Facultad del Ejército
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TRABAJO FINAL INTEGRADOR

Título: "La importancia de la Ciberdefensa y la Guerra Electrónica a nivel Táctico en el marco de las Operaciones Multidominio"

Que para acceder al título de Especialista en Conducción Superior de OOMMTT, presenta la Mayor NOELIA JESSICA ANABEL ORTIZ

Director de TFI: Teniente Coronel JUAN CARLOS GUERRA

Ciudad Autónoma de Buenos Aires, de abril de 2024.

Resumen

Los elementos de Ciberdefensa y Guerra Electrónica tienen un rol fundamental en las Operaciones Multidominio, porque inciden de manera directa en el ciclo de decisión del enemigo y permiten obtener grandes ventajas ántes de empeñar tropas en combate. En el ámbito militar la doctrina con respecto a la concepción estratégica del combate moderno al igual que la ciberdefensa están en desarrollo en este momento, esto genera vacíos de información e incertidumbre en el empleo eficaz de elementos especializados como los de Ciberdefensa y su integración con el resto de la organización.

Durante el desarrollo de la investigación en el primer capítulo explicaré cómo influye la vertiginosa evolución de las nuevas tecnologías de la información (TIC) en las guerras modernas; en el segundo capítulo está destinado al análisis de la doctrina sobre los elementos de Guerra Electrónica y Ciberdefensa (en adelanta GE y CD) como parte neurálgica de los sistemas de comando y control y finalmente en el tercer capítulo abordaré sobre los aspectos a tener en cuenta para la organización de dichos elementos especialmente a nivel Gran Unidad de Batalla (GUB).

La presente investigación permitirá arribar a conclusiones finales, donde se procederá a reunir y organizar toda la información obtenida, para poder determinar cuáles son los lineamientos generales para la organización de elementos de Ciberdefensa y Guerra Electrónica de la Gran Unidad de Batalla en marco de las Operaciones Multidominio, especialmente por la particularidad que tiene este tipo de operaciones en el combate moderno.

Palabras Clave: Ejército Argentino, Guerra moderna, Operaciones Multidominio, Ciberdefensa, Guerra Electrónica.

Índice

Índice de Figuras

Introducción

Antecedentes y justificación

En el ámbito de la Escuela Superior de Guerra del Ejército (ESGE) y la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas (ESGCFFAA) se realizaron trabajos de investigación con diferentes aspectos referidos a la Ciberdefensa y Guerra Electrónica (en adelante CD y GE).

En el repositorio digital del Centro Educativo de las Fuerzas Armadas (CEFA, 2023) se pueden observar los Trabajos Finales Integradores (TFI) realizados años anteriores donde los autores han investigado temas relacionados con el presente trabajo; Anca (2015a). *La conducción de las operaciones de Ciberdefensa: Principios básicos en el campo de combate moderno*, [Tesis de Especialización, Facultad del Ejército - Escuela Superior de Guerra]. Repositorio digital – CEFA y Anca (2015b). *La Ciberdefensa hacia el desarrollo de la interoperabilidad conjunta en el Teatro de Operaciones* [Tesis de Especialización, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas]. Repositorio digital – CEFA. En ambos trabajos desarrolla los conceptos de Operaciones Cibernéticas y la defensa cibernética en apoyo a las operaciones tácticas, el autor relaciona los principios a tener en cuenta en los escenarios de las Guerras Modernas y destaca la ejecución de acciones seguras en el ciberespacio para garantizar la Libertad de Acción en la Toma de Decisiones,

Por otro lado Cabrera(2019). *La importancia de redes informáticas en Ciberoperaciones en el marco de la GUB* [Tesis de Especialización, Facultad del Ejército - Escuela Superior de Guerra]. Repositorio digital – CEFA. En este trabajo el autor resalta el vacío de reglamentación vigente sobre estos aspectos en el nivel Táctico, y el Trabajo Final Integrador de Lamberti(2020). *La capacitación de los oficiales subalternos en organizaciones militares relacionadas con la CD* [Tesis de Especialización, Facultad del Ejército - Escuela Superior de Guerra]. Repositorio digital – CEFA. El último autor citado desarrolla entre otros

conceptos la importancia de la Capacitación y Concientización de los miembros del Ejército Argentino para que todo el personal opere de forma segura en el ciberespacio.

Estas investigaciones citadas anteriormente están directamente relacionadas y se tomarán de referencia para el desarrollo del presente trabajo.

El marco de referencia para las definiciones conceptuales será la doctrina rectora de las Fuerzas, Particularmente el reglamento "Conducción de las Fuerzas Terrestres" Ejército Argentino (2015) capítulo VII, sección VIII donde se refiere a conceptos generales de GE y sección XV describe lo referido a CD, su finalidad y responsabilidades.

Otra reglamentación rectora será el reglamento de "Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y GE de la Fuerza" Ejército Argentino (2017); el de ¨Organización y Funcionamiento de los Estados Mayores¨ Ejército Argentino (2023a) y el Glosario para la Acción Militar Conjunta, Proyecto Ejército Argentino (2023b).

El presente trabajo de investigación tiene la finalidad de profundizar sobre la esencialidad de la CD y la GE especialmente en el nivel de la Gran Unidad de Batalla en el marco de las Operaciones Multidominio (en adelante Op MD).

La CD y la GE han cobrado significativa importancia por la revolución tecnológica, los efectos de la proliferación a nivel mundial de las nuevas tecnologías de la información y las comunicaciones (TIC) impactaron en forma directa en el ambiente operacional lo cual provocó como resultante emergente la gran complejidad del concepto ¨multidominio¨ en los escenarios de las guerras actuales, realmente constituye un verdadero desafío poder controlar estos denominados dominios del ciberespacio y espacio electromagnético para garantizar el comando y control de las operaciones.

Hace unos años se analiza esta influencia de la revolución tecnológica, por ejemplo, Trama (2017) sostiene: ¨La diversa y amplia cantidad de agentes que utilizan o explotan esta

revolución tecnológica plantean una grave amenaza a la infraestructura crítica de los Estados y a las Misiones Operacionales¨ (p.56)

Los conflictos en la actualidad nos demuestran a diario que con la evolución en la forma de hacer la guerra, debemos adaptar nuestras organizaciones y nuestros conceptos de empleo a la realidad que vivimos, en la cual debemos hablar de este tipo de operaciones complementarias que serán prioritarias y hasta en ocasiones serán determinantes para lograr nuestros objetivos.

Con respecto a esto, Agumosa Pila (2020) indicó en su artículo lo siguiente:

> Las caracteristicas del tipo de operaciones militares en el futuro, en donde el entorno Volatil, Incierto, Complejo y Ambiguo (VICA) y los cambio de era que vivimos en los terrenos de la seguridad, de la energía, de la biotecnología o de la tecnología de la informática, hacen oportuno preguntarse ¿cuáles son los diferentes tipos de operaciones que pueden aparecer en el nivel regional o el internacional mirando por ejemplo, al año 2035?
>
> De esta forma, se pueden preparar y adiestrar a las 3 Fuerzas Armadas para que puedan hacer frente a las nuevas amenazas, además de facilitar el diseño de la estructura orgánica, la adquisición de capacidades militares de alta tecnología y otras complementarias, junto con el personal que se necesitará para dichas operaciones. (p. 2)

En el análisis que realiza el autor, hace hincapié en la importancia de evolucionar lo más rápido posible para estar a la altura de las necesidades de los nuevos escenarios del conflicto. Esto involucra también una evolución en la cultura de la organización, lo cual no es tan sencillo de alcanzar.

Luego de analizar las citas de diferentes autores, se observa cómo evolucionan en nuestro país estos conceptos relacionados a las nuevas amenazas de la guerra moderna.

Con respecto a lo que especifica actualmente nuestra doctrina, se observa que en la doctrina, Estado Mayor Conjunto Operacional (2023) establece el concepto de Op MD dentro de la nueva Concepción Estratégica de Restricción de Área el cual lo define de la siguiente manera:

> Las Operaciones Multidominio son operaciones tácticas planificadas y conducidas por el nivel operacional, donde determinadas capacidades de organizaciones normalmente modulares que actúan en ámbitos físicos y no físicos se conjugan en un espacio multidimensional a través de un enlace operacional, las cuales generan efectos sincronizados en momentos del ritmo operacional relacionados con a la identificación de vulnerabilidades críticas y disponibilidad de recursos (p.14)

En función de estas características de la Guerra moderna, mi intención es focalizar en el nivel táctico, analizar cuales son las necesidades del componente terrestre del teatro de operaciones (CTTO), sin dejar de lado que su planeamiento será centralizado en los más altos niveles pero su ejecución será descentralizada y de acuerdo al efecto a lograr se podrá ejecutar en cualquier nivel.

Para ello es necesario contar con estructuras orgánicas organizadas, equipadas e instruidas para llevar a cabo la operación de manera íntegra y eficiente garantizado especialmente la preservación de infraestructuras críticas de la información de los Sistemas de Comando, Control, Comunicaciones, Inteligencia, Informática y GE (en adelante C3I2 y GE).

Con respecto a los conceptos de CD y GE, normalmente lo encontraremos de manera individual, efectivamente son dos operaciones complementarias totalmente distintas, como se desarrolla en nuestra reglamentación anteriormente citada.

Es relevante que para llevar a cabo Operaciones de CD y/o de GE, debemos descartar que la organización en su conjunto posee la conciencia situacional y cumple detalladamente con los procesos de trabajo y las medidas pasivas ordenadas para evitar que los sistemas de

armas sean vulnerados por la explotación de una debilidad nuestra por parte del enemigo y preservar la seguridad tanto individual como del conjunto en todo momento.

Estos aspectos son el punto de partida, porque de otra manera no se podrá cumplir eficientemente con la misión asignada lo cual influirá significativamente en los niveles superiores y afectará directamente las infraestructuras críticas del estado.

Se debe entender también el concepto de Infraestructuras críticas e Infraestructura Crítica de Información, las cuales fueron determinadas inicialmente por la Ex Secretaría de Gobierno de Modernización de fecha 12 de septiembre de 2019, luego en el año 2021 fueron aprobadas por Boletín Oficial.

> Por la Resolución N°1523 se aprueba la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.
>
> Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.
>
> Que, de igual modo, la mencionada Resolución determina como Infraestructuras Críticas de Información a aquellas tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas. (Sain, 2021)

Una vez definidos estos conceptos, abordaré la temática desde el punto de vista de las estructuras organizacionales con las que cuentan las Fuerzas Armadas de nuestro país.

Con respecto a la CD (Ciberdefensa), inicialmente el Libro Blanco de la Defensa establece el Comando Conjunto de CD mediante Resolución MD 344/2014 el cual depende

orgánica, funcional y operacionalmente del Estado Mayor Conjunto Operacional (EMCO). Tiene como objetivo principal generar la capacidad de conjurar y repeler ciberataques contra las infraestructuras críticas de la información y los activos del Sistema de Defensa Nacional y de su instrumento militar.

> Las actividades desarrolladas por el comando se han centrado principalmente en la determinación de necesidades de equipamiento, comunicaciones y redes; el relevamiento de capacidades de cada fuerza, el análisis de proyectos de investigación y desarrollo en la materia; y la coordinación de los cursos de capacitación vinculados.
>
> La dirección general de CD fué creada por la Decisión Administrativa 15/2015 dentro de la estructura del Ministerio de Defensa (MINDEF). Tiene como responsabilidad primaria intervenir en el planeamiento, formulación, dirección, supervisión y evaluación de las políticas de CD para la jurisdicción y para el instrumento militar. Dentro de sus funciones se encuentra la coordinación con otros organismos y autoridades estatales y la promoción de vínculos de intercambio y cooperación con los ámbitos académico, científico y empresarial.
>
> Ambos organismos, el Comando Conjunto de CD y la dirección general de CD, funcionan integradamente y tienen por sede principal el Centro de CD. (Rossi, 2015)

Estos organismos que estipulaba inicialmente el Libro Blanco de la defensa, evolucionaron durante el paso de los años.

Se observa según lo investigado que el Comando Conjunto de Ciberdefensa, actualmente tiene la misión de conducir las operaciones de ciberdefensa, en forma permanente, con el objetivo de garantizar las operaciones militares del instrumento militar de la Nación de acuerdo con los lineamientos establecidos en el planeamiento estratégico militar.

¨Asimismo, deberá ser capaz de conjurar y repeler los ciberataques contra las infraestructuras críticas de la información y los activos del Sistema de Defensa Nacional y de su instrumento militar dependiente¨. (Ciberdefensa, 2023)

En el Ejército Argentino, dentro del Sistema Único de Comunicaciones e Informática (SUCOMI), a partir del año 2021 se creó el Subsistema Único de CD del Ejército Argentino (SUCEA)/ Dirección de CD del Ejército Argentino (DCEA), el cual depende de la Dirección General de Comunicaciones e Informática (DGCI) y junto con las direcciones de CD del resto de las Fuerzas Armadas se encuentra bajo control funcional del Comando Conjunto de Ciberdefensa (CCD). La DCEA tiene un elemento de Investigación y Desarrollo y un centro de operaciones de CD.

Con respecto al Apoyo de Guerra Electrónica (AGE), cuando se conforme un Teatro de Operaciones (TO) se apoyará sobre el sistema táctico de guerra electrónica (SITAGE) el cual estará apoyado sobre el nivel estratégico militar en el sistema estratégico de guerra electrónica (SIEGE) y a su vez ejecutará acciones de GE a nivel táctico con los elementos específicos de GE que tenga cada uno de los componentes. La doctrina lo establece de la siguiente manera:

> En el Ejército Argentino, las tareas que comprenden el Apoyo de Guerra Electrónica serán desarrolladas desde el subsistema fijo, por elementos pertenecientes al arma de Comunicaciones y a la tropa técnica de Inteligencia; pudiendo ser complementadas por tareas ejecutadas por el subsistema móvil o de campaña que deberán establecer, operar y mantener elementos del arma de Comunicaciones con capacidad específica para acciones de guerra electrónica. (Ejército Argentino, 2017, p.137)

Actualmente se encuentra en ejecución la Orden Especial del JEMGE Nro 60/5P/22: Acciones complementarias de evolución orgánica, la cual hace referencia a la Resolución Estratégica Militar del Estado Mayor Conjunto de las Fuerzas Armadas (EMCFFAA) la misma

tiene la finalidad de adecuar la estructura orgánica propia actual según la evolución orgánica prevista para los años 2022/2024.

Estas acciones de evolución orgánica involucran misiones particulares para llevar a cabo las la reorganización, la reestructuración y/o reingeniería en algunos casos, en los elementos ordenados.

Actualmente, según lo establece Ejército Argentino (2020). en el más alto nivel de la Fuerza el SUCOMI está conformado por CUATRO (4) subsistemas:

- El Subsistema de Comunicaciones e Informática Guarnicional del Ejército (SUCOIGE).
- El Subsistema de Comunicaciones e Informática de Campaña del Ejército (SUCOICE).
- El Subsistema de Guerra Electrónica del Ejército (SUGE).
- El Subsistema de Ciberdefensa (SUCIDEFE).

La reestructuración demuestra la importancia que tienen los elementos de CD y GE ante la necesidad del manejo de la información para la ¨Toma de Decisiones¨ en todos los niveles especialmente ante Op MD, donde las operaciones eficaces se lograrán por la sinergia de los efectos conjuntos, lo cual sólo se obtendrá mediante la conectividad e integración de todos los sistemas de armas, especialmente al garantizar los enlaces de todos los Puestos Comando.

Formulación del Problema

¿Cuáles son las principales características que deben tener los elementos de CD y GE para garantizar el Comando y Control a nivel de la GUB en el marco de las Operaciones Multidominio?

Objetivos

Objetivo General

Establecer lineamientos generales para organizar elementos de CD/GE y garantizar la Función de Comando y Control en la GUB en el marco de Operaciones Multidominio.

Objetivos Específicos

1. Explicar la evolución de la Guerra como consecuencia de los avances en las nuevas tecnologías de la información y las comunicaciones junto a las características de las Operaciones Multidominio para entender la influencia que tienen la GE y CD en este marco.
2. Analizar los elementos de CD y GE existente en apoyo a la GUB para identificar su importancia dentro de los Sistemas de Comando y Control.
3. Sintetizar los principales aspectos a tener en cuenta al organizar los elementos de CD y GE a nivel GUB para garantizar la función de comando y control.

Metodología a emplear

Explicación del Método

El método a emplear será deductivo.

Diseño de la Investigación

El diseño a utilizar será explicativo.

Técnicas de Validación

Las técnicas a emplear serán análisis bibliográfico, análisis documental y análisis lógico.

Capítulo 1

La Evolución de la Guerra y las Operaciones Multidominio

El propósito de este capítulo es analizar el impacto de las TIC en la evolución de la Guerra para entender los conceptos y las principales características de las Operaciones Multidominio.

Sección 1: Nuevas formas de hacer la Guerra por la influencia de la evolución de las TIC

Para iniciar esta sección es importante explicar que las TIC son las nuevas Tecnologías de la Información y las Comunicaciones.

Estamos en la ¨Era de la Información¨ la cual está en pleno auge; esta ¨Era¨ está asociada a la revolución digital iniciada en la segunda mitad de siglo XX, en la que las innovaciones como la radio, la televisión y el teléfono revolucionaron la forma de comunicarnos.

Luego el avance de las comunicaciones pasó de lo analógico a lo digital, donde la capacidad de transmisión de la información era mayor y mucho más rápida.

En la década de los 50, en los avances en programas informáticos y redes de computadoras enlazadas con internet, dieron origen a los distintos protocolos que más adelante se utilizaron para el diseño de nuevas topologías de redes.

En la década de los 70 ya se modificó la manera de almacenar los datos, la digitalización de dispositivos comenzaba a surgir, pero recién en la década del 90 impactaron en la sociedad, obviamente este impacto fue inicialmente en países más desarrollados, los cuales comenzaron a incorporar nuevas tecnologías inmediatamente en el ámbito de la educación, la industrialización y particularmente en las empresas.

Este aspecto no es menor, porque surge una gran diferencia con respecto a la interacción que tuvieron a lo largo de la historia las necesidades militares y las revoluciones que se acontecieron.

Por ejemplo los conceptos de ¨Estrategia¨, ¨Organización¨ y ¨Logística¨, que en su esencia surgieron en el ámbito militar y luego en su evolución fueron empleados para el ámbito civil, especialmente en la producción y en lo empresarial.

Esta evolución en las tecnologías de información, tuvo un evento importante y reciente que fué el episodio mundial de la Pandemia (COVID- 19). Ante este nuevo escenario, la sociedad en su conjunto tuvo que adaptarse a lo virtual y esto obligó a todas las generaciones a amigarse de alguna manera con la tecnología para poder cumplir con sus obligaciones; desde los niños que aún no sabían leer ni escribir hasta nuestros abuelos que debían realizar sus trámites de manera virtual.

Esta emergencia sanitaria aceleró drásticamente los cambios de la TIC, obligó la creación de nuevas tecnologías que soporten gran magnitud de datos y permitan el acceso a todo tipo de información. Estos cambios abruptos también trajeron grandes inconvenientes especialmente en la falta de clasificación de la información y el tráfico de datos.

Como señala Pedroza (2021) ¨Se ha evidenciado que el exceso de información ha ocasionado que los seres humanos se sumerjan en ella. No sabiendo, de este modo, distinguir entre la realidad virtual del mundo real¨ (p.1)

Ante esta realidad, debemos entender que el entorno en el que vivimos realmente es complejo, mucho más complejo de lo que podemos comprender o imaginar, por lo tanto describiremos este tipo de ambiente particular en el que hoy en día operan las fuerzas armadas de todo el mundo.

Lo describe en detalle Ministerio de Defensa de España (2019) dónde analiza los retos del entorno operativo para el año 2035, en el informe desarrolla los conceptos del entorno VICA e identifica la incertidumbre como una características constante que los Estados, de distintos actores no estatales y de la sociedad en general, plantea que la incertidumbre moldea y condiciona la forma en que los actores del sistema internacional planifican, actúan, responden

y se relacionan estratégicamente con el entorno, tanto a nivel internacional como doméstico.(p.19)

En cuanto a la volatilidad, se identifica esta cualidad en entornos que provocan cambios vertiginosos donde se dificulta la identificación de tendencias o patrones y afecta también la estabilidad de los procesos.

Estos cambios generalmente disruptivos, dificultan la capacidad de anticipar distintas amenazas y riesgos por lo cual es muy difícil la proyección de escenarios futuros deseados, esto afecta de esta manera en forma directa la metodología de la toma de decisiones.

Ésta es la razón por la cual el planeamiento debe ser la principal herramienta que nos permita la aproximación sistémica al análisis y síntesis de los problemas complejos, comprender la situación con pensamiento holístico, mente abierta y visión de futuro para poder visualizar la multiplicidad de causa y factores que están directamente relacionados con eventos o situaciones inesperadas.

Ante estos entornos cada vez más complejos es necesario evitar estereotipos o sesgos como también soluciones simples e inequívocas, porque si proponemos soluciones rápidas sin tener en cuenta este entorno VICA, nos llevará a cometer grandes errores.

Ante la ambigüedad de estos entornos, es muy difícil adoptar una solución completamente correcta, por lo cual es fundamental entender que debemos tener flexibilidad, agilidad y adaptabilidad ante este tipo de situaciones confusas.

Este tipo de entorno exige que las Fuerzas Armadas estén preparadas para nuevas amenazas o en su defecto, en capacidad de adaptarse rápidamente a los cambios que se presentan.

Obviamente estos entornos VICA se intensifican con el empleo de las nuevas tecnologías, es por ello que debemos pensar en la prioridad y urgencia de digitalización del campo de batalla.

Figura 1.

Entorno VICA

	Características	Efectos	Se requiere
Volatilidad	• Naturaleza del cambio • Velocidad del cambio • Dinámica del cambio	• Dificulta identificación de tendencias y patrones • Genera inestabilidad	VISIÓN
Incertidumbre	• Impredecibilidad • Desconocimiento de los resultados	Dificulta la anticipación de: • Riesgos y amenazas • Oportunidades	COMPRENSIÓN
Complejidad	• Multiplicidad de causas • Interrelación de factores	Dificulta la toma de decisiones	CLARIDAD
Ambigüedad	• Multiplicidad de interpretaciones	Desconocimiento de la situación	AGILIDAD

Nota. La figura resume lo citado del entorno VICA. Adaptado del Min Def España (p.19) por Ministerio de Defensa de España, 2019, Publicación de Defensa.

En el artículo sobre la evolución tecnológica de los sistemas de armas Navarro, J.M (2018) indica lo siguiente:

> La tecnología tiene un papel predominante en los combates modernos, da lugar a conflictos que se caracterizarán por el dominio y control de la información y el empleo eficaz de nuevos dispositivos, donde los conceptos para la resolución del problema militar ya no aplican al empleo tradicional, sino que mutan a la prevalencia de la ciberguerra, la guerra de la información y la influencia que esto implica en la opinión pública internacional, busca en todo momento lograr su Efecto Final Deseado (EFD) con acciones no cinéticas.(p.1)

Luego de analizar los avances tecnológicos, el entorno actual y su influencia en la forma de hacer la guerra, profundizaré sobre los conceptos de los dominios donde se desarrollan las acciones bélicas.

Actualmente los conflictos bélicos no se desarrollan solamente en la combinación del dominio aéreo, el terrestre y naval como en las guerras tradicionales anteriores a las guerra de cuarta generación, sino que debido especialmente a los avances tecnológicos los conflictos bélicos se desarrollan en todos los dominios de manera simultánea.

Nuestra doctrina conjunta incorporó los dominios del espacio, el ciberespacio, el espectro electromagnético y el humano en el proyecto del año 2018, donde expone muy escuetamente el concepto de multidominio, término que actualmente lo desarrolla y explica el Boletín Informativo Conjunto del EMCO desarrollado en el presente año. (Expuesto anteriormente en los antecedentes de la esta investigación).

En cuanto a los Dominios es de interés destacar las características especiales por la cual el Ciberespacio, es considerado un ¨Dominio¨ según la Junta Interamericana de Defensa (2020):

- Requiere capacidades únicas para operar en ese ámbito.
- No está totalmente abarcado por ningún otro ámbito (tierra, mar, aire, espacio).
- Se caracteriza por una presencia compartida de capacidades aliadas y adversarias.
- Es capaz de ejercer control sobre un oponente a través de la influencia y el dominio.
- Brinda oportunidades de sinergia con otros ámbitos.
- Proporciona oportunidades asimétricas entre todos los ámbitos. (p.23)

En este documento citado anteriormente se desarrollan algunas características particulares de este dominio, que es necesario destacar, donde explica que es un entorno artificial, creado por el hombre y de la misma manera que lo ha creado, puede modificarlo a voluntad.

Se observa que este dominio va mutando como lo desarrolla la Junta Interamericana de Defensa (2020) ¨El ciberespacio adquiere una nueva dimensión a medida que se desarrollan nuevas tecnologías y servicios; a esta altura poco tiene que ver internet original de la web y el correo electrónico a la actual de las redes sociales¨ (p.24).

Después de esta aclaración de porque es considerado un dominio particular, desarrollaré lo que explica el boletín informativo conjunto, que si bien desarrolla la nueva concepción estratégica para nuestro país, quedan todavía vacíos de información en cuanto a la aplicación

de las estrategia, por esta razón analizaré el concepto del Multidominio bajo el enfoque de otros países más desarrollados, como el de Estados Unidos de Norteamerica.

> En el desarrollo del concepto de la batalla multidominio, el Ejército intenta seguir el camino que fue abierto por los que desarrollaron el Combate Aeroterrestre. La batalla multidominio es un concepto impulsado por una elección proactiva y basado por la amenaza del fracaso.
>
> Es una evolución del concepto operativo del Ejército, detallando la respuesta a nuestras observaciones de los acontecimientos en el mar del Sur de China, la guerra de Nueva Generación rusa y los constantes desafíos en el Medio Oriente. Es un conocimiento del que Estados Unidos está alcanzando al final de un período en el que puede hacer cambios en forma voluntaria y sin tener que sufrir pérdidas severas. El Ejército debe desarrollarse y cambiar. (Perkins, 2018, p. 46)

Se observa en la cita anterior que el concepto de multidominio es la resultante de las lecciones aprendidas fruto de las experiencia de las Fuerzas Armadas de los Estados Unidos de Norteamérica (en adelante EEUU), la cual es muy valiosa para los paises como la Argentina que si bien tenemos experiencia en combate, no es la suficiente ni aplica actualmente como para llegar a este tipo de conclusiones.

Los estudios realizados sobre la experiencia de EEUU demuestran también la evolución en su pensamiento militar, donde adaptan las estrategias a las aristas tecnológicas de los conflictos con flexibilidad para no estancarse en conceptos erróneos.

> La renovación intelectual del nuevo modo de hacer la guerra para las Fuerzas Armadas de EEUU desembocó en el concepto de batalla multidominio en el año 2017, para luego evolucionar considerablemente al de operaciones multidominio en 2018, además de plasmarse en varios documentos de estrategias de modernización de material

y a la sorprendente creación del Mando de Futuros, que gestionaría los programas de modernización. Pulido, G.(Esp, 2021)

Luego de estos conceptos, el Comando de doctrina y adiestramiento del Ejército de los EEUU ha actualizado y desarrollado nuevos enfoques en función de las últimas experiencias y sobretodo la observancia de distintos conflictos.

Describe EEUU (2018) que las Operaciones de Múltiples Dominios y objetivos estratégicos, buscan que la Fuerza Conjunta amplíe el espacio competitivo (idea clave de la Estrategia de Defensa Nacional de 2018 y es una extensión lógica del Concepto Conjunto para Campañas Integradas de 2017) a través de un compromiso activo para contrarrestar la coerción, la guerra no convencional y la guerra de información dirigida contra socios.

Estas acciones disuaden simultáneamente la intensificación de hostilidades, vencen los intentos de los adversarios de "ganar sin luchar" y establecen las condiciones para una rápida transición al conflicto armado.

En el conflicto armado, la Fuerza Conjunta derrota la agresión al optimizar los efectos de múltiples dominios en espacios decisivos para penetrar en los sistemas enemigos estratégicos y operacionales de negación de área o de acceso, desintegrar componentes del sistema militar enemigo y explotar la libertad de maniobra necesaria para lograr objetivos estratégicos y operacionales que crean condiciones favorables para un resultado político.

Luego, la Fuerza Conjunta consolida las ganancias y disuade más conflictos para permitir la regeneración de fuerzas y el restablecimiento de un orden de seguridad regional alineado con los objetivos estratégicos de los Estados Unidos. (EEUU , 2018) (p.VII)

Tambien en esta publicación encontraremos que lo primero que describe como aspecto fundamental es el ambiente operacional emergente.

EEUU (2018) aborda tendencias que interrelacionadas configuran la competencia y el conflicto:

- Los adversarios disputan todos los dominios, el espectro electromagnético (EMS), y el ambiente de la información y el dominio de los EE. UU. no están asegurados
- Los ejércitos más pequeños combaten en un campo de batalla expandido que es cada vez más letal e hiperactivo
- Los estados nacionales tienen más dificultades para imponer su voluntad en un ambiente político, cultural, tecnológico y estratégicamente complejo
- Los estados casi similares compiten más fácilmente por debajo del conflicto armado, lo que hace que la disuasión sea más desafiante. (p. 6).

Desarrolla también aspectos sobre los estudios que lleva a cabo el Comando de doctrina y adiestramento del Ejercito de EEUU sobre potencias como China y Rusia, las cuales se destacan por haber aprovechado estos cambios abruptos del entorno complejo para expandir el campo de batalla en el tiempo, ellos buscan permanentemente no poder definir claramente entre paz y guerra; en los dominios del espacio y del ciberespacio y en geografía para crear un enfrentamiento táctico, operacional y estratégico distinto.

Sección 2: Análisis de las Op MD según la doctrina de nuestro país

Esta sección tiene la finalidad de analizar los principales lineamientos básicos para ejercer la conducción táctica y los pilares de nuestro accionar bajo el enfoque de las Op MD, como los factores de la Táctica, los factores del ambiente operacional; la relación de las Op MD con la estrategia de restricción de área y otros conceptos como los de gestión de la Información, conectividad y tecnología disruptiva directamente relacionados con el tema.

Como se describió anteriormente el concepto de MD integra todos los espacios en los ámbitos físicos y no físicos donde pueden desarrollarse las acciones bélicas. Normalmente se relacionan de acuerdo al nivel de la conducción, es decir a nivel táctico y operacional se desarrollan acciones cinéticas y los niveles estratégicos se caracterizan por las acciones no cinéticas. Este concepto se modificó debido a la evolución tecnológica, es decir en la actualidad las acciones no cinéticas se pueden dar en todos los niveles de la conducción.

Las acciones cinéticas y no cinéticas se refiere a lo establecido como Fuegos Cinéticos y no Cinéticos en el Boletín Informativo conjunto año 2023, donde estipula lo siguiente:

> Los "Fuegos Cinéticos" serán aquellos cuyo efecto es provocado por la fuerza destructiva proveniente de la energía cinética librada durante el impacto de proyectil que portan una carga explosiva y los "Fuegos No Cinéticos" serán aquellos cuyos efectos son de naturaleza indirecta, funcional, sistémica, psicológica o conductual, provocados por el uso de herramientas provenientes esencialmente de los ámbitos de la información, guerra electrónica, Ciberdefensa.
>
> Constituyen un concepto operativo integral donde los ámbitos no físicos se entrelazan para lograr superioridad en dicho entorno no cinético. Los fuegos no cinéticos cobrarán una relevancia superlativa, accionando no sólo sobre los ámbitos físicos sino también sobre los ámbitos no físicos. EMCO (2023,p.33)

Aclarados estos conceptos, se observa que las Op MD son parte de la estrategia multicapa, la cual buscará el dominio transversal a todos los espacios y en todos los ámbitos y en función de la misión se organizará para accionar en mosaicos (según capacidades o medios), sobre distintas plataformas (sistemas de armas tradicional) y/o con la metodología de enjambres (sistemas diversificados que actúan coordinadamente: ¨dispersión – concentración¨). Ejército Argentino (2023c)

Para analizar más en detalle este tipo de operaciones particulares y cómo influye en nuestros conceptos básicos, abordaré el tema relacionándolo con aspectos doctrinarios, en este caso, a los factores de la táctica: Espacio, Tiempo y Poder de Combate; los cuales cambian notablemente en las Op MD.

La combinación de estos factores buscará los momentos y lugares que aprecien convenientes para producir una serie de efectos sincronizados, con una coherencia y cadencia de las operaciones necesarias; de esta manera marcará así el ritmo de la operación según lo indica nuestra doctrina Ejército Argentino (2015,p.22 - III)

Se observa que estos conceptos básicos son alterados bajo la óptica de este tipo de Op ¨MD¨ donde se buscan explotar principalmente ventanas de oportunidad que se presente (o en ocasiones crearlas) y las vulnerabilidades en la integración de los dominios del adversario.

Se abordará a continuación cada uno de los factores de la táctica. Entre ellos se destaca el factor del espacio porque se ve seriamente afectado desde el punto de vista que ya no podemos determinar un espacio específico y tangible cuando empezamos a hablar que las acciones se desarrollaran en los espacios no físicos como son el espacio cognitivo, electromagnético, el espacio humano, espacial y el ciberespacio es muy difícil materializar los limites.

El primer factor a analizar es el espacio, que a los fines de esta investigación, es el más complejo y donde los aspectos legales todavía tienen vacíos importantes, al desarrollar el concepto de ¨ciberespacio¨, según el Comando Conjunto de Ciberdefensa (CCC); se observa que el mismo es entendido como:

> La infraestructura tecnológica, de propiedades físicas y virtuales, desplegada territorialmente, que permite la creación, procesamiento, almacenamiento, transporte y destrucción de información mediante el empleo de las tecnologías de la información, la

> operación y la comunicación, es el ámbito sobre el que se despliegan las acciones u operaciones de ciberdefensa encomendadas.
>
> Una de sus principales características es que, con medios y reglas propias, este no constituye un "espacio en sí mismo", sino que se trata de una dimensión que atraviesa a todos los espacios tradicionales (tierra, mar, aire y espacio), lo cual requiere un planeamiento y conducción militar de naturaleza conjunta. Ciberdefensa (2023)

Las Op MD justamente buscarán accionar en el ciberespacio para afectar de manera sinérgica y simultánea o no al resto de los espacios.

El segundo factor es el tiempo, bajo este concepto es importante valorar y visualizar el momento de las ventanas de oportunidad, debido a que estas Op MD pueden caracterizarse por tener otra concepción de tiempo, de un tiempo virtual o programado y desde cual se ven reflejados los efectos de determinadas acciones totalmente distanciado en el tiempo.

Con respecto a este factor uno de los aspectos que señaló (Intini, 2023) en el Seminario de ¨Tecnología Espacial para la Defensa¨ desarrollado en la Escuela Superior de Guerra (ESG) ¨Tte Grl Luis Maria Campos¨, fué que si bien tenemos grandes desarrollos en cuanto a tecnología de punta en Argentina, particularmente referido a tecnología satélital, por ejemplo, todavía hay partes componentes que no son desarrollados por nuestro país, por lo tanto aquellas partes (normalmente chinas) que se emplean para el desarrollo de tecnología espacial, pueden ser activos programados estratégicamente los cuales pueden despertar en un par de años.

El tercer factor es el Poder de Combate en este tipo de operaciones se observa que es realmente un desafío poder definirlo, especialmente el poder de combate relativo, porque si bien se puede apreciar las capacidades de las fuerzas convencionales del adversario, no se podrá definir en estos nuevos entornos operativos las dimensiones reales que puede tener. Se puede citar por ejemplo, en el conflicto de Rusia- Ucrania las acusaciones sobre el empleo de fuerzas Proxy.

Para poder hacer una aproximación de la medición del poder de combate relativo, hay que evaluar seriamente la multiplicidad de factores que influyen en este aspecto, más allá de las capacidades por cada uno de los dominios, la capacidad de integración y cooperación con otros actores, capacidad de obtención de recursos, capacidad de proyección de poder, estudiar sus posturas con respecto al uso de la información y como la integra entre dominios.

En conclusión, los 3 Factores de la Táctica se ven desvirtuados ante la caracterización de las Op MD.

A continuación analizaré los factores del ambiente operacional, este análisis se realiza para tener un entendimiento común de la situación donde representa un sistema complejo en un modelo teórico simple para facilitar su comprensión e identificar los efectos necesarios. Estos factores deberán hacerse sobre los ámbitos de competencia de cada fuerza y en cada nivel de la conducción.

Esto permitirá a todos los niveles tener actualizado el desarrollo y la evolución de la campaña y de las operaciones, como así también la importancia de sus contribuciones a la situación general. Lo expresado facilitará el control sobre las acciones de las unidades subordinadas, permitiendo a estas desarrollar acciones basadas en una iniciativa responsable y acorde con la intensión del comandante. Ejército Argentino (2015, p.1-VI)

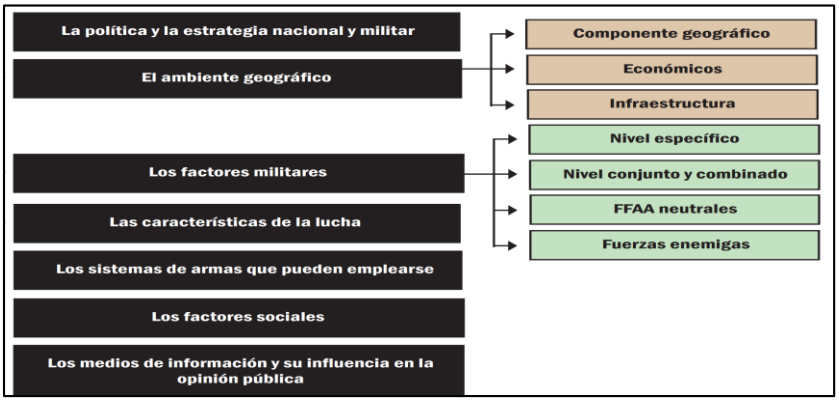
Ejército Argentino (2015) ¨Se entiende por ambiente operacional al conjunto de factores de diversa naturaleza que existen en forma estable y semiestable en una determinada región¨. (p.11- I)

Ante el enfoque de las Op MD todos los factores se verán particularmente afectados, especialmente si tenemos en cuenta que los avances tecnológicos influyen directamente en este tipo de operaciones.

Este análisis de los factores señalados debidamente integrados, como lo indica nuestra doctrina vigente, determinará el grado de complejidad en donde operarán nuestras fuerzas y el grado de libertad de acción de las mismas.

Figura 2.

Factores del Ambiente Operacional



Nota. La figura resume los Factores del Ambiente Operacional. Adaptado de *ROB 00-01* (p.11-I), por Ejército Argentino, 2015, Publicaciones Militares.

Se observa que los factores del ambiente operacional más afectados desde el punto de vista de la CD y GE en el marco de las Op MD, son:

- El del ambiente geográfico, el cual influirá de manera determinante en la ¨Conectividad¨ de los sistemas
- Los factores militares, en cuanto al estudio de las capacidades, limitaciones e integración de las fuerzas en el ámbito específico, conjunto y combinado; las características de la lucha en cuanto a la tecnología aplicada
- Los sistemas de armas que puedan emplearse incrementarán el poder de combate, pero será de vital importancia la integración y control de todos estos sistemas para evitar daños colaterales y disminuir vulnerabilidades, especialmente para no presentarle una ventana de oportunidad propia que

pueda explotar el adversario y al mismo tiempo adoptar las previsiones necesarias antes amenazas de los sistemas de armas del enemigo.

- Los factores Sociales, es uno de los más complejos, porque en el combate moderno las acciones operacionales interactúan en todo momento con aspectos civiles, desde la percepción y las actitudes que pueda tener la sociedad y los distintos actores involucrados y como esto puede favorecer o no al desarrollo de las operaciones
- La influencia que ejerce la opinión pública debido a lo difícil que es controlarla en esta Era de la información, donde no se puede diferenciar entre lo real y lo virtual, sumado a la manipulación de la información en forma intencional.

El estudio detallado de estos dos últimos factores y la previsión de distintas acciones para minimizar los efectos negativos en todos los niveles de la conducción brindará mayor grado de legitimidad a nuestras acciones.

En este análisis de los factores del ambiente operacional se puede destacar que es un desafío importante, desde el punto de vista de las comunicaciones, la CD y GE que podamos garantizar los enlaces y la conectividad efectiva entre las fuerzas que operan en los distintos dominios.

También es un gran desafío trabajar en cooperación con distintas entidades para evitar acciones de ciberataques o interferencias del adversario que afecten sensiblemente la seguridad y la sinergia de las operaciones propias sobre las cuales intentarán en todo momento accionar para cortar la continuidad de nuestro dispositivo.

Con respecto a la concepción de la Estrategia de Restricción de área, el Glosario de la Acción Militar Conjunta lo define como el concepto central inherente a la concepción estratégica militar que busca en primer lugar denegar al enemigo el acceso al teatro de operaciones, acción sobre el mismo desde las más largas distancias y; en caso de que el agresor

logre ingresar, negarle el control efectivo de áreas consideradas estratégicamente críticas. Ejército Argentino c, 2023, p.180)

Este concepto distingue cuatro capas para poder cumplir con la finalidad de la restricción de área, las capas son: Anticipar, prevenir, conjurar y repeler. Estas capas representan las acciones ántes, durante y después de las operaciones tácticas, otorgándole vital importancia a la protección de nuestras infraestructuras críticas para evitar una batalla decisiva.

Al abordar el concepto de restricción de área y su relación con las Op MD, se observa que dentro de la concepción estratégica de restricción de área, la línea de operaciones multidominio es la que combina los ámbitos físicos y no físicos, donde el campo de batalla moderno representa una integración completa de dominios a través de medios de combates que accionan en diferentes espacios.

Figura 3.

Operaciones Multidominio

Nota. La Figura muestra los distintos espacios y dominios. Adaptado del Comando Operacional de las Fuerzas Armadas, por Ejército Argentino, 2023, (Exposición en ESG).

La importancia que tienen estas Op MD bajo la concepción estratégica militar, presenta un gran desafío, el cual es la integración de todas las acciones conjuntas para lograr efectos

sinérgicos, lo cual principalmente se logrará con una eficiente y segura conectividad de todos los sistemas en todos los ámbitos y en todos los niveles de la conducción.

Para que esto sea posible debemos focalizar especialmente en el principio de Unidad de comando, pero en este caso esta unidad de comando deberá observarse como la unidad de esfuerzo adaptable para poder alcanzar la mayor expresión de la guerra de maniobras con ataques convergentes desde la dispersión, o desde distintos espacios de acción, como lo establece la doctrina anteriormente citada.

En este sentido la información y la conectividad desempeña un papel crítico, debido a que en función de cómo se gestione esa información, bajo los criterios de integración, seguridad, rapidez, redundancia, oportunidad y necesidad de saber será la influencia que pueda tener en el ciclo de decisión del enemigo y en la ejecución exitosa de nuestras operaciones, para lograr la mayor legitimidad posible.

Para que esto sea posible debemos focalizar en la importancia de organizar Puestos Comando en todos los niveles con la capacidad de gestionar correctamente la información mediante tableros de comando que permitan fusionar la información necesaria en imágenes o cartas de situación para que de un golpe de vista táctico se pueda interpretar la información disponible en tiempo real para la toma de decisiones como lo desarrolla en su investigación (Castillo, 2023, p.1)

Para lograr la situación militar favorable que persigue toda misión en la ejecución de operaciones eficaces, además de tener en cuenta las características de las mismas y su relación directa con los principios para la conducción de las operaciones militares, debemos centrar nuestros esfuerzos en la integración y coordinación mediante el enlace de todas las partes de sistema.

En este sentido, la conectividad y la tecnología disruptiva tienen un impacto significativo ya que permite una mayor integración, eficiencia y capacidad operativa en múltiples dominios.

Podemos citar por ejemplo la implementación de vehículos autónomos o drones para la obtención de información más precisa integrados con los sistemas de inteligencia y vigilancia para poder alertar sobre posibles amenazas y un mejor entendimiento junto a la continua actualización del ambiente operacional; esto permitirá a las fuerzas ser más resilientes y adaptables en este tipo de ambiente dinámico y complejo.

Conclusiones parciales

A partir de las características expuestas anteriormente del entorno complejo en el que están inmersas las Op MD y de la importancia de analizar exhaustiva y constantemente los factores del ambiente operacional, podemos inferir que es de suma importancia tener la capacidad de planificar e integrar de manera efectiva las capacidades de todos los dominios y la concepción de organizaciones flexibles que cuenten con recursos y equipamiento particularmente modulares e interoperables y logísticamente independiente.

Estos medios deberán estar respaldados por tecnología avanzada que permita la detección y neutralización de las fuerzas adversarias mediante elementos ágiles y resilientes que puedan realizar fuegos cinéticos y no cinéticos de largo alcance muy precisos, con el objetivo de desestabilizar al adversario a las más largas distancias.

No debemos dejar de lado que la percepción pública y la opinión nacional e internacional pueden afectar la legitimidad y el apoyo a las operaciones militares, lo que puede tener implicaciones políticas y estratégicas, para lo cual es muy importante, dentro de las fuerzas también contar con elementos específicos de Operaciones de Información que funcionen integrados permanentemente con el sistema de Comando y Control en las

operaciones y con acuerdos de cooperación con las distintas agencias con injerencia en este aspecto en todos los niveles.

Capítulo 2

Estructura Orgánica y Concepto de Empleo de Elementos de GE y CD dentro del Sistema de C3I2 en Apoyo a la GUB

Este capítulo tiene el propósito de identificar la organización y el concepto de empleo de los elementos actuales de GE y CD en apoyo a la GUB y su funcionamiento dentro de los Sistemas de Comando, control, comunicaciones, Informática e Inteligencia (C3I2).

Sección 1: Características de los Sistemas de C3I2

Para iniciar con la temática, es necesario especificar las características que tienen los sistemas de comando y control, visualizar cuáles son sus partes componentes y que elementos son necesarios para garantizar justamente la función de comando y control desde el punto de vista de las comunicaciones en lo referido a CD y GE.

> Un sistema de Comando y Control, como lo establece nuestra doctrina es un conjunto de medios humanos, equipos y materiales de alta tecnología que, integrados y estructurados en forma automatizada y por medio de procedimientos normalizados, posibilitará al comandante o jefe y a su órgano de asesoramiento, ordenar, controlar, comunicarse, conocer la situación de otras fuerzas amigas, las condiciones del terreno, las condiciones meteorológicas y al enemigo y sus acciones, en tiempo cuasi real. (EA, 2017, p 27).

En el mismo reglamento podemos encontrar varias definiciones de interés, especialmente a lo referido a la integración o la dinámica dentro del Sistema de C3 I2, como la que se describe a continuación.

> En un sistema de comando y control existe una interdependencia e integración entre sus partes constitutivas, es decir, entre sistemas de sensores para vigilancia y reconocimiento, facilidades o sistemas de comunicaciones, equipos de procesamiento de datos, personal afectado a las funciones de conducción y sus órganos de

> asesoramiento, procedimientos específicamente concebidos para tal fin, etc., a través de los cuales las partes obtienen información, la clasifican, la intercambian, la analizan, piensan, adoptan decisiones, imparten órdenes y supervisan la ejecución de las acciones, para lo que el Ejército Argentino adopta "conceptualmente" la sigla de C 3 I 2 que significa: Comando, Control, Comunicaciones, Informática e Inteligencia. (EA, 2017, p.28)

Dentro de los aspectos de importancia que debe reunir un Sistema de C3I2 según nuestra doctrina, es justamente un eficiente sistema de guerra electrónica y de ciberdefensa junto a enlaces eficientes de las redes de Comunicaciones e informática entre otros.

Particularmente quiero hacer hincapié en una de las características funcionales y operativas requeridas para que un sistema de C3I2 cumpla eficientemente con su finalidad, la cual es la alta capacidad de supervivencia que debe tener, ya que es una de las características imprescindibles para garantizar la función de Comando y Control.

(Ejército Argentino, 2017) Según indica la doctrina esta característica dependerá de:

- La resistencia a las acciones de guerra electrónica del enemigo.
- La resistencia a los ataques desde la superficie y desde el espacio aéreo.
- El grado de protección de los sistemas informáticos mediante las acciones de ciberdefensa directas contra los ataques enemigos.

La evasión y el engaño para evitar la localización física por medios ópticos, medios electrónicos y optoelectrónicos.

Todos estos aspectos son fundamentales para diseñar el Sistema de C3I2, estos sistemas se materializan en el diseño y dinámica que tiene los diferentes Puestos Comandos especialmente a nivel de la GUB.

Figura 4.

Características del Sistema C3I2

CARACTERÍSTICAS DE UN C^3 I^2 TÁCTICO		
GENERALES	**FUNCIONALES/OPERATIVAS**	**ESTRUCTURALES**
- Sistema auxiliar - Sistema adaptable	- Confiable - Alta capacidad de supervivencia - Amigable al usuario - Seguro - Potente - Flexible - Móvil - Interoperable	- Expandible - Integrado - Multifunción - Distribuido

Nota. La Figura resume las características del Sistema C3I2. Adaptado de *ROD 05-01* (p.8-1), por Ejército Argentino, 2017, Publicaciones Militares.

Sección 2: Estructura orgánica y concepto de empleo de elementos de GE y CD dentro de los Sistemas de C3I2 a nivel GUB

Esta sección tiene el propósito de identificar la organización y el concepto de empleo de los elementos actuales de GE y CD.

> En nuestro país actualmente está conformado el Comando Conjunto de Ciberdefensa (CCCD) el cual articula, coordina e integra el planeamiento, conducción y ejecución de las operaciones de Ciberdefensa entre la Subsecretaria de Ciberdefensa del Ministerio de Defensa de la Nación, los organismos pertinentes del Estado Mayor Conjunto de las Fuerzas Armadas y las dependencias específicas de cada Fuerza Armada del Instrumento Militar. (Ciberdefensa, 2023)

En el ámbito específico, el Ejército Argentino dentro del Arma apoyo de combate de Comunicaciones cuenta con la Dirección General de comunicaciones e Informática, la cual hasta el año pasado nucleaba las Comunicaciones e informática, la Guerra Electrónica y la Ciberdefensa del Ejército Argentino, en la misma dirección. El arma de comunicaciones lleva a cabo sus actividades mediante Unidades y Subunidades Independientes desplegadas a lo largo y ancho del país.

Con respecto a los temas necesario para esta investigación veremos los aspectos relacionados con los sistemas de Guerra Electrónica y la Ciberdefensa.

Referido a la GE (Guerra Electrónica), el Ejército Argentino cuenta con el Subsistema Único de GE (SUGE). El SUGE está actualmente conformado por el Sistema estratégico de GE (SIEGE), el cual cuenta con elementos de GE de Comunicaciones e Inteligencia, materializados en estaciones fijas y permanentes las cuales desarrollan las actividades de Apoyo de GE de manera ininterrumpida (Nivel Estratégico Militar y Operacional).

Otra organización del SUGE es el Sistema Táctico de GE (SITAGE) el cual en la paz se integra con el SIEGE para completar las capacidades de GE. El SITAGE en campaña brindará apoyo al CTTO y ejecutará tareas de Apoyo de GE (AGE) y Ataque Electrónico (AE).

En forma permanente todas las tropas ejecutaran actividades de Protección Electrónica. (PE) (EA, 2017, p.3 V)

La Unidad que hasta el momento centraliza este tipo de actividades de carácter táctico es el Batallón de Operaciones Electrónica 601 perteneciente a la Agrupación de Comunicaciones 601, la cual está en este momento en reestructuración por la Órden Especial de evolución Orgánica del arma. (Ejército Argentino, 2022)

Con respecto a la evolución orgánica de la Dirección General de Comunicaciones e Informática (DGCI), la cual durante este año desarrollará las modificaciones ordenadas, se constituye como ¨Dirección General de Comunicaciones, Informática y CD (DGCI y CD), la cual estará dividida a su vez en cuatro Direcciones: Dirección de CD (DCEA), la Dirección de Comunicaciones (Dir Com), la Dirección Informática (Dir Info) y la Dirección de GE (Dir GE).

Dentro de las misiones particulares de la orden, se establece que hasta el 31 Oct 23 se podrá proponer cambios y/o propuestas sobre la nueva organización de la DGCI y CD.

En esta evolución se ordenó también (a partir de la firma ministerial) el cambio de denominación del Batallón de Operaciones Electrónicas 601 (B Op Electron 601) a Batallón de GE y CD (B GE y CD) dependiente de la Jefatura de Agrupación de Comunicaciones 601 (Jef Agr Com 601).

La organización actual del Batallón de Operaciones Electrónicas 601 como fue explicado anteriormente, se denominó B GE y CD (a partir de la firma ministerial).

La misión del Batallón de Operaciones Electrónicas (la cual no está actualizada según las últimas modificaciones organizacionales) es la siguiente:

Según la doctrina vigente, (Ejército Argentino, 2017) El B Op Electrón (o B GE) establecerá, operará y mantendrá el principal sistema táctico de guerra electrónica (SITAGE) del componente terrestre del teatro de operaciones, para obtener información de las emisiones electromagnéticas del enemigo y afectarlas mediante acciones de ataque electrónico, a fin de contribuir con la neutralización o degradación del comando y control de las fuerzas enemigas y con la protección de las emisiones radioeléctricas de comunicaciones y especiales que ejecute la propia fuerza durante el desarrollo de operaciones militares. (p.182)

Para esta Actividad, el B Op Electrón, está conformado por:

- Compañía comando y servicios (Ca Cdo Ser).
- Compañía de guerra electrónica “A” (Ca GE “A”).
- Compañía de guerra electrónica “B” (Ca GE “B”).
- Compañía comando y control del procesamiento de guerra electrónica (Ca CCPGE).

Dentro de sus funciones que establece actualmente la reglamentación en vigencia (Ejército Argentino, 2017) podemos distinguir las siguientes:

- Establecer, operar y mantener el principal sistema táctico de guerra electrónica (SITAGE) del componente terrestre del teatro de operaciones.

- Ejecutar apoyo de guerra electrónica (AGE), mediante el desarrollo de las tareas de búsqueda, interceptación, escucha, localización, análisis, identificación, evaluación y registro de emisiones en el espectro electromagnético (EEM), particularmente en las bandas de alta frecuencia (AF/HF), muy alta frecuencia (MAF/VHF) y ultra alta frecuencia (UAF/UHF).
- Ejecutar acciones de ataque electrónico (AE) en el espectro electromagnético (EEM), mediante el desarrollo de tareas de interferencia electrónica (de comunicaciones y de no comunicaciones) y tareas de engaño electrónico en comunicaciones (engaño manipulativo y engaño imitativo).
- Establecer, operar y mantener UN (1) centro de procesamiento de guerra electrónica (CPGE) de nivel componente terrestre del teatro de operaciones.
- Integrar los centros de procesamiento de guerra electrónica establecidos por el B Op Electron y las Ca(s) Op Electron en el teatro de operaciones.
- Integrar el SITAGE en el sistema de inteligencia de señales que operan elementos de la tropa técnica de inteligencia.
- Integrar el SITAGE en los sistemas de guerra electrónica de las otras fuerzas armadas
- Entender en el análisis técnico de las emisiones electromagnéticas (inteligencia de mediciones y firmas de emisores – MASINT) que hayan sido interceptadas y escuchadas.
- Proporcionar la información obtenida, a través de las tareas de apoyo de guerra electrónica, a los órganos de dirección de inteligencia del componente terrestre del teatro de operaciones que sean definidos en el planeamiento.
- Eventualmente, establecer, operar y mantener estaciones fijas para la ejecución de tareas de apoyo de guerra electrónica.

- Asesorar a los oficiales de comunicaciones, informática y guerra electrónica (eventualmente a los comandantes) del comando del componente terrestre y de los comandos de grandes unidades sobre todos los aspectos, que le sean requeridos, relacionados con guerra electrónica, en especial sobre la protección electrónica (PE) que sea necesario aplicar.

En el desarrollo de algunas de las funciones se observa que esta Unidad centraliza las distintas actividades de Guerra Electrónica al más alto nivel, tiene capacidad de integración con otros sistemas, opera con personal altamente especializado en capacidad de procesar información y proporcionarla como input a los distintos órganos de dirección de inteligencia a nivel CTTO.

Este sistema de GE debe estar adecuadamente integrado al SCIP instalado ya que es parte importante del Sistema de C3I2 en este nivel. (Cabe destacar que se encuentra en revisión la reglamentación de dicho batallón, la cual se denomina ¨Conducción del Batallón de Guerra Electrónica y Ciberdefensa¨).

Con respecto a la Ciberdefensa, en este momento está establecida la Dirección de Ciberdefensa del Ejército Argentino (DCEA), según esta dirección podemos definir que entre sus objetivos se encuentran la prevención, el tratamiento, la identificación y la resolución de incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del Ejército Argentino. (DCEA, 2023)

Para ello contará con elementos en los batallones y en las subunidades independientes de comunicaciones los cuales dependerán técnicamente de esta dirección.

El apoyo de Comunicaciones, Informática, Guerra Electrónica y Ciberdefensa se materializará mediante la instalación, operación y mantenimiento de redes informáticas que se integrarán y serán parte del ciberespacio, ámbito donde se desarrollarán las operaciones de ciberdefensa.

Además de la instalación y mantenimiento de las redes, a través de las cuales se ejecutará la ciberdefensa, resultarán esenciales las actividades y tareas de seguridad informática, las cuales son el principal componente de las denominadas operaciones de ciberdefensa directa.

La seguridad informática (como lo establece nuestra doctrina) se proporcionará a través de:

- La protección física, que abarcará a las bases de datos, los servidores de los centros de datos principales y de alternativa en guarnición y aquellos que se establezcan en campaña y la protección a los enlaces (físicos y no cableados) de las redes informáticas
- La protección lógica, que se brinda por medio de software para seguridad en los accesos a la red (proxis, firewall, etc.) y software antivirus, malware, etc; La protección de empleo o utilización, que se logra mediante el cumplimiento de las directivas, normas y procedimientos operativos normalizados en vigencia y el adecuado manejo de los niveles de información. (EA f, 2023, p.6)

La seguridad informática requerirá una permanente actualización en el desarrollo de herramientas y aplicaciones con ese fin y de la "conciencia" de los usuarios para proteger la información y los sistemas frente a los ataques que sufran las redes. Ademas deberá preverse la utilización de canales de comunicación alternativos a la red informática instalada para la comunicación e impartición de órdenes, directivas y procedimientos tendientes a la neutralización y detección de ataques cibernéticos.

Con respecto a la concientización de la Seguridad Informática y de las Políticas de Seguridad para la Transmisión de Datos, la Dirección General de Comunicaciones e Informática como responsable primaria, estableció un manual con disposiciones legales vigentes, con el objeto de brindar una adecuada protección a la información, los sistemas

informáticos y el ambiente tecnológico de la Fuerza. La misma debe ser conocida y cumplida por toda la planta de personal de la Fuerza, tanto se trate de funcionarios como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista. Dirección (2023)

Actualmente además del B GE y CD, el cual apoyará de manera centralizada a un Componente Terrestre del Teatro de Operaciones (CTTO), según Ejército Argentino (2022) los Batallones de Comunicaciones que brindan apoyo a una Gran Unidad de Batalla (GUB) es decir a una División de Ejército, también cuentan con la responsabilidad de establecer la capacidad de Control de Comunicaciones y CD a su nivel.

Según la modificación en el presente año del Reglamento Conducción del Batallón de Comunicaciones, la misión es la siguiente:

> El Batallón de Comunicaciones (B Com) proporcionará apoyo de comunicaciones e informática a un comando de gran unidad de batalla o superior al que sea asignado, tanto en tiempos de paz como durante el desarrollo de las operaciones militares, para posibilitar en forma segura y en oportunidad, la transferencia de información en voz, datos y video con el comando superior, con los comandos subordinados y con los comandos del mismo nivel de conducción, formaciones y elementos dependientes, a fin de facilitar el comando y control. Ejército Argentino (2023d, p.14)

En cuanto a las capacidades desde el punto de vista de CD y GE:

El B Com deberá estar en capacidad de Instalar, operar y mantener un grupo de operaciones de ciberdefensa (perteneciente a la Sec CD/Ca Cdo y Ser) para asegurar el cumplimiento de las restricciones establecidas en el Plan CONEM, de las medidas de seguridad informáticas impuestas y para mitigar los efectos de actividad hostil en la propia red de campaña, preservando el funcionamiento de los servicios críticos del sistema de comunicaciones e Informática particular del comando apoyado. Ejército Argentino (2023d, p.15)

Con respecto a las funciones, el Jefe deberá asesorar al comandante y al estado mayor del comando al que es asignado, sobre los aspectos tácticos y técnicos de comunicaciones, informática, guerra electrónica y ciberdefensa, para la instalación y mantenimiento del Subsistema de Comunicaciones e Informatica Principal (SCIP) - en caso de no constituirse el departamento comunicaciones e informática del comando al que sea asignado.

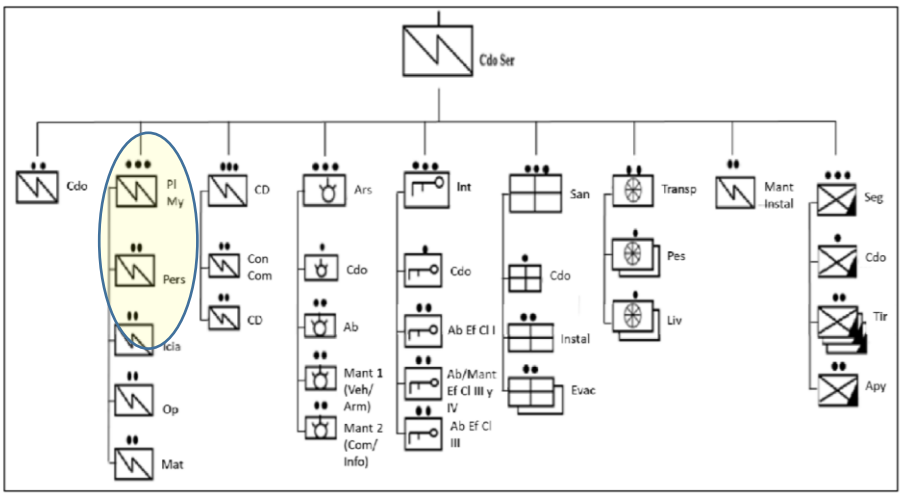
En el B Com se establecerá una sección de Ciberdefensa dentro de la Compañía Comando y Servicio, la cual tiene un grupo de ciberdefensa y un grupo de Control de Comunicaciones con capacidad de ejecutar el control de las comunicaciones en las bandas ordenadas y las acciones de ciberdefensa en las redes que instala, opera y mantiene la unidad.

La misión de la sección de CD es:

> Instalar, operar y mantener sus medios de monitorización, que permitan el control y supervisión del subsistema de comunicaciones e informática particular (SCIP) para asegurar el correcto cumplimiento del plan CONEM, normas operativas de tráfico y de empleo de los subsistemas instalados, es decir las Instrucciones de Empleo y Funcionamiento de Comunicaciones (IEC e IFC) y las políticas de seguridad de informática y de la información en particular, a fin de prevenir y preservar de toda ciberamenaza o ciberataque que afecte o intente afectar la seguridad de las infraestructuras críticas de información del sistema de comando, control, comunicaciones e informática de la fuerza apoyada, y garantizar la plena integridad, confidencialidad y disponibilidad de la información, asegurar el libre acceso al ciberespacio de interés y contribuir al comando y control de las operaciones. Ejército Argentino (2023d, p. 62)

Figura 5.

Sec CD - Ca Cdo y Ser - B Com



Nota. Adaptado de *ROP 05-05* (Anexo 9), por Ejército Argentino, 2023, Publicaciones Militares.

Como podemos observar la nueva reglamentación, contempla una sección de ciberdefensa para prevenir amenazas en nuestro sistema de comando y control.

Conclusiones parciales

De acuerdo a lo desarrollado, los Elementos de CD y GE deben considerarse en una acción conjunta e integrada para poder garantizar el correcto empleo de los sistemas de C3I2.

Ambas acciones están centralizadas a nivel CTTO pero surge el interrogante de como apoyar las operaciones en caso del de tener que apoyar en forma directa al TO.

Dentro del Arma, la Compañía de Comunicaciones Conjunta tendría esta responsabilidad pero no cuenta con elementos de CD ni GE para este apoyo; Si bien se entiende que el Arma cuenta con la Agrupación de Comunicaciones 601, la cual con sus elementos dependientes podrá reforzar las Unidades/ Subunidades de Comunicaciones en el TO, lo cual se establecerá oportunamente.

Con respecto a Ciberdefensa, a diferencia de lo que son las Actividades de Guerra Electrónica, contamos con la Dirección de Ciberdefensa del Ejército Argentino la cual articula

con el Comando Conjunto de Ciberdefensa, que trabaja ántes durante y después de las operaciones en forma conjunta con las Direcciones de Ciberdefensa de otras fuerzas. Actualmente están en desarrollo las capacidades en los batallones de los elementos de Ciberdefensa que apoyarán a las GUB e inferiores.

Referido a la Guerra Electrónica, si bien se constituye este año la Dirección de Guerra Electrónica y simultáneamente se encuentra en desarrollo el reglamento de Conducción del BGE y CD, como se explicó anteriormente, hay una Unidad de GE la cual operará con las prioridades necesarias a criterio del Cte TO.

Por otro lado estas acciones se ven limitadas a las Bandas de Frecuencia de Alta Frecuencia (AF), Muy Alta Frecuencia (MAF) y Ultra Alta frecuencia (UAF); Lo cual es bastante acotado si lo aplicamos a las necesidades de los Sistemas de C3I2 que deben funcionar inmersos en el Ambiente Operacional característico de las Operaciones Multidominio y la influencia de las nuevas tecnologías.

Capítulo 3

Aspectos a tener en cuenta al organizar los elementos de CD y GE a nivel GUB para garantizar la función de Comando y Control

Este capítulo tiene el propósito de identificar las características principales que deben tener los elementos de CD y GE para asegurar la función de Comando y Control según las necesidades de los Sistemas de C3I2 a nivel GUB

Sección 1: Aspectos principales a tener en cuenta para garantizar la función de Combate de comando y control a nivel GUB

La función de Combate de Comando y Control es uno de los subsistemas que permiten el desarrollo armónico y coordinado de las fuerzas para que puedan cumplir con su misión. Para ello desarrollaré los conceptos que involucra esta función, de manera separada para poder visualizar su naturaleza.

> Según nuestra doctrina en vigencia Ejército Argentino (2015), El comando es la función por excelencia del militar, el cual garantiza el óptimo empleo de la Fuerza, confiere a la organización militar flexibilidad, adecuación al desarrollo de las operaciones, elevado grado de reacción frente a situaciones imprevistas y continuidad operativa, aun en condiciones de disminución del poder de combate. Mediante el comando, el comandante / jefe inculca su voluntad e intención en forma de órdenes. (p 6 - Cap II)

Por otro lado define que el control, inherente a la función de comando, permite al comandante verificar y evaluar el desarrollo de la acción y sus resultados, como así también la dinámica adecuación del planeamiento y la dirección de las operaciones a la situación. (La velocidad y fluidez de las operaciones actuales, la información proveniente de múltiples y variadas fuentes y la exigencia de asegurar la presencia del comandante donde sea más necesario harán que este se vea en la necesidad de delegar el ejercicio del control).

Para el ejercicio de esta función, se requiere disponer de un sistema de comunicaciones e informática adecuado, eficaz y eficiente, que posibilite el comando y control, mediante la transferencia de información entre puestos de comando (principal, secundario (retaguardia), alternativa y/o táctico) y entre los comandantes / jefes y su estado mayor / plana mayor asegurando la ejecución de las Actividades Básicas de la Conducción, las cuales son: Planeamiento, organización, dirección, coordinación y control.

Ejército Argentino (2015) Especifica claramente que esta función, analizada desde un concepto sistémico, presenta dos subsistemas: el de comando y control y el subsistema de comunicaciones e informática, este último conforma la columna vertebral para el ejercicio del comando y el control, el cual permite al comandante recibir información en tiempo real e impartir órdenes para conducir desde cualquier punto en que se encuentre ubicado en el campo de combate.

Estos subsistemas, funcionarán integradamente como sistema, posibilitarán, sostendrán y apoyarán la capacidad del comandante o jefe para tomar decisiones basadas en información e inteligencia precisa y oportuna, como así también delegar la autoridad y sincronizar los sistemas operativos de combate para producir efectos en el campo de combate. Además, facilita ajustar sus planes para las operaciones futuras, sin perder el enfoque en las operaciones en desarrollo. (p. 6 Cap II)

Según nuestra reglamentación vigente referida a la Organización y Funcionamiento de los Estados Mayores. Ejército Argentino (2023a), uno de los pilares principales del sistema de Comando y Control es el Estado mayor, porque su organización inteligente se constituye como un multiplicador del poder de combate, es por ello que el estado mayor basará su eficacia en su capacidad para proporcionar información valiosa y en tiempo al comandante, adelantándose al ciclo de la información del enemigo (siempre y cuando tenga la información necesaria en cantidad, calidad y oportunidad de ser empleada en el ciclo de toma de decisiones) de esta

manera asegurar que las acciones de la fuerza logren el efecto deseado con la mayor eficiencia posible.

La organización del sistema de comando y control debe incluir todos los recursos disponibles que le permitan al comandante la conducción de las operaciones militares. El mismo deberá permitir el apoyo en el proceso de toma de decisiones; reunir producir y diseminar información/inteligencia relevante que facilite la comprensión y actualización de la situación táctica/operacional que se vive además deberán preparar y difundir planes y órdenes. Para la organización del comando y control el comandante deberá tener en cuenta:

- La cadena de comando la cual sirve para establecer claramente la autoridad y responsabilidad de cada comandante en su área de responsabilidad.
- El espectro del control, se refiere al número de elementos subordinados o actividades que pueden ser controlados por un solo comandante. Al momento de establecer la organización para el combate se debe tener en cuenta que este aspecto va a condicionar la toma de decisiones por parte del Cte/J.
- Unidad de comando, mientras sea posible, la organización en este tipo de elementos deberá ser hechos entre unidades que formen parte de una misma GUB y estén familiarizadas entre sí en cuanto a la forma de operar, planes de empleo, capacidades y limitaciones.

El Sistema de comando y control está conformado por los siguientes Subsistemas:

- El personal.
- Los procesos y procedimientos.
- Las redes.
- Las instalaciones de puestos de comando.

> El comando y control de las operaciones deberá realizarse en tiempos limitados, en función de los amplios espacios que la guerra moderna y lo que nuestra realidad geográfica impone, especialmente a nivel GUB donde habrá grandes vacíos de espacio e información. ¨El propósito final del propio sistema de comando y control será adelantarse al ciclo de decisión del enemigo. Esto obligará a encontrar el justo equilibrio entre dos extremos a evitar: decidir rápido y mal o decidir exacto y tarde¨. Ejército Argentino (2017,p. 4-Cap VII)

Esta función de Comando y Control está materializada en distintos lugares donde los miembros del Estado Mayor (EM) realizarán sus funciones de asesoramiento y asistencia. A nivel GUB, se materializará en un escalonamiento de cuatro lugares donde funcionarán necesariamente los distintos Puestos Comandos en apoyo a la Operación.

- Puesto Comando Principal.
- Puesto Comando de Alternativa.
- Puesto Comando Táctico.
- Puesto Comando Secundario o de Retaguardia.

Sección 2: Necesidades de elementos de GE y CD a nivel GUB para asegurar la función de Comando y Control

En función de lo desarrollado en la presente Investigación se observa que para poder llevar a cabo la función de combate de comando y control de manera eficiente necesitamos contar con recursos tanto de personal como de material acordes a las necesidades de los distintos Puestos Comandos que se deberán instalar a nivel GUB, para lo cual necesitarán apoyarse especialmente sobre un adecuado y eficiente Sistema de Comunicaciones e Informática, CD y GE

Para ello debemos contar con elementos de Comunicaciones, Guerra Electrónica, Ciberdefensa e Inteligencia, entre otros.

A los fines de esta investigación se focalizará en definir los lineamientos generales a tener en cuenta para organizar elementos específicos de CD y GE a nivel GUB, es decir en apoyo a las Divisiones de Ejercito en el marco de un CTTO, o eventualmente un TO.

A este nivel, la acción tanto de la Ciberdefensa como de la Guerra Electrónica debe visualizarse como una acción meramente conjunta, porque cualquier acción aislada, no controlada ni coordinada en conjunto afectará de manera directa el resto del accionar. Por lo cual es indiscutible que la conducción de estas acciones será de manera centralizada al más alto nivel dentro del TO. Según la investigación realizada el B GE y CD será el responsable a nivel CTTO, eventual u oportunamente también del TO.

Es importante destacar que la GUB necesitará de manera permanente y exclusiva elementos de Com, CD y GE, se entiende según lo desarrollado anteriormente, y lo actualmente ordenado que el B Com será el responsable con su sección de CD de mantener este apoyo.

Ante esta realidad es necesario establecer algunos lineamientos generales para el funcionamiento efectivo de estos elementos como parte del Sistema de Comando y Control.

Aspectos generales que deben tenerse en cuenta:

- Planificación conjunta. Máximo aprovechamiento de los medios existentes e integración.
- Conducción centralizada y ejecución descentralizada con elementos designados para tal fin, reforzados o constituidos como formaciones de la GUB (Esta temática requiere un estudio profundo de los distintos empleos de las GUB y los conceptos de empleo de las formaciones para poder proponer la viabilidad y la magnitud de los elementos de CD y GE como formaciones).
- Coordinación de acciones tanto de CD como de GE de manera conjunta y en forma centralizada, con personal altamente capacitado y equipos de tecnología de avanzada.

- Integración de los sistemas de C3I2, CD y GE de manera conjunta.
- Protección de Comunicaciones con equipos de tecnología avanzada ante ataques electrónicos y cibernéticos, mediante comunicaciones y transmisión encriptado y medidas de seguridad electrónica y cibernética.
- Capacidad de detección y supresión de amenazas.
- Respuesta inmediata de incidentes cibernéticos.
- Inteligencia compartida, mediante los elementos de procesamiento digitalizados dentro de los PC.
- Tableros de mando (Comando y control) digitalizados, con información en tiempo real o cuasi real e integrados con otros niveles a través de sistemas de información compartida y protocolos de comunicación efectivos.
- Adaptación continua, la integración de estas capacidades debe ser adaptable y sujeta a mejoras continuas porque las amenazas y la tecnología evolucionan constantemente.
- Aprovechamiento de las lecciones aprendidas, modificar y mejorar los sistemas después de ejercitaciones, entrenamiento y simulación de ataques cibernéticos y ataques electrónicos en todos los ejercicios (y en todos los sistemas, no solamente dentro del arma de comunicaciones)
- Acción de cooperación con ciberseguridad. Especialmente en las operaciones multidominio, ya que la infraestructura crítica como plantas de energía, sistemas de transporte y redes de comunicaciones, es un objetivo potencial para ataques cibernéticos.
- Operaciones de Información, que recopilen y analicen la información y datos en tiempo real, para una toma de decisiones más acertada.

Conclusiones parciales

Bajo los aspectos desarrollados en el presente capitulo, se observa la importancia del Comando y Control, como una de las funciones de combate más importantes, también es relevante entender que esta función se desarrolla por excelencia en el paso de Supervisión de la Acción (que contempla los conceptos de Comando, Control, Supervisión, Retroalimentación y Dirección) donde integra las Actividades Básicas de la Conducción (ABC) mediante el establecimiento de los diferentes Puestos Comandos para que se puedan desarrollar estas actividades junto a las de asesoramiento y asistencia de los miembros del Esta Mayor.

Para que esto se pueda llevar a cabo es necesario contar con sistemas de Comunicaciones e informática eficientes, seguras y redundantes para que puedan tener la flexibilidad necesaria ante cambios imprevistos, los cuales son característicos en las Op MD.

Bajo estos aspectos es esencial contar con organizaciones de GE y CD altamente capacitadas para proteger las comunicaciones, las redes y los sistemas de armas. Entender que el ciberespacio es transversal a todos los dominios, por ello es necesario contar con protocolos y medidas de seguridad compartidas por todas las Fuerzas Armadas.

Para establecer especialmente las organizaciones de CD y GE es fundamental tener en cuenta los siguientes aspectos:

- Personal altamente capacitado
- Compatibilidad
- Integración
- Protección
- Autonomía
- Automatización
- Protocolos estandarizados
- Sistemas de procesamiento y control de producción nacional

Conclusiones finales

El nivel Táctico, según lo que desarrolla Serrano (2023) se caracteriza por su naturaleza específica pero especialmente coordinada en el marco de acción conjunta, es en donde la esencia es el duelo de acciones y efectos mediante el empleo de los medios para imponer la voluntad y cumplir misiones con mayor grado de concreción.

Se observa que el corazón para la conducción militar en todos los niveles son los Sistemas de C3I2, materializados en los distintos puestos comandos que instalará la GUB, los cuales van a facilitar la concreción de escenarios deseados (dentro de los posibles) que presenta la situación operacional y crear las condiciones para desarrollar las acciones dentro del nivel táctico para lograr con ello un equilibrio entre la percepción y la acción y fundamentalmente minimizar abstracciones.

Dentro de los conceptos desarrollados en el primer capítulo de la presente investigación, se observa cómo las TIC surgen en esta evolución de la era de la información y obliga al Instrumento Militar a cambiar la manera de hacer la guerra, la cultura organizacional, tanto en el empleo de los distintos sistemas de armas como en el tipo de enlaces que se necesita para poder transmitir de manera instantánea y en tiempo real la información necesaria para la toma de decisiones, de esta forma favorecer el ciclo OODA (observación, orientación, decisión y acción) e irrumpir en el ciclo de decisión del enemigo.

Dentro de esta concepción en el nivel de trabajo de la GUB, cobra una vital importancia las características de las Operaciones Multidominio, donde los factores del ambiente operacional son afectados por la complejidad y los avances tecnológicos ante esto es fundamental la integración de ciberdefensa, guerra electrónica y comunicaciones para garantizar la seguridad, la resiliencia y la efectividad de las fuerzas. Esto requiere una coordinación cuidadosa, la cooperación con agencias y una comprensión profunda de las amenazas y las capacidades en cada uno de estos dominios para poder controlarlos.

Si bien en nuestro país tanto la CD como la GE tendrán sus respectivas Direcciones, estos elementos deberán necesariamente accionar también en el campo de combate hasta el menor nivel, es decir con organizaciones asignadas orgánicamente a nivel GUC. (Las cuales según la evolución orgánica del Arma de Comunicaciones, son parte de las Unidades y Subunidades de Comunicaciones asignadas a las GGUU).

También se podrá establecer la necesidad de contar con un elemento especialmente de GE independiente asignado como formación a la GUB; para darle al Comandante del CTTO una herramienta totalmente necesaria para accionar en el dominio electromagnético y poder realizar actividades de AGE en forma permanente sin perder la facilidad, ante un eventual empleo exclusivo en el TO.

En lo expuesto durante el desarrollo de la presente Investigación, se detalla que la Guerra Electrónica y la Ciberdefensa se desarrollan en ámbitos diferenciados porque son de distinta naturaleza, y tiene especificaciones técnicas que requieren ser operadas por personal altamente capacitado en cada una de ellas.

Cabe destacar que mientras las acciones tanto defensivas como ofensivas de CD pueden ser ejecutadas desde los asientos de paz, las acciones de GE muy por el contrario, necesitan estar desplegada en el TO para poder tener el alcance eficaz necesario para llevar a cabo sus acciones tanto de AGE como de AE.

Se observa que bajo el concepto de las Op MD, el término de Sistemas de C3I2 ya queda obsoleto ante las necesidades del ambiente operacional en el marco de las Op MD, de hecho algunos autores de otros países, ya imponen el concepto de Sistemas integrados de Comando, Control, Compunciones, Cibernética, Inteligencia y Guerra Electrónica. (C4IG), otros agregan Vigilancia y Reconocimiento. (C4I2VR)

Otro aspecto importante es la protección de la información ya que en este entorno de ciberataques y de comunicaciones digitales requerirá de los mayores esfuerzos para asegurar el comando y control, a la vez que procura obtener la superioridad sobre el comando enemigo.

Aporte Profesional

Como lineamientos generales, en función de lo observado durante la investigación, los elementos de GE y CD deberían tener las siguientes características y/o capacidades:

- Integrados a todo el Sistema de Comando y Control
- Control y monitoreo centralizado de las comunicaciones y enlaces de todos los sistemas de armas de las GGUU
- Control y monitoreo centralizado de los sistemas guiados
- Deberán tener ejercitaciones permanentes para probar y mejorar los sistemas
- Integración con ciberinteligencia
- Manejo remoto de todos los sistemas.
- Desarrollo de tecnología avanzada nacional para garantizar la automatización de procesos tanto de CD como de GE – capacidades propias.
- Posibilidad de implementar Vehículos Aéreos no tripulados (VANT) para GE con capacidad de ejecutar AGE y AE por saturación. (lo cual amerita una investigación aparte). Especialmente por la dificultad que presenta la localización de los mismos y porque minimiza la afectación de nuestras propias comunicaciones.
- En GE, Implementación de inhibidores de frecuencias, los cuales se podrán establecer si estandarizamos las comunicaciones en todos los niveles y cumplimos acabadamente con los criterios de emisión.
- Integración y cooperación con agencias gubernamentales y no gubernamentales afines.

- Implementación de Inteligencia Artificial dentro de los Sistemas de C3I2 para detectar vulnerabilidades de manera controlada en nueva concepción estratégica de Restricción de área, especialmente en la capa Anticipación.

Sería interesante poder diseñar un Sistema de C4I2VyR integrado, establecidos por los criterios de modularidad, con sistemas compatibles en todos los niveles y logísticamente independientes.

Estos sistemas deben estar equipados con tecnología de punta y personal altamente capacitado para poder hacer frente a las amenazas que representa las nuevas Guerras en Red.

> Como lo define el Glosario Conjunto en Vigencia las Guerras en Red son modos de conflictos (y crimen) a niveles sociales, con pocos puntos de contacto con las guerras tradicionales, en el cual los protagonistas usan las formas de organización en red, doctrinas, estrategias y tecnologías en sintonía con la era de la información. Conformado por organizaciones dispersas, pequeños grupos e individuos que se comunican, coordinan y operan de manera interconectada, a menudo sin un comando y control central. Ejército Argentino (2023b, p. 101)

Este diseño también debería tener en cuenta los aspectos desarrollados en las conclusiones finales y sobre todo sería de mucha utilidad poder contar con medios suficientes desde el punto de vista especialmente de GE, para poder mantener la redundancia de medios específicos y que puedan cumplir su misión de manera independiente y bajo el canal técnico de las Direcciones respectivas.

En este sentido, establecer una Sección de Guerra Electrónica como formación de las Divisiones, comandadas por personal idóneo y especialista, particularmente para que puedan asesorar y asistir al Comandante de la GUB respectiva con la especificidad correspondiente.

Referencias

Argumosa Pila. (21 de Noviembre de 2020). *Academia de las Ciencias y las Artes Militares.* Sección de Futuro de las Operaciones Militares: https://www.acami.es/publicacion/tipos-de-operaciones-militares-2035/

Anca, L. J. (2015a). *La conducción de las operaciones de Ciberdefensa: Principios básicos en el campo de combate moderno*. ESG.

Anca, L. J. (2015b). La ciberdefensa: hacia el desarrollo de una interoperabilidad conjunta del Teatro de Operaciones.

Cabrera, C. I. (2019). Empleo de las redes informáticas en Ciberoperaciones en el marco de la Gran Unidad de Batalla.

Castillo, A. G. (2023). *Tablero de mando como herramienta de apoyo al proceso de toma de decisiones militares en Operaciones Multidominio.*

CEFA. (2023). *Repositorio Digital del Centro Educativo de las FFAA*. Cefadigital: http://www.cefadigital.edu.ar/

CESIM, C. d. (2022). *Conflictos futuros: tendencias para la región sudamericana al 2040.* Chile.

Ciberdefensa, C. C. (2023). *CCC*. Comando Conjunto de Ciberdefensa: https://www.fuerzas-armadas.mil.ar/Comando-Conj-Ciberdefensa/index.html

DCEA. (2023). *Publicaciones de Ciberdefensa*. https://portal.ejercito.mil.ar/proxy/388db1be/https/www.ciber.ea.mil.ar/

EEUU . (2018). *El Ejercito de los EEUU en Operaciones de Multiples dominios 2028.* EEUU: Panfleteo 525-3-1 Tradoc.

Ejército Argentino (2015). *ROB 00-01 Conducción de las Fuerzas Terrestre.* Buenos Aires: Publicaciones Militares.

Ejército Argentino (2017). *ROD 05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, Informatica y Guerra Electrónica de la Fuerza.* Buenos Aires: Publicaciones Militares.

Ejército Argentino (2020). *Conducción del Batallón de GE y CD (Proyecto).* Buenos Aires, Buenos Aires, Argentina: Publicaciones Militares

Ejército Argentino (2022). *JEMGE - Orden Especial del JEMGE nro 60/5P/22.* Buenos Aires: Publicaciones Militares.

Ejército Argentino (2023a). *ROD 71-01 I Organización y Funcionamiento de los Estados Mayores.* Buenos Aires, Argentina: Publicaciones Militares.

Ejército Argentino (2023b). *PC 00-02 Glosario para la Acción Militar Conjunta.* Buenos Aires: Publicaciones Militares.

Ejército Argentino (2023c). Concepción Estratégica Operacional. *Exposición - Clase ESG*. Buenos Aires.

Ejército Argentino (2023d). *ROP 05-05 Conducción del Batallón de Comunicaciones.* Buenos Aires: Publicaciones Militares.

Estado Mayor Conjunto (2023). Comando Conjunto FFAA. *Boletín Informativo Conjunto*. Buenos Aires, Argentina: EMCFFAA.

Pulido, G. Esp. (2021). *Guerra Multidominio y Mosaico.* Madrid: Los libros de la catarata.

Informática, D. G. (2023). *DGCeI- Manual de Seguridad Informática.* Buenos Aires: Publicaciones Militares.

Intini, A. (2023). Tecnología espacial para la defensa. Buenos Aires.

Junta Interamericana de Defensa. (2020). Ciberdefensa. *Guia de Ciberdefensa*, 113.

Lamberti, H. J. (Marzo de 2020). La capacitación del Oficial Subalterno para ocupar puestos en organizaciones militares relacionada con la ciberdefensa.

Min Def España. (2019). *Entornos Operativos 2035.* España: Publicaciones de Defensa del Gobierno de España.

Navarro, J.M. (24 de Junio de 2018). *Defensa.com.* Obtenido de La evolucion tecnológica de los sistemas de armas: https://www.defensa.com/reportajes/evolucion-tecnologica-sistemas-armas

Pedroza, S. (28 de 08 de 2021). *La era de la información* . https://muytecnologicos.com/historia/era-de-la-informacion

Perkins, D. G. (marzo de 2018). *Military Review.* file:///C:/Users/leand/Desktop/TFI/Perkins-batalla-multidominio-1.pdf

Rossi, A. O. (2015). *Libro Blanco de la Defensa.* Mindef: www.libroblanco.mindef.gov.ar

Sain, G. R. (19 de 02 de 2021). *Jefatura de Gabinete de Ministros Direccion Nacional de Ciberseguridad*.boletinoficial.gob.ar: https://www.boletinoficial.gob.ar/detalleAviso/primera/241077/20210222

Serrano, A. (Septiembre de 2023). Estrategia y Pensamiento Militar, EYPM. *Clase*. Buenos Aires, Argentina: Ejército Argentino.

Trama, G. A. (2017). Operaciones Ciberneticas. *Vision Conjunta, 9*(17), 57.