, es importante destacar que este nuevo componente forma parte de un grupo de elementos, llamado Organizationsbereiche, de naturaleza conjunta que apoya a las FFAA en simultáneo. Su magnitud, en cuanto a efectivos, es similar al resto de las fuerzas.

Para poder tener una idea más clara de la organización de las fuerzas militares alemanas, se puede mencionar que se encuentran compuestas por seis fuerzas. Las tradicionales, ejército/armada/fuerza aérea, y las de carácter conjunto que apoyan a las primeras; se encuentran compuestas por el mencionado comando junto a los servicios de sanidad y logística.

Éste elemento tiene la responsabilidad de asegurar el mando y control de las fuerzas armadas en la dimensión ciber y espacio de la información, simultáneamente garantizar el funcionamiento y protección del sistema de información tanto en territorio nacional como en el exterior.

Su estructura está compuesta por tres elementos, un Comando de Inteligencia Estratégica, un Comando Técnico de la Información y un Centro de Geo información como se detallan en la Figura 2.

Figura 2

Estructura del Kdo CIR

Nota. Gráfico de la estructura del Kdo CIR de las FFAA alemanas. Fuente: Cañete (2020). El Comando de Ciberdefensa Alemán, un claro ejemplo de integración. Revista Visión Conjunta (p. 16).

Para el caso particular de análisis de este trabajo de investigación se centrará en el Comando de Inteligencia Estratégica que se especializa en brindar apoyo de inteligencia, guerra electrónica, operaciones psicológicas y ciberoperaciones a las FFAA. En la organización descripta previamente y pese a la falta de terminología doctrinal específica que enmarque ambos tipos de operaciones, es que éste comando conjunto integra distintas capacidades, entre ellas las de interés para esta investigación, bajo una conducción y ejecución centralizada a través de la interoperabilidad de su personal y medios que se encuentran en capacidad de proporcionar a los componentes tradicionales de las FFAA el apoyo necesario.

Del Comando de Inteligencia Estratégica dependen los centros de ciberoperaciones, centro de comunicación operativa, centro de guerra electrónica, centro de imagen de inteligencia, centro de investigación técnica de inteligencia, batallones de guerra electrónica (cuatro) y la escuela de inteligencia.

Convergencia de ambas operaciones en las FFAA de España

Miembro de la OTAN y hace unos años ha integrado ambos tipos de operaciones en el nivel conjunto, el Reino de España en el año 2020 mediante un Real Decreto (521/2020) establece la organización de sus FFAA para permitir que su adaptación a un entorno que evoluciona permanentemente; a través de este otorga al Ministro de Defensa y los Jefes de Estado Mayor las facultades para que puedan, en el momento que crean necesario, adecuar sus la estructura de sus organizaciones de un forma rápida y ágil (Fernández, p.58837).

Dentro de los puntos que se detallan en dicho decreto se establece cómo debe estar organizado el Estado Mayor de la Defensa (EMAD) y sus normas fijadas en la Orden Ministerial 26/2020. En su artículo 1° establece la siguiente estructura del EMAD: Cuartel General del EM, Mando de Operaciones, Centro de Inteligencia de las FFAA, Mando Conjunto del Ciberespacio y Centro Superior de Estudios de la Defensa Nacional.

A su vez establece los ámbitos en que debe estar en capacidad de operar las FFAA, el físico comprendido por el ámbito terrestre, marítimo y aeroespacial, y en los espacios cognitivos y virtual. De interés para este trabajo, en al ámbito ciberespacial debe asegurar la libertad de acción de las fuerzas; para esto se creó el Mando Conjunto de Ciberespacio (MCCE) sobre la base y reemplazando al Mando Conjunto de Ciberdefensa y la Jefatura de Integración de Sistemas de Información y telecomunicaciones (BOE, 2020).

De acuerdo al BOE N°204 “Este nuevo organismo es el responsable de llevar adelante el planeamiento, coordinar, controlar y ejecutar acciones tendientes a asegurar la libertad de acción de las FFAA en el ciberespacio” (p. 58844). Es el encargado de todos aquellos aspectos relacionados con la ejecución de operaciones militares en el ciberespacio.

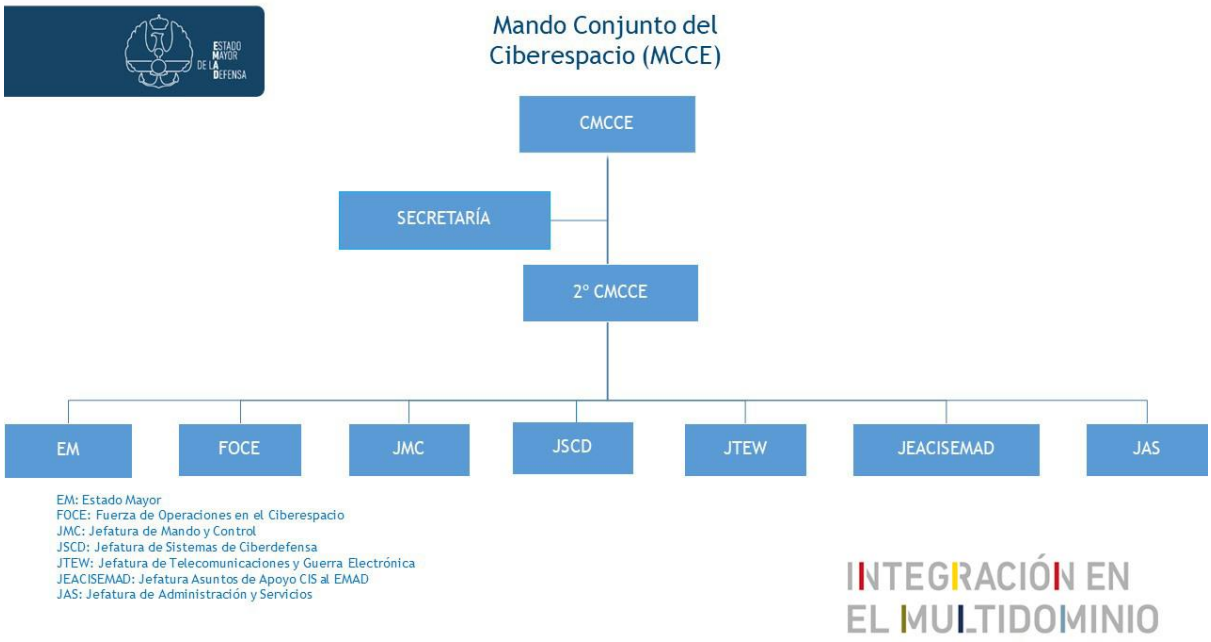
De acuerdo a Boletín Oficial del Estado N°204, del 28 de julio del 2020, el MCCE

> "Asegurar la autoridad de JEMAD sobre la infraestructura integral de información para las defensa (I3D) en el ámbito operativo. Es responsable, en colaboración con el EMACON, de la definición de requisitos operativos, seguimiento de la obtención y el sostenimiento de los medio de ciberdefensa, sistemas de información y telecomunicaciones (CIS) conjuntos de mando y control, de guerra electrónica y navegación, identificación y sistema de observación de la tierra, velando por la interoperabilidad de estos con los específicos de los Ejércitos (tierra y aire) y de la Armada. Asimismo, prestar apoyo CIS a la estructura de la EMAD" (p. 58844).

Esta nueva y moderna unidad de las FFAA españolas depende operativamente del JEMAD y su estructura, del MCCE, se puede ver detallada en las Figura 3.

Figura 3

Estructura del MCCE.



Nota. Gráfico de la estructura organizacional de MCCE del EMAD. Fuente: Estado Mayor de la Defensa (EMAD), unidades dependientes del EMAD. https://emad.defensa.gob.es/unidades/mcce/

Se puede observar en el gráfico de la Figura 3, dentro de la estructura del MCCE se encuentran la Jefatura de Sistemas de Ciberdefensa y la de Telecomunicaciones y Guerra Electrónica, de manera de actuar en forma coordinada bajo un mismo elemento de comando. En el mismo nivel dentro de la organización y dependiente del comandante de éste mando conjunto se encuentra la Fuerza de Operaciones en el Ciberespacio (FOCE). Ésta fuerza tiene

la responsabilidad de ejecutar las operaciones militares para asegurar la libertad de acción de las FFAA españolas en el ciberespacio. A su vez es responsable de coordinar entre las fuerzas y el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones las acciones que sean necesarias. Cuando se realicen acciones en el espectro electromagnético, deberá coordinar las actividades ciber que sean concurrentes a estas (BOE, 2020).

De lo descripto en los párrafos anteriores del análisis de las FFAA españolas, analizando la información de público acceso que se encuentra disponible, se puede inferir que no emplean un término en particular para la convergencia entre ambos tipos de operaciones, como se verá en otros casos, pero en la creación dentro de su organización conjunta de nuevos subsistemas se ha observado que llevaron adelante y concretaron este concepto materializado bajo la dependencia del MCCE.

Convergencia de ambas operaciones en las FFAA del Reino Unido de Gran Bretaña

De acuerdo a la concepción del Ministerio de Defensa Británico, las actividades que llevan adelante las fuerzas armadas deben incorporar e incrementar la interacción entre las actividades ciberelectromagnéticas y de información e integradas en medida que sea requerido con los efectos quinteticos (Gady y Stonell, 2020).

En el año 2017 el Ministerio de Defensa del Reino Unido a través de su Centro de Desarrollo, Conceptos y Doctrina (DCDC, siglas en inglés) edita la nota conceptual JCN 1/17 “Conceptos de la Futura Fuerza”. Este documento proporciona una orientación para el futuro desarrollo de las FFAA británicas, propone un cambio radical de enfoque hacia uno de mayor integración conjunta. Reúne en una sola publicación la combinación de los conceptos operativos por separado; busca guiar el desarrollo de esta futura fuerza en todos los niveles. En el contexto actual establece que el éxito ante las diversas y complejas amenazas que explotan el entorno de la información requiere de esta realizar las cosas de manera diferente (JCN 1/17, p. V).

El concepto de Fuerza Futura que desarrolla esta nota conceptual, proyecta una fuerza a treinta años (2035) y se basa en un propósito común y promoviendo una mentalidad conjunta. Estas bases se obtienen de lecciones operativas, del adiestramiento y experimentación de las FAA británicas y de sus socios de la OTAN.

En su tercera parte, “Características, desafíos y oportunidades en todos los dominios”, dentro de la sección 1 se refiere al dominio cibernético, en el que implementa y desarrolla como parte de la doctrina el empleo del término CEMA y su vínculo con el concepto de Fuerza Futura. Estipula que los avances tecnológicos y la digitalización del campo de combate han llevado a la convergencia de las actividades de ciberdefensa y de información, en donde la

coordinación en el ámbito conjunto mediante el concepto CEMA conducirá al éxito de las operaciones. La libertad con la que se cuente para emplear el ciberespacio y/o el espectro electromagnético, simultáneamente degradar o restringir el empleo del mismo al enemigo generará una ventaja significativa. Los equipos CEMA que realicen estas actividades necesitaran ser multidisciplinarios, contar con una adecuada preparación, no solamente técnica, en todos los niveles (JCN 1/17, p. 20).

El cambio constante en el ámbito cibernético, refiriéndonos a hardware, software o la misma configuración de las redes, llevan a que los especialistas en actividades ciberelectromagnéticas deben perfeccionarse en comprender y conocer la situación en tiempo real lo que permitirá una gestión con dinamismo del espectro mejorando la resiliencia de las fuerzas conjuntas. Es un desafío dentro de las fuerzas crear conciencia situacional con respecto a estas actividades dada la evidente dificultad de atribuir la autoría de las mismas a un actor específico (JCN 1/17, 2017).

Apunta a un comando y control centralizado de estas actividades pero su ejecución descentralizada. Asegurando, por parte de los equipos CEMA, la integración de estas actividades con el resto que llevan a cabo las fuerzas conjuntas. Para lograr esto se necesitan especialistas con experiencia en ciberdefensa, guerra electrónica, comunicaciones y gestión del espectro electromagnético más analistas de inteligencia.

Continuando con el análisis de documentos doctrinales del actor en cuestión, y en concordancia con el JCN 1/17, en el año 2018 el DCDC publica la Nota de Doctrina Conjunta (JDN) 1/18 “Actividades cibernética y electromagnéticas”. En contraste con el JCN 1 /17, en donde establece la necesidad de generar la capacidad de CEMA, ésta JDN detalla cómo se implementa este concepto.

El objetivo de este documento conjunto es delinear una base para las actividades de CEMA dentro de los organismos que componen la defensa, junto con otros órganos que conforman el gobierno. Les proveerá una descripción de trabajo para el entorno CEMA permitiendo que individualmente las distintas ramas desarrollen su propio concepto sobre estas actividades pero alineado en la intención del comando de las fuerzas conjuntas y la sede de comunicaciones del gobierno (GCHQ). También aborda la temática cómo las actividades CEMA pueden apoyar operaciones ofensivas, defensivas y permitir a los comandantes y sus estados mayores tomar decisiones más detalladas y simultáneamente generar efectos dentro del espectro.

Estas actividades son interdependientes con el espectro electromagnético, en el que ambos actores se disputan el control mediante el uso de actividades CEMA para obtener una

ventaja en el desarrollo de las operaciones militares. Esta ventaja será dada en medida de la libertad con las que se pueda usar el espectro y el ciberespacio, con respecto al enemigo (JDN 1/18, 2018).

La visión que refleja sobre las actividades de CEMA es que sincronizan y coordinan las actividades cibernéticas y electromagnéticas para brindar libertad en la configuración de movimientos, la obtención de efectos pero simultáneamente denegar o degradar el uso de ambos dominios al adversario. La necesidad de este tipo de actividades se ha incrementado en estos años por la necesidad de compartir información en el campo de combate, el creciente volumen de información que se necesita transmitir así como la disponibilidad de medios a ser explotados para su transmisión.

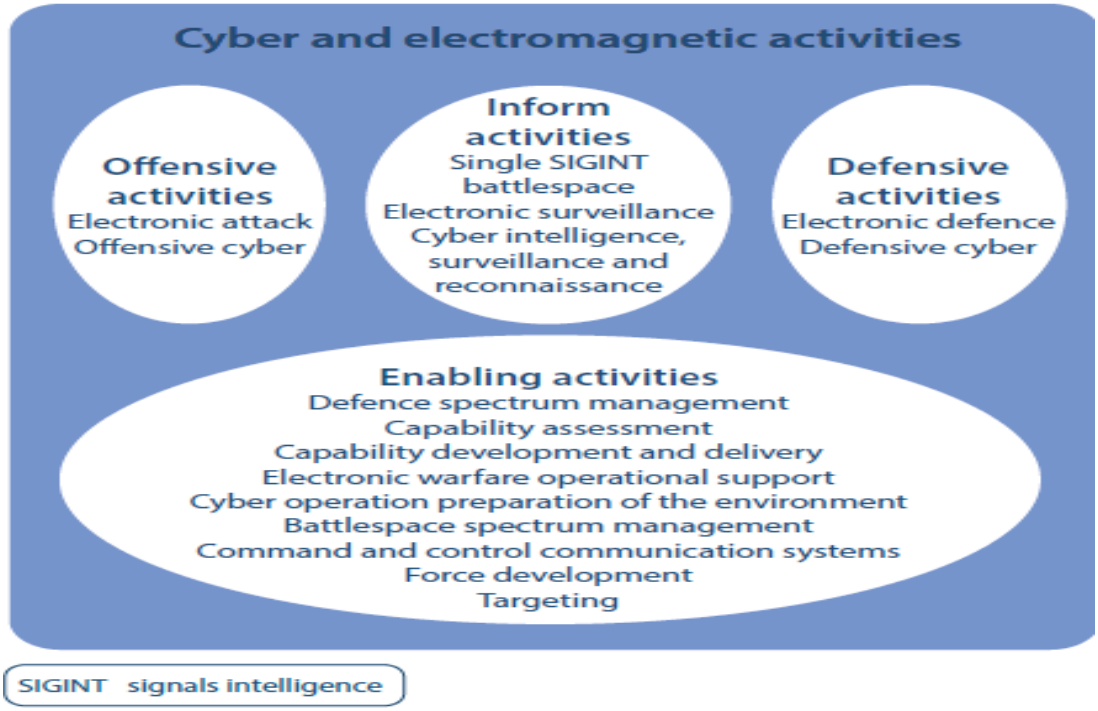
La tecnología continuará siendo un elemento relevante en el desarrollo de los conflictos actuales y futuros, que genera un cambio en los asuntos militares. Requerirá mantener una ventaja tecnológica con respecto al adversario. Esta tecnología ha acrecentado las actividades no cinéticas. La sincronización de operaciones cibernéticas junto a las de guerra electrónica permitirá un enfoque completo del espectro, que actualmente las fuerzas del Reino Unido no lo tienen al no estar preparadas para operar de esta forma en ambos entornos (JDN 1/18, p. 6).

Este documento menciona que dentro del Plan de Comando para el Comando de las Fuerza Conjuntas 2016/17 se busca establecer un Grupo Conjunto de actividades CEMA que coordine, planee y ejecute la defensa CEMA para optimizar las capacidades de ciberdefensa y de guerra electrónica mediante un programa de ocho años que se desarrolle en tres fases (JDN 1/18, p. 13).

El JDN 1/18 define a las actividades de CEMA “como la sincronización y coordinación de actividades ofensivas, defensivas, de información y habilitadoras, estas últimas contribuyen con las otras actividades, a través del ciberespacio y el espectro electromagnético” (p. 13). Menciona las actividades que realiza, en donde se llevan a cabo y claramente existe la posibilidad de combinarlas. Esta definición se encuentra respaldada por el Grupo de integración de capacidades CEMA. Es necesario resaltar, como se expresa en este documento, que al momento de su redacción no existen definiciones aprobadas para actividades cibernéticas o electromagnéticas.

Figura 4

Actividades CMA en el Reino Unido.



Nota. Gráfico de la clasificación de las Actividades CEMA del MOD del Reino Unido de Gran Bretaña. Fuente: Centro de desarrollo de Conceptos y Doctrina (2018). Actividades Cyber y Electromagnética. JFN 1/18 (p. 14).

Dentro de su documento aclara que también este tipo de actividades pueden contribuir con las operaciones psicológicas que son parte de las operaciones de información, abre la posibilidad de combinarlas de forma de lograr efectos contribuyentes.

Es importante destacar que los principios y conceptos abordados por este documento no se encuentran totalmente estandarizados en todas las fuerzas, lo que ha tratado de establecer inicialmente una base.

Prevé la creación de Unidades específicas de CEMA dentro de las organizaciones y de la cadena de comando mediante un Grupo de coordinación y sincronización de estas actividades; compuesta por equipos de planificación y evaluación del efecto junto con una célula de coordinación.

En este mismo año el DCDC realizó la publicación de Doctrina Conjunta 0-01, en la que dentro de los dominios operativos que componen el ambiente operacional se encuentran el marítimo, el terrestre, el aéreo, el espacial y el ciberelectromagnético. Toma como un quinto dominio operativo en los conflictos al Ciberelectromagnético.

Relacionado con lo desarrollado por el documento analizado, en el año 2020 el MOD británico a través del DCDC publica la nota JCN 1/20 “Integración Multidominio”. En ella ratifica que los dominios intangibles como el espectro electromagnético, el ciberespacio o el

espacio son parte del campo de combate. En especial los dos primeros son transversales a los demás. También hace hincapié en su importancia por cómo estos a su vez integran a los dominios mediante los enlaces y sistemas de redes (JCN 1/20, p.18).

Dentro de los documentos consultados de acceso público, se pudo analizar al componente terrestre y puntualmente como en concordancia con los documentos mencionados anteriormente, lleva adelante desde hace unos años, dentro de su organización un proceso de reestructuración a fin con ellos. En marzo del año 2017, el área de publicación de doctrina del Ejército en su AC 71940 hace mención a la integración entre el ciberespacio y el espectro electromagnético en afirmar que deben considerarse juntos para el desarrollo de operaciones militares.

En él emplea el término CEMA estableciendo que se refiere a la integración de las actividades en ambos dominios. Describe las operaciones en cada ámbito en concordancia con las publicaciones conjuntas del MOD, pero aclara que en los mayores niveles se llevarán a cabo el total de las operaciones mientras que en nivel más tácticos solo algunas específicas; pero en todos los casos las fuerzas terrestres deben considerar los efectos a lograr en ambos dominios dentro de su entorno operativo. Las actividades Ciberelectromagnéticas que realiza el Reino Unido se llevan adelante en el mismo marco legal que las de los dominios físicos, pero reconoce la complejidad en la determinación del origen de las agresiones.

En el mes de marzo de 2021 el Ejército Británico publicó “The future Soldier Guide”, en él desarrolla un plan de transformación bastante profundo y ambicioso que se haya proyectado en los últimos años; buscando conformar un ejército moderno que pueda afrontar las exigencias futuras. Como principal información de interés relacionada con el tema de investigación, es el detalle de la futura estructura y roles de cada unidad en donde hace mención a la creación de un Grupo de Efectos CEMA. Este elemento estará compuesto por dos regimientos de inteligencia de señales y guerra electrónica, 14to y 21er Regimientos de Señales; y el Regimiento Cyber, el 13er Regimiento de Señales. Operarán bajo el mando centralizado del Field Army Troops. Este proyecto realizó la fusión más profunda de las capacidades cibernéticas y electrónicas del ejército.

En la explicación del concepto de cambio de batalla cercana a profunda, establece que el ejército incrementará sus capacidades para producir efectos en la profundidad del enemigo, en los ámbitos físicos y virtuales. Dentro de estas capacidades se incluyen las actividades de ciberelectromagnéticas.

Luego de lo descripto y analizado en los párrafos precedentes; podemos entender que producto del cambio doctrinario y organizacional que han iniciado las FFAA británicas con

vistas a las exigencias de los conflictos futuros es que han incorporado la integración entre las operaciones de ciberdefensa y de guerra electrónica. Se encuentran en un momento de transición en donde deben ir incorporando este concepto y traducirlo en obras concretas como es la formación del personal especialista en ellas y la creación de unidades que lleven a cabo todos los procesos para concretar su uso en el campo de combate. Como se ha descripto uno de los primero es dar este cambio, comenzando por la reestructuración de su organización ha sido el ejército Británico.

Convergencia de ambas operaciones en las FAA de los Estados Unidos de América

Dentro de la extensa doctrina conjunta en vigencia de las FFAA de los Estados Unidos de América del Norte, se encuentra el reglamento de Operaciones Conjuntas–Joint Operations (JP 3-0) actualizado en el año 2018, es la doctrina fundamental que guía a las operaciones de esta naturaleza.

Sostiene que las operaciones militares en el nivel conjunto generalmente pueden definirse por su enfoque; en otros casos su denominación cubre una variedad de misiones, tareas y actividades. Desarrolla las operaciones militares a nivel conjunto aclarando que éstas se pueden clasificar en general por su enfoque y a su vez la clasificación puede basarse en las misiones, tareas o actividades; pero siempre bajo cobertura y un comando conjunto.

Dentro de la lista de clasificación de las operaciones en dicho documento y analizando cada una en particular, se puede establecer que no existe una palabra en particular para referirse a la integración entre las operaciones de ciberdefensa y guerra electrónica, o que las contemple como una operación en sí misma. Sin embargo, más allá de que cada operación puede ser llevada a cabo de forma independiente, pueden y deben también ser integradas, sincronizadas y coordinadas en las operaciones conjuntas.

Sin embargo, relacionado con el análisis del reglamento anterior y en el ámbito de la doctrina militar conjunta, el JP 3-85 “Operaciones Conjuntas en el Espectro Electromagnético” publicado en el año 2020 describe inicialmente a las operaciones que se ejecutan en este dominio particular.

Asegura que las acciones de Operaciones Conjuntas en este ambiente para explotar, atacar, proteger y gestionar el entorno operativo del espectro electromagnético (EMOE) dependen del personal y de los sistemas de las áreas de guerra electrónica, gestión del espectro electromagnético, inteligencia, el espacio y ciberespacio.

Exige que en estas áreas se planifique y ejecute de manera coordinada; la finalidad de estas operaciones es orientar y priorizar los procesos que integren, sincronicen y eliminen

conflictos que puedan surgir de las fuerzas conjuntas operando en el espectro unificando esfuerzos.

A su vez hace referencia a que la mayoría de los Sistemas militares que operan dentro del campo de combate poseen componentes que dependen del empleo del ciberespacio y el espectro electromagnético. Esto requiere que exista una integración estrecha de las capacidades de ciberdefensa y de las operaciones conjuntas en el espectro para asegurar prioridades, la sincronización de las mismas y eliminación de posibles superposiciones.

En concordancia con lo planteado anteriormente, este documento establece que cada componente tiene su propio enfoque particular para organizarse, en el caso del Ejército el comandante y su estado mayor conducen actividades ciber electromagnéticas (CEMA) para planificar, sincronizar e integrar las operaciones que se ejecutan en el ciberespacio y el espectro electromagnético para unificar esfuerzos y proyectar poder en y a través de ambos dominio. La capacidad de ejecutar este tipo de operaciones permite al ejército asegurar y proteger sus redes y equipos.

En el reglamento conjunto JP 3-12 “Cyberspace Operations” en donde aborda el tema de la integración de ataques en el ciberespacio aclara que las capacidades de ataque en el ciberespacio incrementan su efectividad si se integra con otros tipos de ataques. Apela a un ejemplo de integración de ataque dentro del ciberespacio, “al querer afectar el sistema de defensa aérea del enemigo empleando una acción ofensiva de ciberdefensa pero por medio del espectro electromagnético, introduciendo mensajes en sus comunicaciones, afectando los sistemas de navegación terrestres (GPS) como así los de comando y control “(JP 3-12, p. IV-19).

También hace referencia a la importancia de administrar el espectro electromagnético del campo de combate para la planificación de las operaciones de ciberdefensa (JP 3-12, 2018). Dentro de las funciones conjuntas y las operaciones en el ciberespacio, afirma que las para poder desarrollar las operaciones en el ciberespacio no solo requiere de la protección de los equipos con sus componentes (antenas, cables, enrutadores, etc) que la llevan adelante sino del espectro electromagnético en donde se establecen los enlaces inalámbricos satelitales, celulares) que transportan los datos/información que es vital en las operaciones militares.

Por su parte, el Ejército de los Estados Unidos, incorporó el empleo del término CEMA en el año 2011, pero recién en el 2014 lo incluye dentro de su doctrina específica en el FM 2-38. Pero en 2017 reemplaza ese reglamento por el FM 3-12 “Cyberspace and Electromagnetic warfare Operations”, el cual ha sido actualizado en 2021.

Este documento define las operaciones de CEMA, da una descripción general de ellas y establece cómo debe llevarse adelante el planeamiento, la integración y sincronización de las operaciones en el ciberespacio y el espectro electromagnético.

Detalla que ambos dominios son fundamentales para lograr el éxito en las operaciones dentro del entorno operacional. El mando y control, la obtención y transmisión de información dependen del empleo de la tecnología que emplea el ciberespacio y el espectro.

Para ello los comandantes deberán estar en capacidad de aprovechar las capacidades que brindan el empleo de las operaciones que se desarrollan en ambos dominios, lo que requerirá el empleo de las CEMA. En su definición indica que "son un proceso de planificación, integración y sincronización de operaciones de ciberdefensa y de guerra electrónica que apoyan en forma unificada a las operaciones terrestres. Integrando y sincronizando estas operaciones se obtiene una ventaja en múltiples dominios" (FM 3-12, 2021, p. 1-1).

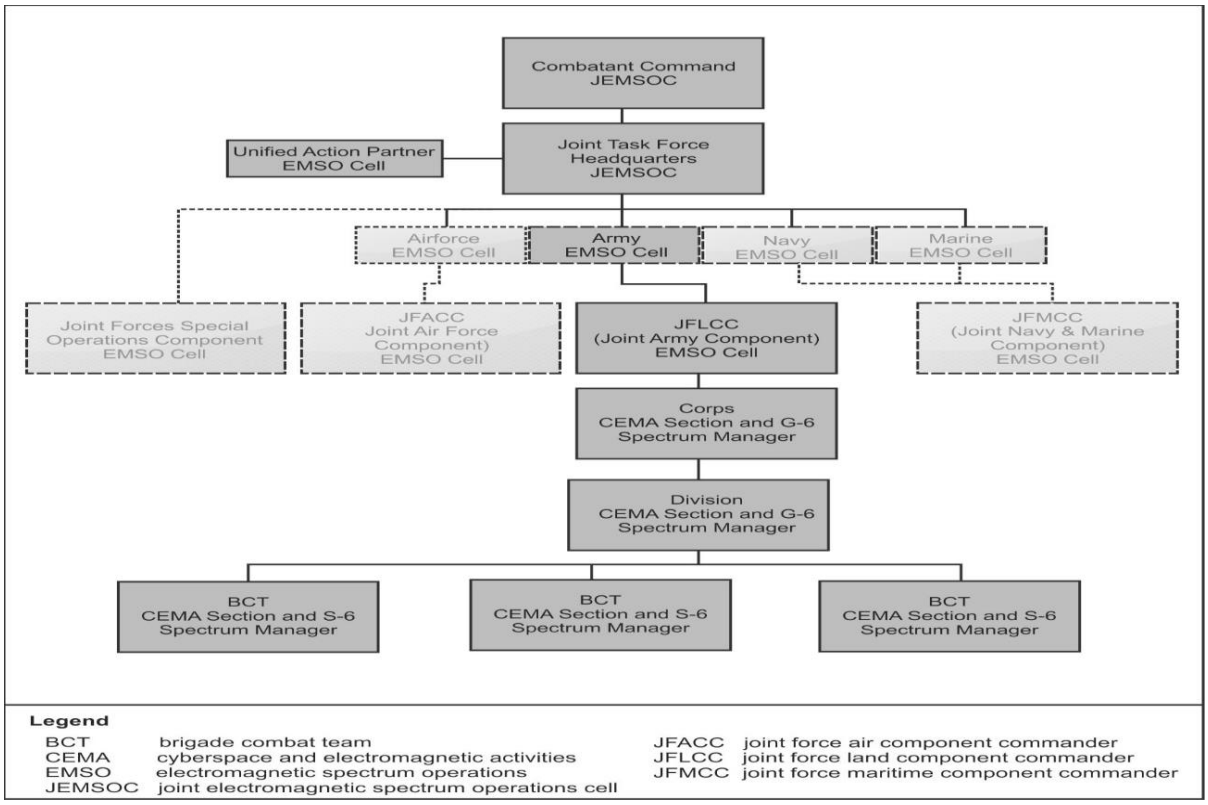
Dentro de la estructura organizacional del ejército se encuentra el Comando Cibernético del Ejército de los Estados Unidos (ARCYBER), es el comando operacional para operaciones en el ciberespacio. Es el encargado de dirigir y conducir en forma integrada las operaciones de guerra electrónica, de información y en el ciberespacio asegurando la propia libertad de acción y negarle al enemigo su empleo en el entorno del ciberespacio y de información que les otorgue a los comandantes una ventaja en ellos durante la campaña.

Dentro de las unidades asignadas al ARCYBER se encuentra el 915to Batallón de Guerra Cibernética, este elemento fue creado en 2018, se encuentra compuesto por "Expeditionary CEMA team(s)" (ECT, por sus siglas en inglés). Estos equipos se conforman por fuerzas de ciberdefensa, operadores de guerra electrónica, oficiales de operaciones de inteligencia, una celda de targeting y personal de inteligencia. Estos elementos apoyan a los comandos subordinados mediante la ejecución de operaciones de ciberdefensa, de inteligencia y de guerra electrónica.

A su vez en un nivel menor de la conducción para apoyar a los comandos subordinados (cuerpos, divisiones, brigada) posee Secciones CEMA asignadas al G3 o S3 según corresponda.

Figura 5

Estructura de las Operaciones CEMA



Nota. Gráfico de la estructura Nacional de las Operaciones en el Espectro Electromagnético. Fuente: Sede del Departamento del Ejército (2021). Operaciones en el Ciberespacio y de Guerra Electrónica. FM 3-12 (p. D9).

Como podemos observar, de lo descripto en los párrafos precedentes, se desprende que dentro del marco la doctrina conjunta, JP 3-12 y el JP 3-85, aceptan el término particular que emplea el Ejército de los Estados Unidos en el FM 3-12 para referirse a la integración entre ambas operaciones y a su vez tienen presente la relevancia de contar con la capacidad de ejecutar operaciones en ambos dominios e integrarlas para obtener una ventaja.

CAPÍTULO II

SITUACIÓN NACIONAL ACTUAL PARA EL DESARROLLO DE OPERACIONES DE CIBERDEFENSA Y GUERRA ELECTRÓNICA

Conceptos generales

Luego de haber descripto y analizado en el capítulo anterior la convergencia de ambos tipos de operaciones desde distintos enfoques en el ámbito internacional se pasará al entorno nacional. Para ello, el desarrollo del presente capítulo tiene por objetivo realizar un análisis descriptivo de la actualidad organizacional de las FFAA Argentinas en el nivel conjunto operacional y específico para llevar adelante operaciones de ciberdefensa y guerra electrónica.

En primera instancia se expresa como es la estructura organizacional actual en el marco conjunto de cada elemento encargado particularmente de llevar adelante todo los procesos relacionados con cada tipo de operación y finalmente realizar una vinculación con los niveles específicos de cada una de las fuerzas.

La relevancia de efectuar este análisis en ambos niveles es que permita obtener elementos de juicio permitiendo arribar a las conclusiones finales, para poder contemplar la factibilidad de concretar la convergencia de ambos tipos de operaciones comenzando por pergeñar un posible diseño desde lo doctrinario y luego llevarlo a su concreción sobre un elemento particular que permita llevar adelante esto.

Estructura Nacional Actual

Es importante resaltar que en el presente no existe en el ámbito conjunto ningún organismo que unifique o integre ambos tipos de operaciones o que tenga la responsabilidad de llevar adelante procesos estandarizados que permitan concretarlas en forma convergente o integrada, tanto en la paz como cuando se configure un conflicto. La diferencia entre ambos estadios radica en que en caso de un conflicto, luego de decretarse la conformación de un teatro de Operaciones y la designación de su comandante (Cte) se configura un Estado Mayor particular para él, que será el órgano de asesoramiento y asistencia durante la campaña.

De acuerdo al reglamento conjunto PC 10-01 “Estado Mayor Conjunto del Comando de un Teatro de Operaciones” (2018) establece una organización tipo de un comando de este nivel, dentro de la misma se conforman dos jefaturas (C) separadas que tiene la responsabilidad de llevar adelante todos aquellos aspectos relacionados a ambos tipos de operaciones. Estos integrantes se denominan Jefatura CVI (Comunicaciones, Informática y Guerra Electrónica) y la Jefatura CIX (Ciberdefensa), si bien ambas jefaturas dependen de un mismo Jefe de Estado Mayor, requieren para la planificación, sincronización e integración una comunicación fluida y detallada en lo que respecta a realizar simultáneamente las operaciones correspondientes.

Estas jefaturas deben integrar los planes, tareas y operaciones de los elementos que se encontrarán dentro del teatro de operaciones

Es necesario resaltar que estos órganos no poseen elementos orgánicos de combate que le dependan bajo su comando para desarrollar operaciones, sino que son solo de planeamiento. Eventualmente se puede conformar, de manera transitoria o temporal, un elemento que dependa directamente del Cte TO para su empleo, pero este es el que decide cómo y cuándo emplearlo no las jefaturas mencionadas. Un ejemplo de ello, es la Compañía de Comunicaciones Conjuntas.

Actualmente los elementos que llevan adelante ambos tipos de operaciones dependen y forman parte de los elementos que le asigna cada fuerza a la organización de cada componente del TO. Estos forman parte de las herramientas con las que cuentan los Cte(s) de componente para cumplir con las misiones particulares que le son ordenadas/asignadas por el nivel operacional.

A diferencia del nivel operacional en el nivel táctico, dentro de los órganos de planeamiento, en el Ejército Argentino, encargado de conformar el componente terrestre del TO, dentro de la organización de un estado mayor en todos los niveles de la conducción es responsabilidad del Oficial de Comunicaciones, Informática y Guerra Electrónica (OCIGE) todo lo concerniente a el planeamiento para el desarrollo de actividades de guerra electrónica o ciberdefensa, junto con lo correspondiente a comunicaciones e informática, permitiendo que la convergencia entre ambos tipos de actividades se concreten desde el inicio.

Relacionado con el párrafo anterior y con el tema de investigación, sobre la convergencia entre ambos tipos de operaciones y el proceso para llevarlas a cabo; recientemente, a partir del año 2021, se encuentra en discusión y análisis la conveniencia de cambiar la denominación del Batallón de Operaciones Electrónicas a Batallón de Guerra Electrónica y Ciberdefensa, esto conlleva realizar un cambio dentro de su estructura. Este elemento es asignado al componente terrestre, depende directamente del Cte de componente, decidiendo cuándo emplearlo y con qué finalidad.

Este proceso de cambio no es solo en su estructura, sino que como corresponde, es acompañado por la doctrina que actualmente se encuentra en proceso de desarrollo, análisis y evaluación para su futura implementación. Éste proyecto de nuevo reglamento es denominado “Conducción del Batallón de Guerra Electrónica y Ciberdefensa”, en él fijan los conceptos doctrinarios sobre los dos campos, cómo debe realizarse el apoyo en cada operación en particular y en su conjunto, como se clasifican las actividades de ambos tipos de operaciones y fija conceptos doctrinarios sobre cómo conducir y organizar el elemento.

El Batallón tendrá la responsabilidad de entender en todo lo relacionado con la planificación y ejecución de ambas operaciones dentro del componente terrestre, mediante la instalación, operación y mantenimiento del Subsistema de ciberdefensa y guerra electrónica para asegurar el comando y control propio; y afectar el del enemigo, asegurando la propia conducción.

Al presente, dentro de su orgánica, se ha creado una fracción de ciberdefensa, de nivel subunidad. Este renovado elemento permite en el nivel táctico tener bajo un único comando todo el proceso desde la planificación hasta la ejecución de ambas capacidades integradas, permitiendo obtener por múltiples medios los efectos solicitados. Más allá de las capacidades propias en cuanto a la concreción de las operaciones, cuenta con las facilidades móviles necesarias para desplegarlas en el campo de combate en el lugar y momento que sea necesario.

En el presente año, 2022, continuando con el proceso de conversión y modernización de dicho elemento se le ha provisto de vehículos todo terreno equipados con equipos informáticos y software de última generación que componen la subunidad especializada en ciberdefensa, estos medios le permitirán mediante su despliegue extender el alcance de sus capacidades en el campo de combate.

Lo descripto en los párrafos precedentes hace referencia específica a una situación particular en donde se configuran todos los medios para el desarrollo de un conflicto armado en un lugar físico/geográfico específico denominado TO.

Fuera de una situación de conflicto descripta previamente, dentro de la doctrina en vigencia para la acción militar conjunta, el reglamento OC 30–00 (2020) aborda la estructura y organización del Estado Mayor Conjunto de las Fuerzas Armadas (EMCOFFAA) que asesora y asiste al Jefe del Estado Mayor Conjunto de las Fuerzas Armadas (JEMCO) en temas relacionados que son de incumbencia de sus respectivas direcciones.

Este documento, relacionado con el tema de interés, establece que dentro de dicha organización se encuentra establecida una Dirección General de Comunicaciones e Informática (DGCI) que entre sus responsabilidades entiende en los aspectos relacionados con la GE, dependiente del Subjefe del EMCO.

También dentro de dicha estructura se encuentra el Comando Conjunto de Ciberdefensa (CCCD), pero en un nivel operacional dependiente directamente del JEMCO; este comando entiende en todos los aspectos relacionados con el ciberespacio y las acciones que se ejecutan en él.

Éste CCCD fue creado en el año 2014, mediante una resolución del Ministerio de Defensa N°343 y a diferencia de la DGCI se encuentra al mismo nivel que el Comando

Operacional de las FFAA (COFFA). Su misión “es conducir las operaciones de Ciberdefensa a fin de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional, en cumplimento de la misión principal y de acuerdo a los lineamientos establecido en el planeamiento. Durante la paz, mantener una estructura funcional que le permita cumplir con las tareas de planeamiento y ejecución del corto plazo, además de las normales de mediano y largo plazo” (https://www.fuerzas-armadas.mil.ar/Comando-Conj-Ciberdefensa/mision.html)

A partir de su creación, el EMCO ha ido incrementando su asignación presupuestaria hacia esta nueva área que se tradujo en recursos para la consolidación del mismo; a través de la infraestructura edilicia y la adquisición de equipamiento de última generación.

Esto en concordancia con la Directiva de Política de Defensa Nacional 2021, en donde dentro de los factores relacionados al diseño de la fuerza que se establece del ciclo de planeamiento de la defensa nacional, fija el desarrollo de capacidades operacionales de ciberdefensa y capacidades para proteger la seguridad de las redes del Sistema de Defensa Nacional (DPDN 2021, p.25).

La estructura actual del CCCD está formada de la siguiente manera; posee un Cte Conj de Ciberdefensa, que le dependen el JEM, una secretaria y un departamento de planes y presupuestos; un Centro de Operaciones de Ciberdefensa (COC) y finalmente un Centro de Ingeniería de Ciberdefensa (CIC).

Hasta el presente año, este comando no cuenta con elementos móviles de campaña que le permita proyectar sus capacidades dentro del espacio físico en donde se conforme un TO.

En línea con él nivel operacional, cada una de las tres FFAA poseen una Dirección de Ciberdefensa, dentro del ámbito de la Dirección General de Comunicaciones e Informática de cada fuerza. Estas direcciones, por el momento, poseen solo una relación funcional y no de comando con el CCCD mediante el establecimiento de reuniones de enlace para compartir información y tratar aspectos comunes.

En lo que respecta a guerra electrónica tuvo su auge, mediante la incorporación de equipos móviles y sistemas de software de última generación, en el período comprendido entre las décadas de 1990 y 2000; pero principalmente fue en forma específica de acuerdo a las necesidades dentro de cada fuerza incrementando las capacidades individuales en el desarrollo de éste tipo de operaciones. Luego tuvo un período de desaceleración en la renovación y actualización del material, principalmente por el costo de los mismos. Esta situación se ha ido cambiando nuevamente gracias a la sanción del FONDEF, permitiendo de a poco ir actualizando nuevamente los sistemas.

En relación al contenido desarrollado en los párrafos anteriores y la hipotética situación en que se configuren las condiciones para el desarrollo de un conflicto, en el caso particular de los elementos mencionados previamente, para la convergencia de dichas operaciones específicas y poder ejecutar actividades ciberelectromagnéticas, exige previamente la sincronización y la coordinación interagencial así como una responsabilidad compartida.

De lo descripto en el presente capítulo se desprende que en la actualidad existe una estructura fija fuertemente consolidada relacionada a la ciberdefensa y la guerra electrónica. Comenzando por los elementos en el nivel operacional encargados de su planeamiento hasta los niveles inferiores que las concretan. Esto permite que para lograr la convergencia de estos tipos de operaciones se requiera analizar la factibilidad de unificar ambas bajo un mismo comando y cuál sería la mejor manera de llevarlo adelante.

Para finalizar el desarrollo del presente capítulo, es importante mencionar que en la actualidad, desde el mes de marzo de 2022, el EMCO ha comenzado un programa de revisión de publicaciones para la acción militar conjunta (AMC) en vigencia para su actualización. Dentro de este proceso, una de las comisiones se le ha encomendado dicha tarea sobre la doctrina referida a la “Ciberdefensa y Guerra Electrónica en la AMC”. Esta comisión tiene dentro de sus tareas definir si la doctrina de ambos tipos de operaciones deberá ser en publicaciones separadas o en solo una. Esto marca una tendencia o por lo menos que dentro de las FFAA ya se está pensado, por lo menos en una etapa inicial dentro de la doctrina, la integración de ambos tipos de operaciones. Una de las propuestas surgidas del análisis inicial es la de trasladar todo lo concerniente a guerra electrónica bajo la órbita de ciberdefensa, es decir que en el nivel operacional dependa orgánicamente del CCCD y a su vez dotarlo de equipos móviles que estén en capacidad de ejecutar ambas actividades, pudiendo ser desplegadas en por ejemplo para la protección de una infraestructura crítica como la estación de anclaje de los cables submarinos que provee el servicio de internet al país.

CONCLUSIONES FINALES

Los avances tecnológicos experimentados en las últimas décadas se han ido acrecentando en forma cada vez más acelerada; simultáneamente se fueron incorporando cada vez más al campo de batalla moderno produciendo un salto cualitativo en las capacidades militares. Esto ha repercutido en el modo de empleo de la fuerza y ha incentivado la incorporación a las FFAA de tecnologías que permitan obtener a través de ellas una superioridad o ventaja. En este sentido, la presente investigación tiene como base para su desarrollo el siguiente interrogante guía: ¿cómo la convergencia entre las operaciones de ciberdefensa y guerra electrónica bajo un único elemento de comando facilita su ejecución en el nivel operacional?

Considero que en base a lo desarrollado en la introducción y en ambos capítulos, es necesario aclarar como primera conclusión que la integración de ambos tipos de operaciones no quiere decir que sean lo mismo ya que se diferencian en algunos aspectos pero existe una relación estrecha entre ambas. Una de las diferencias que se puede destacar, es la naturaleza del ámbito en que se generan las agresiones, en el caso de la guerra electrónica es netamente militar y dentro del espectro electromagnético del campo de batalla; mientras que en el caso de las operaciones en el ciberespacio es un poco más difuso, pudiendo ser fuera de los límites del TO y de múltiple naturaleza lo que implicaría poder discernir si corresponde a ciberdefensa o ciberseguridad. Ambos dominios, en donde se ejecutan cada tipo de operación, fueron creados por el hombre pero cabe resaltar que una diferencia sustancial en el caso de las operaciones CEMA posibilita el empleo del espectro electromagnético para producir efectos cibernéticos. Por ejemplo, se puede provocar una disrupción en la capa 1 y de esta manera neutralizar el empleo del ciberespacio. La integración se da en que algunos sistemas de armas informatizados emplean el espectro electromagnético para la transmisión de información; por ejemplo los sistemas satelitales de comunicación o navegación. A raíz de esta vinculación estos sistemas pueden ser afectados, independientemente del efecto a lograr, por medio electrónico o informático como así en forma combinada entre ambas.

Para lograr los cambios que permitan la integración se plantean importantes desafíos en ambas áreas; conlleva desde la modificación de la doctrina actual, la estructura de la organización, la capacitación del personal, el material, instalaciones. Pero los activos más críticos para concretar estos cambios son el personal y la doctrina, ya que son los que requieren más tiempo para su concreción.

La materialización de un cambio en la doctrina que adopte el concepto CEMA u otro nombre que determinen las propias FFAA, provocará modificaciones en la estructura

organizacional que permitan concretar la integración en todos los niveles así como en los procesos de ambos tipos de operaciones. Estos cambios contribuirán a avanzar un paso más en el desarrollo de capacidades que permitan operar de manera exitosa en un entorno multidominio en sintonía con las tareas de modernización que lleva adelante el Estado Mayor Conjunto de acuerdo a lo expresado en la Directiva de Política de Defensa Nacional.

Atendiendo a lo detallado sobre la factibilidad en la convergencia de ambos tipos de operaciones desarrollado en el capítulo uno, tomando como referencia la experiencia en fuerzas extranjeras, y observando la actual organización nacional de ambos sistemas en el nivel operacional. Se puede concluir que en este nivel dentro de la conformación de un estado mayor de un teatro de operaciones, en lo concerniente al planeamiento, coordinación y sincronización de las operaciones de guerra electrónica junto con las de ciberdefensa, se verá favorecido colocando ambas bajo la esfera de un solo órgano de planeamiento. Esto permitirá al momento de llevar adelante estas actividades una visión más integral de aquellas capacidades que permitan lograr los efectos requeridos para afectar el comando y control del enemigo a través de formas diferentes, asegurando el propio. A la vez reducir los tiempos mismos del planeamiento, al eliminar la parte burocrática que lleva el coordinar entre órganos distintos. Estructuralmente, estas modificaciones no requieren grandes cambios a la actual organización de comando. Sino sólo la transferencia del personal idóneo en ambos campos en uno solo, contenidos dentro de un mismo campo de la conducción con conocimientos de ambos.

En relación al párrafo anterior, estos cambios deben motorizar o generar la creación de un elemento conjunto que reúna y ejecute, en el campo de batalla, ambos tipos de operaciones. Este deberá estar conformado por un elemento de comando que planifique las operaciones, estado mayor, y otro de ejecución. El personal integrante de ambos elementos deberá contar con la formación técnica profesional especializada en el desarrollo de cada tipo de operación y sus procesos para llevarlas adelante. Pero será una responsabilidad del elemento de comando la sincronización y convergencia de ambas en su ejecución.

En cuanto a las operaciones que surgen de la convergencia de las operaciones de guerra electrónica y ciberdefensa, de lo analizado e investigado en la doctrina extranjera, surge que los países que lo poseen más desarrollado han decidido emplear el término CEMA para referirse a ella.

En base a todos los aspectos expuestos anteriormente permiten confirmar que lo planteado en la hipótesis es parcialmente correcto. Por un lado que los países miembros de la OTAN analizados, contemplan y ya tienen en un grado avanzado incorporado dicho concepto de integración, con estructuras particulares encargadas de llevar adelante todos los aspectos

relacionados a ambas operaciones integradas. No existe uniformidad en el empleo de términos pero sí de conceptos.

Por otro lado es que en el ámbito nacional, si bien hasta el presente, no hay en el nivel operacional un elemento u órgano de planeamiento que agrupe o integre ambos tipos de operaciones, es por esto la parcialidad de la hipótesis, en el nivel conjunto y específico se ha comenzado a trabajar desde diferentes aspectos para evaluar la posibilidad de concretar la convergencia de ambas operaciones. Esto respaldado por el diseño de unas FFAA futuras que se encuentren en capacidad de operar en forma coordinada y sincronizada en los múltiples dominios que conforman el ambiente operacional.

Finalmente, al momento de llevar adelante e incorporar las actividades ciberelectromagnéticas, lo que en menor o mayor tiempo sucederá, contará con una base doctrinaria extranjera en la cual pueda apoyarse para su desarrollo, encontrando aportes y análisis sobre el tema desde el nivel operacional hasta el táctico.

BIBLIOGRAFÍA

Centro de Desarrollo de Conceptos y Doctrina (2016). Cyber Primer, segunda edición. Ministerio de Defensa del Reino Unido de Gran Bretaña.

Centro de Desarrollo de Conceptos y Doctrina (2017). JDN 1/17 Future Force Conept. Ministerio de Defensa del Reino Unido de Gran Bretaña.

Centro de Desarrollo de Conceptos y Doctrina (2018). JDN 1/18 Cyber and Electromagnetic Activities. Ministerio de Defensa del Reino Unido de Gran Bretaña.

Collantes, L. (2012). La Ciberguerra en los conflictos modernos. Chile, Santiago.

De Vergara, E y Trama, G. (2017). Operaciones Militares Cibernéticas – Planeamiento y Ejecución en el Nivel Operacional. Editorial Visión Conjunta.

Departamento del Ejército (2021). FM 3-12 Cyberspace Operations and Electromagnetic Warfare. Ejército de los Estados Unidos de Norte América.

Departamento del Ejército (2014). FM 3-38 Cyber Electromagnetic Activities. Ejército de los Estados Unidos de Norte América.

Donoso, R. (20 de Octubre de 2017). Infodefensa.com. https://www.infodefensa.com/texto-diario/mostrar/3118289/ciberdefensa-efectos-campo-batalla-y2

Ejército Argentino. (2016). ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza. Dirección General de Organización y Doctrina.

Estado Mayor Conjunto (2018). JP 3-12 Cyberspace Operations. Estado Mayor Conjunto de las Fuerzas Armadas de Estados Unidos de Norteamérica.

Estado Mayor Conjunto (2020). JP 3-85 Joint Electromagnetic Spectrum Operations. Estado Mayor Conjunto de las Fuerzas Armadas de Estados Unidos de Norteamérica.

Estado Mayor Conjunto (2014). PC-00-02 Glosario de Términos de Empleo Militar para la Acción Militar Conjunta. Estado Mayor Conjunto de las Fuerzas Armadas.

Estado Mayor Conjunto (2018). PC 10–01 Estado Mayor Conjunto de un Teatro de Operaciones. Estado Mayor Conjunto de las Fuerzas Armadas.

Estado Mayor Conjunto (2012). PC 13–50 Guerra Electrónica Para la Acción Militar Conjunta. Estado Mayor Conjunto de las Fuerzas Armadas.

Fernández, M. (2020). Orden DEF/710/2020, Boletín Oficial del Estado. Ministerio de Defensa Español.

Herrera, A (2017). Diseño y Planificación de las Actividades de Guerra Electrónica en el Ambiente Operacional. Escuela Superior de Guerra Conjunta.

Junta Interamericana de Defensa (2020). Guía de Ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. Gobierno de Canadá.

Ministerio Federal de la Defensa (2019). Kommando Cyber- und Informationsraum https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum

Martínez, F. (21 de abril de 2020). Elradar.es. https://www.elradar.es/las-acciones-ciberelectromagneticas-y-el-futuro-de-la-guerra-electronica/

Martínez, P. (2013). Guerra Electrónica. Academia Politécnica Militar. Ejército de Chile

Marrupe Pereyra, A. (2014). Diseño de un órgano director de guerra electrónica en apoyo al comando de nivel operacional. Escuela Superior de Guerra Conjunta.

Ejército del Reino Unido de Gran Bretaña (2017). Land Operations. Publicación de la Doctrina del Ejército AC 71940. Centro de desarrollo de Guerra Terrestre.

Rojas, S. (2014). Ciberdefensa y Ciberseguridad: una nueva prioridad para las naciones. Universidad Militar Nueva Granada Facultad de Relaciones Internacionales, Estrategia y seguridad Programa Relaciones Internacionales y Estudios Políticos.

Zsolt, H (2017). Guerra Electrónica en el Ciberespacio. Facultad de Ciencias Militares y Formación de Oficiales. Universidad Nacional de Servicio Público, Budapest, Hungría