



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



## **TRABAJO FINAL INTEGRADOR**

**Título: “Diseño de unidades en el marco de una Brigada Multidominio que combine capacidades de comando, control, comunicaciones, guerra electrónica, cibernética y de inteligencia (C4IG)”**

**Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor José GARAY**

**Director de TFI: TC Martín URQUETA**

**Ciudad Autónoma de Buenos Aires, de marzo de 2023**

## Resumen

Las características de los combates actuales imponen a las Fuerzas Armadas Argentinas la necesidad de adoptar una nueva concepción estratégica orientada a las operaciones multicapa y multidominio. Las operaciones multidominio son planificadas y sincronizadas por el nivel operacional a través de un estado mayor multidominio, que, mediante tecnología avanzada, integran todos los espacios en los que pueden operar las Fuerzas Armadas. Sin embargo, considerando que estas operaciones son ejecutadas por el nivel táctico, es crucial contar con una integración de todos los elementos a través de un sistema de comando, control, comunicaciones, ciberdefensa, inteligencia y guerra electrónica. Este sistema debe permitir, en tiempo real, recopilar información, almacenarla, procesarla, adoptar una resolución e impartir las órdenes necesarias para afectar vulnerabilidades críticas del adversario. En este contexto, la investigación se propone diseñar los elementos de una Brigada Multidominio capaz de integrarse al sistema del nivel operacional para llevar a cabo operaciones multidominio de manera efectiva y eficiente.

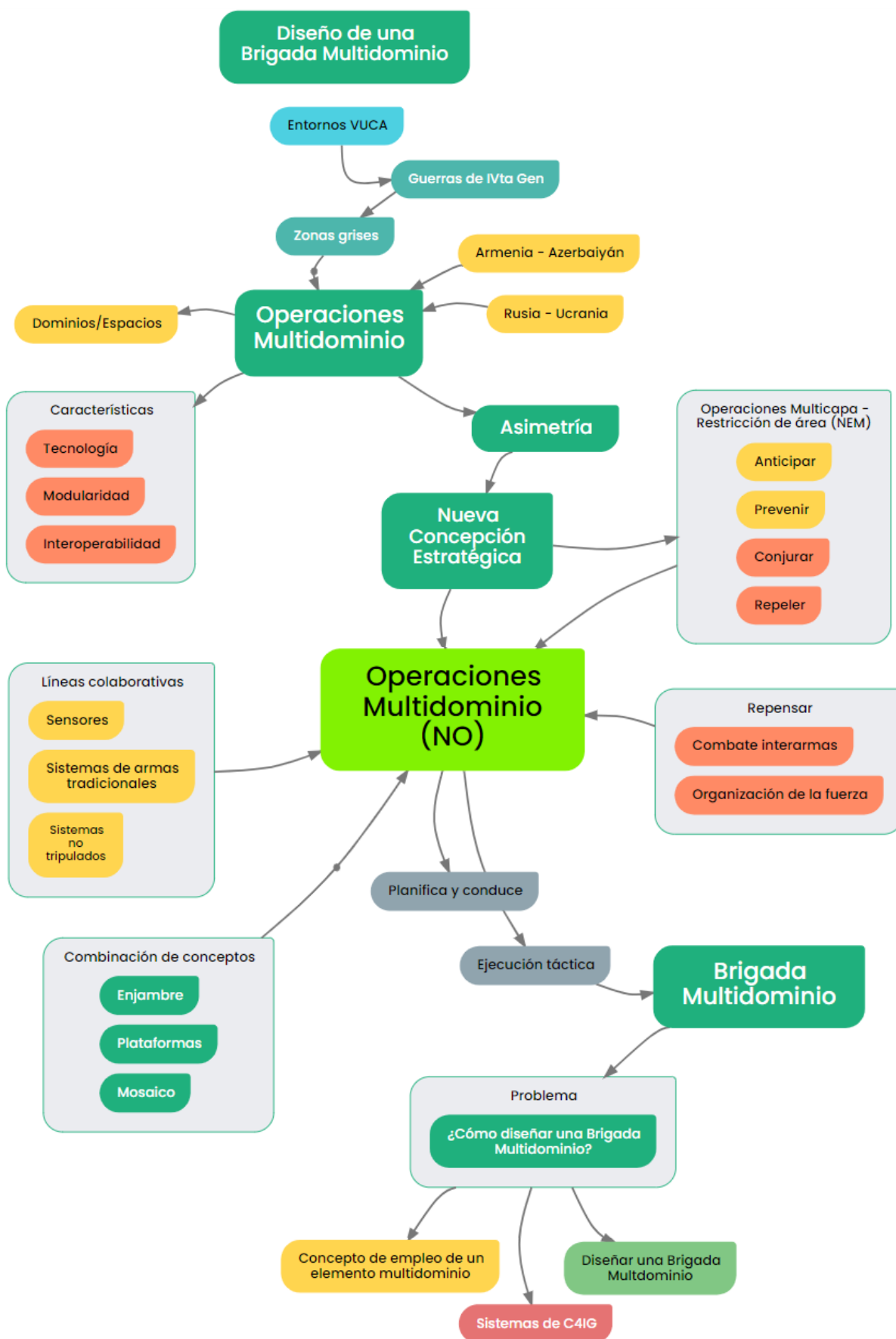
*Palabras clave:* operaciones multidominio, brigada multidominio, comando, control, comunicaciones, transmisión en tiempo real, organizaciones modulares.

## Tabla de contenidos

Resumen.....	ii
Tabla de contenidos .....	iii
Mapa conceptual .....	1
Introducción .....	2
Antecedentes y Justificación .....	2
Formulación del Problema .....	11
Objetivos .....	11
Objetivo General.....	11
Objetivos Específicos .....	11
Metodología a Emplear .....	11
Explicación del Método.....	11
Diseño de la Investigación.....	11
Técnicas de Validación.....	12
Capítulo 1.....	12
Concepto de Empleo de la Brigada Multidominio.....	12
Propósito del Capítulo .....	12
Sección 1 Desarrollos y Experimentaciones .....	12
EEUU.....	13
España.....	13
Israel .....	14
Rusia .....	14
Sección 2 Concepto de Empleo de un Elemento Multidominio .....	15
Conclusiones Parciales .....	16
Capítulo 2.....	17
Sistemas de C4IG Multidominio.....	17
Propósito del Capítulo .....	17
Sección 1 Herramientas para el C4IG Multidominio .....	17
El Satélite.....	19
Inteligencia Artificial.....	21
Servicios de Nubes Digitales .....	22
Transmisión en Tiempo Real.....	23
Sección 2 Integración de los Sistemas C4IG a las operaciones multidominio .....	24
Conclusiones Parciales .....	26
Capítulo 3.....	28
Diseño de la Brigada Multidominio .....	28
Propósito del Capítulo .....	28
Sección 1 Diseño de la Red de C4IG de la Brigada Multidominio.....	28
Sección 2 Diseño de los Elementos para Integrar las Capacidades C4IG a la Brigada Multidominio .....	30
Conclusiones Parciales .....	32
Conclusiones .....	34
Conclusiones Finales .....	34
Aporte Profesional del Autor .....	35

Bibliografía .....	37
Apéndice A .....	39
Figura A1 .....	39
Tabla A1 .....	40
Figura A2 .....	41
Apéndice B.....	42
Figura B1 .....	42
Figura B2 .....	43
Figura B3 .....	43
Figura B4 .....	44
Figura B5 .....	45
Figura B6 .....	45
Figura B7 .....	46
Figura B8 .....	47

### Mapa conceptual



## Introducción

### Antecedentes y Justificación

Al momento de describir los conflictos armados hoy en día, existen dos variables importantes, el entorno en el que operan las fuerzas armadas y el tipo de guerra que desarrollan.

Entendiendo que el entorno en el que operan las fuerzas armadas se caracteriza por ser volátil, incierto, complejo y ambiguo (VICA), muy dinámico y difícil de predecir, lo que puede presentar desafíos significativos para las fuerzas armadas que operan en él; este fenómeno se hizo popular luego de la caída de la Unión Soviética y se emplea para definir los conflictos futuros.

Las características de un entorno VICA son:

1. Volátil: es altamente inestable y puede cambiar rápidamente, por lo que las fuerzas armadas deben ser capaces de adaptarse a los cambios de manera efectiva y rápida.
2. Incierto: las condiciones pueden ser difíciles de prever y los planes pueden tener que ajustarse en función de los cambios inesperados.
3. Complejo: debido a la gran cantidad de factores que influyen en él. Las fuerzas armadas deben ser capaces de entender la complejidad del entorno y adaptarse en consecuencia.
4. Ambiguo: la información puede ser confusa y contradictoria, lo que puede dificultar la toma de decisiones.

Según Lind (1989), los principales conflictos armados desde la caída de la Unión Soviética son definidos como guerras de cuarta generación, donde sus principales cuatro características son:

1. La gran dispersión de las tropas, incluyendo como participantes del conflicto también a la totalidad de la sociedad, propia y del enemigo, derivando al empleo de fracciones menores, flexibles y trabajando bajo la intención del comandante;
2. La decreciente dependencia de logística centralizada, donde esta descentralización, sumada a la importancia de la oportunidad, requiere una gran habilidad para vivir de la tierra y del enemigo;
3. El énfasis en la maniobra, en la cual, la masa y el poder de fuego no son factores determinantes sino la maniobra en sí, hasta llegar al punto que la gran cantidad de medios y personal pasan a ser una desventaja, y donde fuerzas ágiles tienden a dominar el combate.
4. El objetivo se cumple con el colapso de la voluntad de lucha del enemigo en vez de su destrucción física, desviando la atención de los medios de combate del enemigo a aquellos elementos que afecten la moral, como ser el apoyo de la población enemiga a sus fuerzas armadas y al poder político y esto conlleva la importancia de la correcta identificación de los centros de gravedad de la estrategia enemiga.

A estas características que se van trasladando desde las generaciones de la guerra anteriores, Lind (1989) agrega: (a) los avances tecnológicos como impulsores de cambios, (b) la participación en las operaciones de actores estatales y no estatales y (c) el manejo de la información y una mayor implicación de la población civil. (p. 22-26)

Todas estas características dirigen las guerras del Siglo XXI, a una ausencia de líneas de frente claras, llevando el combate a zonas grises y según Ceresoli (2019):

Las amenazas modernas exponen como factores de fuerza, la posibilidad de afectar distintos dominios de la estrategia nacional, valiéndose de actores u organizaciones sustitutas que actúan bajo la órbita de intereses del actor principal enfrentado. Esto implica que, para resolver un conflicto complejo moderno, el poder militar adquirirá un sentido mayormente

disuasorio mientras los restantes factores de poder de la estrategia nacional configuran el diseño de la maniobra estratégica.

Pulido (2021) definió como zona gris a:

Un área de conflicto en la que las líneas de autoridad y responsabilidad son poco claras, y en la que las fuerzas militares y civiles pueden tener dificultades para coordinar y colaborar de manera efectiva. La zona gris a menudo se refiere a áreas en las que los conflictos son difusos y no se ajustan a la típica dinámica de guerra entre estados-nación. En estas áreas, es común que las fuerzas militares operen junto con organizaciones civiles, como agencias humanitarias y organizaciones no gubernamentales, para abordar una variedad de problemas, desde el mantenimiento de la paz hasta la ayuda humanitaria. Además, identificó que la falta de claridad en las líneas de autoridad y responsabilidad en la zona gris puede llevar a situaciones en las que los militares y los civiles no estén seguros de quién tiene el control o de quién es responsable de tomar decisiones críticas. Esto puede llevar a confusiones y tensiones en la cooperación entre los diferentes actores, lo que a su vez puede dificultar la efectividad de las operaciones en la zona.

Las características del combate moderno analizadas hasta ahora han abierto un abanico de posibilidades de empleo para poder contrarrestar las diferentes variables planteadas. Dentro de ellas se han desarrollado los conceptos de operaciones multidominio y las operaciones multicapa.

El Estado Mayor Conjunto de las Fuerzas Armadas (EMCFFAA) (2023) define las operaciones multidominio como:

Operaciones militares concebidas por el nivel operacional donde las capacidades modulares pertenecientes a cualquiera de los dominios existentes convergen en cualquiera de los otros, creando un dilema al oponente y generando una ventana de oportunidad que permita obtener el punto decisivo. Son operaciones de alto tempo y alcance que,



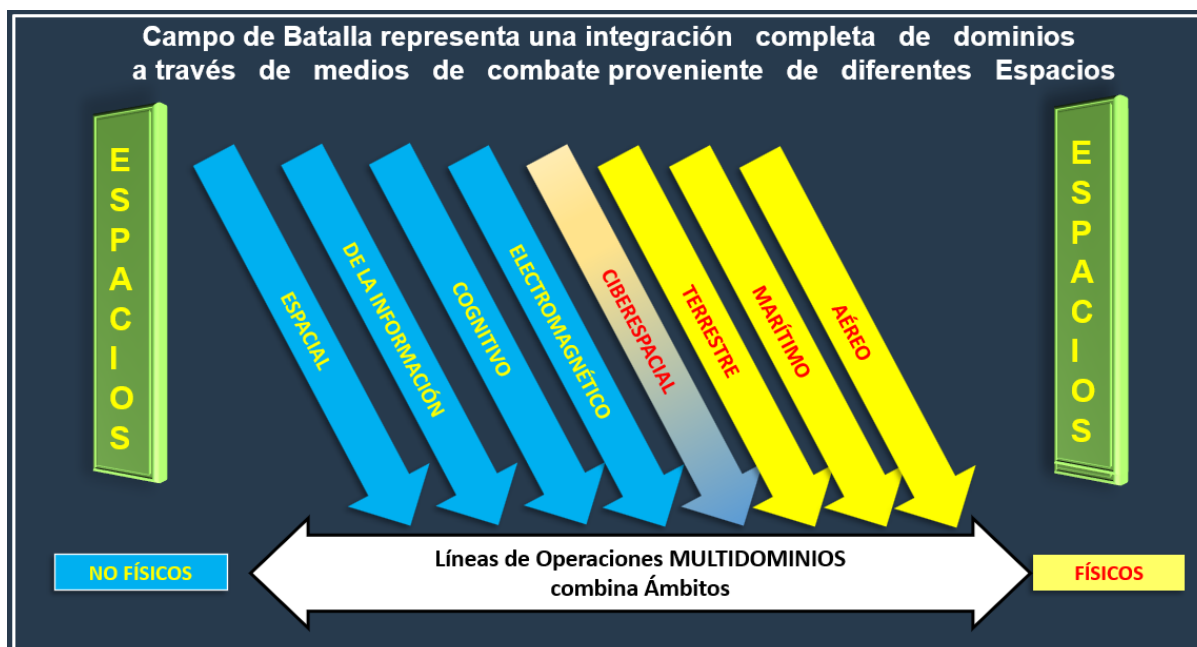
sincronizando sus efectos, permitan generar un dilema cognitivo al oponente que afecte su toma de decisiones (dislocamiento y parálisis) en un tiempo y momento dados, afectando así sus Vulnerabilidades Críticas. Las capacidades modulares pivotean y se reconstituyen en la medida en que el diseño de la Maniobra Operacional le permita al comandante mantener su iniciativa.

El conflicto entre Armenia y Azerbaiyán en la región de Nagorno-Karabaj en 2020 es considerado un ejemplo de guerra multidominio, debido a la complejidad de las operaciones militares que se llevaron a cabo en múltiples espacios. Algunas de las experiencias y lecciones aprendidas sobre la guerra multidominio en este conflicto según Pulido (2021) son:

- La importancia de la integración de las capacidades cibernéticas y de inteligencia artificial en la planificación y ejecución de las operaciones militares: durante el conflicto, se observó que ambos bandos utilizaron activamente la ciberdefensa y las capacidades de inteligencia artificial para monitorear y controlar la situación en el campo de batalla. También se utilizaron drones y vehículos autónomos que permitieron llevar a cabo tareas de reconocimiento y ataque.
- La necesidad de desarrollar capacidades de defensa multidominio: el conflicto demostró la importancia de contar con la capacidad de defenderse y atacar en múltiples dominios simultáneamente. Esto incluye la integración de capacidades en el dominio cibernético, espacial y de información con la defensa terrestre y aérea.
- La importancia de la coordinación y cooperación entre distintas ramas y servicios militares: se puso de manifiesto como un elemento fundamental en la planificación y ejecución efectiva de operaciones militares en múltiples dominios. La habilidad para integrar y coordinar las acciones en tierra, aire, mar, ciberespacio y la utilización de la inteligencia artificial se reveló como un factor crítico para alcanzar el éxito en el campo de batalla. (p. 63, 141, 171)

**Figura 1**

*Características distintivas de las Operaciones Multidominio.*



*Nota.* Adaptado de *Concepción Estratégica de Restricción de Área y Operaciones Multidominio*, de COFFAA, 2023.

Si el conflicto entre Armenia y Azerbaiyán destacó la importancia de la planificación, coordinación y ejecución de operaciones militares multidominio, y la necesidad de desarrollar capacidades y estrategias de defensa que tengan en cuenta múltiples dominios simultáneamente, la operación militar especial rusa en Ucrania demostró la necesidad del empleo de operaciones multidominio, involucrando aún más el factor social a la ecuación.

Algunos aspectos principales que el Comando Operacional de las Fuerzas Armadas (COFFAA) (2023) resaltó como conclusión de dicho conflicto son:

- La necesidad de contar con un sistema de comando, control y comunicaciones basados en la interconexión en red, entre sensores, centros integradores de inteligencia y targeting con medios de apoyo de fuego, que eleven el rendimiento de estos últimos en forma exponencial, empleando celulares, sistemas de

aeronaves no tripulados, satélites tanto civiles como militares, redes sociales o sistemas de adquisición de blancos tradicionales, aplicados a ciclos de aprobación cortos.

- El instrumento militar debe poseer capacidades modulares adaptables al entorno, mediante bloques, versátiles, encastrables y escalables, tipo mosaico.
- La movilidad, se ha convertido en la mejor medida de protección, ya que, a causa de los modernos sistemas de obtención de información, la supervivencia se basa en un combate en permanente movimiento.
- Organizar pivots defensivos, obligando al enemigo a combatir en núcleos poblacionales transformados en centros de resistencia o puntos de apoyo.
- Desarrollar la capacidad para ejecutar ataques convergentes desde la dispersión a modo de “enjambre”.
- Fortalecer la función de movilidad a través de unidades de ingenieros polivalentes con equipos modulares intercambiables, reforzados con empresas civiles.
- Contar con un sistema integrado de fuegos a nivel teatro de operaciones con la incorporación de expertos logísticos en targeting para determinar los blancos de alto valor logísticos.
- Desarrollar una robusta capacidad de ataque y defensa cibernética, en capacidad de atacar nodos de telecomunicaciones o energía eléctrica para generar apagones de conectividad, o bien manipular flujos de información, narrativas, imágenes y uso de inteligencia artificial para influir en la moral del enemigo. (p. 14-19)

Es importante destacar que, en la actualidad, el enfoque de la ciberdefensa en nuestras fuerzas armadas se centra en garantizar la seguridad de nuestras propias redes y sistemas, sin llevar a cabo ciberataques.

Ante esta nueva forma de desarrollar la guerra, en las FFAA Argentinas, el COFFAA (2023) desarrolló en su ciclo de planeamiento estratégico, la necesidad de plasmar un nuevo pensamiento militar y concepto estratégico operacional. Este enfoque se conoce como la Restricción de Área y se fundamenta en la implementación de dos herramientas esenciales: la Defensa por Capas a nivel estratégico militar y las Operaciones Multidominio a nivel estratégico operacional.

El EMCFFAA (2023), definió el concepto de restricción de área como: “un concepto de empleo que busca mediante, diversas acciones, anular o restringir la libertad de acción del agresor estatal militar externo (AEME) en una zona determinada, impidiendo su control efectivo.” De este mismo glosario, se desprende el concepto de Operaciones Multicapa, siendo estas: “operaciones Multidominio, que se ejecutan buscando negar el acceso al propio territorio, al oponente y en caso de no poder impedirlo, restringiendo sus posibilidades de acceder al propio centro de gravedad, intentando en todo momento afectarlo por medio de burbujas activas con la finalidad de lograr su punto culminante antes de que el acceda al propio.”

De acuerdo a lo que plantea el Ejército de Tierra de España (2019), podemos agregar que ante un enfrentamiento de alta intensidad contra un enemigo tecnológicamente avanzado, las características del combate se establecerán de acuerdo al adversario y su capacidad de (a) negar el acceso a zonas determinadas a través de guerra electrónica, defensa antiaérea y fuegos profundos y de precisión, (b) sus medios de observación y adquisición de blancos, sistemas de navegación y guiado de municiones, (c) potencia de combate igual o superior a la propia y (d) su capacidad de ciberguerra y de desarrollar operaciones de información. (p. 14)

La concepción estratégica militar de restricción de área según el COFFAA (2023), se divide en esfuerzos activos, a través de operaciones permanentes y/o periódicas y esfuerzos

reactivos, creando condiciones de dislocamiento o desgaste, para luego rechazar las amenazas.

Esto se basa en el empleo combinado de capas, las cuales son:

1. Anticipar: mediante operaciones permanentes de vigilancia y control de espacios aéreos.
2. Prevenir: con operaciones periódicas de despliegues estratégicos de disuasión por presencia.
3. Conjurar: accionar con el poder militar para desgastar al enemigo y obligarlo a llegar a su punto culminante
4. Repeler: una vez dislocado, obligarlo a retirarse o rendirse ante la amenaza de ser destruido.

Las dos primeras capas materializan el esfuerzo activo buscando la alerta temprana y profundidad estratégica, mientras que las dos restantes son esfuerzos reactivos a orden mediante la planificación y ejecución de operaciones militares.

El nivel operacional planificará y conducirá las operaciones, buscando sincronizar con velocidad relativa superior, efectos provenientes de ámbitos físicos y no físicos, en determinadas ventanas de oportunidad asociadas a vulnerabilidades críticas y disponibilidad de recursos para afectar centros de gravedad del agresor a través de puntos decisivos, conformando un ritmo de operaciones multidominio caracterizado por un enlace operacional que amalgama dichos activos en determinados momentos seleccionados.

Estos combates se manifiestan en tres líneas colaborativas e integradas, combinando los conceptos de mosaico, plataformas y enjambre. Estas líneas son:

1. Sensores (espaciales, guerra electrónica y ciberespacio).
2. Sistemas no tripulados.
3. Sistemas de armas tradicionales organizados modularmente.

Esta nueva forma de emplear el instrumento militar implica repensar el combate interarmas, y por ende su organización.

A nivel global, países como España, Rusia y China, entre otros, han comenzado a explorar la creación de organizaciones especializadas destinadas a abordar operaciones de restricción de área frente a la amenaza de una superpotencia o coaliciones de naturaleza similar.

Por nuestra parte, y teniendo en cuenta que las capacidades actuales permiten el dominio o supremacía temporal de ciertos espacios, las FFAA no cuentan con ningún elemento organizado, equipado e instruido para operar en todos los dominios y que permita cumplir con lo planificado en el nuevo ciclo de planeamiento estratégico.

Teniendo en cuenta lo establecido por el COFFAA en su planificación, debería crearse un elemento que (a) cuente con los medios necesarios, (b) sea autosuficiente, (c) tenga capacidades tecnológicas superiores, y (d) a partir de la dispersión pueda incidir en una ventana de oportunidad sobre el centro de gravedad (CDG) del enemigo, generando en él, su disloque.

Esta organización debe estar en capacidad de conducir elementos orgánicos o no, de apoyo de fuego de alta precisión, sistemas no tripulados (SNT), comando, control, comunicaciones, informática e inteligencia (C3I2) y ciberdefensa, bajo las características de una gran unidad de combate (GUC) o batalla (GUB), comando conjunto subordinado (CCS) o fuerza de tareas conjunta (FTC), debido a su necesidad de accionar en múltiples dominios simultáneamente. Esto demandará un alto grado de flexibilidad y profesionalismo.

## **Formulación del Problema**

¿Cómo diseñar unidades en el marco de una Brigada Multidominio que combinen capacidades de comando, control, comunicaciones, guerra electrónica, cibernéticas y de inteligencia?

## **Objetivos**

### ***Objetivo General***

Diseñar unidades en el marco de una Brigada Multidominio que combinen capacidades de comando, control, comunicaciones, guerra electrónica, cibernéticas y de inteligencia.

### ***Objetivos Específicos***

1. Explicar el concepto de empleo de una Brigada Multidominio para definir sus capacidades.
2. Analizar los procesos de trabajo de los sistemas de C4IG para integrarlos a operaciones multidominio.
3. Sintetizar las capacidades de C4IG multidominio para diseñar unidades en el marco de una Brigada Multidominio.

## **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, documental y lógico.

## **Capítulo 1**

### **Concepto de Empleo de la Brigada Multidominio.**

#### **Propósito del Capítulo**

Definir las capacidades con las que debe contar una Brigada Multidominio.

#### **Sección 1 Desarrollos y Experimentaciones**

En el contexto de las operaciones multidominio, el concepto de empleo tradicional de las fuerzas armadas ha evolucionado hacia un concepto de empleo más amplio y sofisticado que se ha forjado a través de una serie de desarrollos y experimentaciones que han demostrado ser cruciales para el éxito en el campo de batalla moderno.

Teniendo en cuenta las capacidades tecnológicas y las características particulares de los diferentes ambientes operacionales en los que prevén combatir, varios países han desarrollado estudios e iniciado etapas de desarrollo y prueba de diferentes organizaciones que satisfagan la necesidad de operar en todos los dominios.

Como principales referentes, y de acuerdo con la información disponible, podemos identificar a los EEUU, España, Israel o Rusia, de los cuales, de acuerdo con Baez (2022), el único que ha empleado una fuerza multidominio en combate ha sido Rusia con sus fuerzas de tarea de nivel batallón o *Battle Tactical Group* (BTG) por sus siglas en inglés.



## ***EEUU***

De acuerdo al Jefe del Estado Mayor del Ejército de los EEUU (2021), el Ejército de los Estados Unidos ha iniciado el desarrollo de brigadas multidominio bajo el objetivo de adaptar a toda su fuerza para el año 2035, con la finalidad de operar de forma conjunta mediante apoyo de fuego de largo alcance, sostenimiento, protección y fuerzas en capacidad de penetrar y maniobrar a través de las defensas enemigas.

Estas fuerzas cuentan con capacidades de C4IG, respaldadas por inteligencia artificial y sistemas de almacenamiento en la nube. Lo más destacado, es la implementación de una doctrina estandarizada que les permite operar de manera integrada en todos los ámbitos y niveles de la conducción. Esto, a su vez, facilita y agiliza el proceso de toma de decisiones, permitiéndoles anticiparse al ciclo de observación, orientación, decisión y acción (OODA) del enemigo.

## ***España***

El Ejército de Tierra de España (2019) presentó la *Brigada 35* como la pionera dentro de su Ejército. Esta Brigada está orientada a la modularidad de sus medios (8x8), a un salto en capacidad tecnológica en apoyo al comando y control (C2) y a un concepto de descentralización de las operaciones lo que otorgaría velocidad e iniciativa en todos los niveles.

Esta modularidad plasmada en la estandarización de plataformas o medios, con el apoyo de inteligencia artificial para el análisis de información y nuevas tecnologías principalmente orientadas a las comunicaciones y obtención de información, le permitirá operar en todos los dominios.

## ***Israel***

Lappin (2020) publicó la información sobre la creación de una nueva unidad experimental multidominio denominada *Unidad 888 “Refaim”* de la Fuerza de Defensa Israelí (IDF) con características algo diferentes a las expuestas por EEUU y España.

La IDF busca influir en todos los dominios mediante la formación de esta fuerza compuesta por elementos de élite provenientes de diversas especialidades, que incluyen exploración, blindados, paracaidistas, comandos, ingenieros, comunicaciones, ciberguerra e inteligencia entre otros. Incluso se incorporan miembros de la Fuerza Aérea Israelí. Esta integración de personal y recursos, respaldada por tecnología avanzada, permite mejorar significativamente la interoperabilidad y, agiliza la identificación rápida de objetivos y blancos, así como su neutralización.

## ***Rusia***

Según Baez (2022), durante la guerra entre Rusia y Ucrania, el Ejército de la Federación Rusa desplegó sus BTG a través de los cuales se buscó otorgar libertad de acción a los elementos en el terreno para lograr de forma rápida los objetivos impuestos.

Teniendo en cuenta lo establecido por Galeotti (2019) los BTG son elementos de nivel Fuerza de Tarea o Brigada disminuida integrada por elementos de todas las armas, buscando la capacidad de afectar la mayor cantidad de dominios posibles. Con el transcurso de las operaciones estas capacidades se fueron ampliando de acuerdo con la necesidad de los elementos, como por ejemplo con ciberguerra o aeronaves no tripuladas, esto a través de una correcta interoperabilidad de sus medios.

## **Sección 2 Concepto de Empleo de un Elemento Multidominio**

La piedra angular de este enfoque multidominio, según estos países, es la combinación de medios altamente flexibles, modulares e interoperables de variadas formas. Estos medios comprenden una amplia gama de capacidades, desde fuerzas terrestres y navales hasta capacidades aéreas y cibernéticas. La flexibilidad y modularidad de estos recursos permiten una adaptación rápida y efectiva a las cambiantes condiciones del campo de batalla, lo que a su vez aumenta la versatilidad de las fuerzas militares.

Sin embargo, la mera presencia de medios diversos no es suficiente. La capacidad de detectar y destruir las fuerzas del adversario se ha vuelto esencial, y las tecnologías de vanguardia desempeñan un papel fundamental en este aspecto. Los sistemas avanzados de sensores, el reconocimiento de imágenes, la inteligencia artificial y la guerra cibernética se han convertido en pilares centrales en la ejecución de estas operaciones.

Uno de los aspectos que integra este enfoque multidominio es la utilización de elementos menores y ataques de largo alcance. Estas capacidades permiten a las fuerzas militares desestabilizar al adversario, generando dilemas constantes, antes de lanzar un ataque frontal con sus fuerzas principales. Esta estrategia puede incluir operaciones especiales, ataques de misiles de largo alcance y operaciones de ataque cibernético, todas diseñadas para minar la capacidad del adversario para resistir.

Finalmente, es importante destacar que, a pesar de la diversidad de personal, recursos y tecnologías que hacen posible las operaciones multidominio, el éxito de estas operaciones depende en gran medida de un sostenimiento logístico adecuado que se adapte a las misiones y a los recursos disponibles. Según Baez (2022), esta es una de las principales debilidades de los BTG. La logística en este tipo de operaciones no se limita únicamente al suministro y transporte de personal, recursos e información, sino que también incluye aspectos como la

reducción de firma térmica y electrónica, la dispersión de medios, la rapidez y la precisión. Esto permite liberar a las unidades de las servidumbres logísticas y les otorga una mayor libertad de acción en el campo de combate.

### **Conclusiones Parciales**

A partir de esta comparación entre diversos desarrollos y experimentaciones en el ámbito multidominio, podemos inferir que su concepto de empleo se basará en una combinación de recursos flexibles, modulares e interoperables de diversa índole. Estos medios estarán respaldados por tecnología avanzada que permitirá la detección y neutralización de las fuerzas adversarias mediante elementos de menor envergadura y fuegos cinéticos y no cinéticos de largo alcance muy precisos, con el objetivo de desestabilizar al adversario.

De lo anterior podemos definir capacidades comunes con las cuales se busca dotar a una Brigada Multidominio que va a operar en varios dominios o en todos ellos. Estas capacidades son:

1. Modularidad a través de plataformas comunes facilitando la adaptación de medios y recursos, reduciendo a su vez la servidumbre logística.
2. Interoperabilidad mediante la estandarización de doctrinas, procedimientos y principalmente la integración orgánica de elementos de diferentes características, específicos, conjuntos o combinados.
3. Tecnología como factor fundamental debe otorgar:
  - a. Facilitar la obtención de información en tiempo real mediante sensores o sistemas como ser SNT.
  - b. Comunicaciones y transmisión de la información obtenida mediante enlaces satelitales propios y seguros.

- c. Procesamiento de la información de forma ágil mediante sistemas de inteligencia artificial.
  - d. La capacidad de integrar en todos los niveles la información disponible a través de nubes o sistemas similares.
  - e. Alcance y precisión en los diferentes sistemas de armas para facilitar la maniobra de los elementos en tierra.
4. Rapidez en la transmisión de información que permita tomar decisiones de forma ágil y rápida en todos los niveles.
  5. Sistema logístico por nodos que reduzca la cantidad de personal logístico y agilice la distribución otorgando mayor libertad de acción a los elementos.

## **Capítulo 2**

### **Sistemas de C4IG Multidominio.**

#### **Propósito del Capítulo**

Integrar los sistemas de C4IG a las operaciones multidominio.

#### **Sección 1 Herramientas para el C4IG Multidominio**

Las operaciones multidominio, son operaciones ejecutadas en el nivel táctico a través de la sincronización de diferentes efectos en diferentes dominios para el logro del objetivo. Esto es planificado y sincronizado por el nivel operacional, quien es el que identifica la vulnerabilidad crítica del enemigo en una ventana de oportunidad. Esto es posible a través de una coordinada y rápida transmisión de información en tiempo real desde los menores niveles al comando del teatro de operaciones, lo que permitirá procesar la información de forma ágil y en el menor tiempo posible buscando tomar las decisiones correctas y transmitir las órdenes con la misma velocidad hacia quienes las ejecutarán.

Si bien la concepción de empleo de las fuerzas no varía del desarrollo de cualquier otra operación, el factor que influye como ya se ha tratado en esta investigación, es la tecnología.

La tecnología ha permitido perfeccionar las funciones de combate en todos los niveles dotando a las fuerzas de mayor alcance, precisión, movilidad, rapidez y letalidad, y a su vez agilizar las funciones de combate, principalmente las de comando y control e inteligencia.

Estas últimas se ven potenciadas por la aplicación de cinco avances tecnológicos: los avances en la comunicación, los satélites, la inteligencia artificial, los servicios de nube, y la transmisión de la información en tiempo real, ya que tanto el acceso a la información como su proceso, son factores fundamentales para el desarrollo de una operación multidominio.

### ***Los Avances en las Comunicaciones***

El avance tecnológico en las comunicaciones otorga a los elementos que planifiquen y ejecuten operaciones multidominio la capacidad de transmisión de información, coordinación de acciones y toma de decisiones más rápidas y de forma más segura.

Estos avances son:

- El crecimiento de internet como fuente de obtención, almacenamiento y transmisión de información.
- Las redes de comunicaciones fijas y móviles de alta velocidad como ser la fibra óptica o la red 5G las cuales permiten la transmisión de datos de forma confiable y rápida entre los diferentes elementos.
- El desarrollo de equipos de comunicaciones militares más versátiles y seguros que otorgan interoperabilidad con otros sistemas de comunicaciones civiles y militares, que transmitan su identificación y posicionamiento, y permiten la conexión de dispositivos como ser tabletas, notebooks, etc a la red de comando y control.

- Otros avances relacionados son el satélite y la transmisión en tiempo real que serán desarrollados más adelante.

Si bien estos avances son necesarios para poder ejercer el comando y control, también tienen sus desventajas, siendo las principales el costo de adquisición y desarrollo, como también la vulnerabilidad de los sistemas de comunicaciones dada su apertura.

La seguridad informática y de las comunicaciones se vuelve esencial, ya que de ella depende la salvaguarda de información sensible, la protección de sistemas de armamento y la continuidad de las operaciones. Con el objetivo de garantizar la protección adecuada de diversas redes, se han realizado avances significativos en ciberseguridad, contramedidas electrónicas y sistemas de encriptado tanto en equipos civiles como militares. Estos desarrollos son fundamentales para enfrentar las crecientes amenazas cibernéticas y asegurar la integridad y confidencialidad de la información crítica.

### *El Satélite*

El desarrollo de los sistemas y tecnologías satelitales ha expandido las capacidades militares en lo que respecta a las comunicaciones, sistemas de posicionamiento global e inteligencia geoespacial.

Los satélites permiten una comunicación rápida y segura entre fuerzas militares desplegadas en diferentes ubicaciones geográficas facilitando la transmisión de datos, voz y video y mejorando la coordinación y la toma de decisiones en tiempo real, ya que no presenta la limitación de infraestructura fija o en las características del terreno como lo son otros sistemas.

Los sistemas de posicionamiento global facilitan no sólo la navegación desde el punto de vista táctico, sino también el conocimiento de la posición en tiempo real de todos los elementos desplegados en el teatro de operaciones, propios y del enemigo. Factor

fundamental para la planificación y conducción de las operaciones, optimizando recursos, favoreciendo al desarrollo de la conciencia situacional y a evitar fratricidio.

La inteligencia geoespacial a través de los satélites de observación militares o civiles proporcionan información detallada sobre el terreno, condiciones meteorológicas y actividades enemigas, monitoreando de forma continua áreas críticas y así facilitando la identificación de posibles amenazas u oportunidades proporcionando inteligencia en tiempo real.

Si bien los satélites como herramientas permiten establecer redes de comunicaciones entre los diferentes dominios facilitando la coordinación y el control de las operaciones de forma sincronizada y eficaz en todo tipo de terreno, la obtención de información y permitiendo la navegación y ubicación de fuerzas de forma sencilla y precisa, también tiene sus serias vulnerabilidades como ser:

- La guerra espacial a través de sabotajes o destrucción por medio de armas antisatélite.
- Limitaciones meteorológicas adversas pueden afectar la eficacia de los satélites, especialmente en lo que hace a operaciones de observación y reconocimiento.
- La detección e interferencia de las funciones del satélite a través de ciberataques o interferidores.
- Costo elevado de desarrollo, lanzamiento y mantenimiento que, si bien nuestro país ya se cuenta con una alta capacidad de desarrollo, aún dependemos de terceros para el lanzamiento, lo que nos hace más sensible al sabotaje o espionaje.
- Por último, puede generar dependencia tecnológica y volverse un problema grave en caso de interrupciones, fallas técnicas o ataques.



## ***Inteligencia Artificial***

Si bien estos avances son muy beneficiosos al momento de la obtención de información, también generan un problema que es el de la sobreinformación y la dificultad de un estado mayor o un elemento de inteligencia de procesarla en el tiempo necesario para la correcta toma de decisiones. Por esta razón, la inteligencia artificial desempeña un papel importante como herramienta contribuyente en este tipo de operaciones.

La inteligencia artificial, de acuerdo con el nivel de desarrollo que se disponga, permite analizar grandes cantidades de información en segundos, filtrando al usuario la información necesaria de acuerdo con la configuración que éste disponga. Esta puede detectar elementos del enemigo, su identificación, equipamiento y ubicación exacta al entrecruzar diferentes imágenes almacenadas en redes sociales, situación que ya se vio plasmada en la guerra entre Rusia y Ucrania en más de una oportunidad, permitiendo a una célula de targeting emplear acertadamente los medios y neutralizar un adversario. Esto se logra a través de los siguientes procesos:

- Recopilación de datos de texto o voz vinculado a palabras clave que resulten de interés. Esto puede incluir mensajes de texto, voz, llamadas o transmisiones, correos electrónicos, documentos, etc.
- Procesamiento de datos eliminando ruido de acuerdo con las características especiales que se necesiten.
- Análisis de sentimientos para determinar el tono de las comunicaciones y así extraer características de los usuarios de esa red.
- Construcción de modelos de red que representen las interacciones entre los diferentes nodos de comunicaciones del adversario.
- Análisis de imágenes y video para la identificación de blancos o modificaciones producidas en el terreno.

Esta herramienta no sólo nos permite el análisis de la información, sino que también, gracias a la predicción, puede acotar un proceso de planeamiento de comando de días u horas a segundos o minutos, presentando al comandante o al jefe del área correspondiente, diversos modos de acción orientados en la personalidad del comandante gracias al aprendizaje autónomo o machine learning. Un ejemplo de uso habitual de la inteligencia artificial en este proceso es mediante la aplicación de Googlemaps, la cual analiza toda la situación (origen, destino, tránsito, tiempos, cortes, obras, etc) y genera el mejor modo de acción de acuerdo con la configuración que desee el usuario.

### ***Servicios de Nubes Digitales***

Estos servicios permiten recopilar y almacenar toda la información suministrada por los medios de obtención, la información básica disponible y la inteligencia generada en base a la misma y con el adecuado permiso de acceso, esta se encuentra a disposición de todos los niveles de la conducción, agilizando de esa manera su diseminación, análisis y con ello la toma de decisiones.

El principal beneficio de esta herramienta son los servicios de colaboración. Esto otorga la capacidad de compartir información en tiempo real con todos los elementos que puedan necesitarla desde diferentes ubicaciones, como también herramientas digitales y bases de datos.

McChrystal, Collins, Silverman y Fussell (2015) destacaron, en el contexto de las operaciones en Afganistán, la importancia de contar con información completa en todos los niveles. Esto permitiría vincular datos aparentemente dispersos e insignificantes para generar la inteligencia necesaria e identificar vulnerabilidades críticas del adversario. Este mismo concepto es el que se persigue en las operaciones multidominio en relación con el C4IG a través del empleo de estos servicios de nube.

Como toda herramienta virtual, los riegos en lo que respecta a seguridad y privacidad, dependencia de la conectividad y la latencia, son altos y requieren una gran estructura física de servidores, un desarrollo de software importante y una alta capacitación del personal que va a operar y controlar el sistema.

### ***Transmisión en Tiempo Real***

Si bien no es una herramienta obligatoria para la conducción, teniendo en cuenta la necesidad de rapidez en la toma de decisiones, asignación de medios e impartición de órdenes, todo basado en la inteligencia disponible para aprovechar las ventanas de oportunidad, la transmisión de información en tiempo real agiliza el proceso favoreciendo al cumplimiento de la misión.

La transmisión en tiempo se materializa en sistemas o tableros de comando y control como lo es el Sistema Integrado Táctico de Comando y Control del Ejército Argentino (SITEA). Estas plataformas de integración recaban la información de los sensores, dispositivos e inteligencia artificial que recopilan datos en tiempo real desde diferentes dominios. Esto se logra mediante la implementación de los sistemas de comunicaciones seguros y eficientes que permiten la transmisión instantánea de datos entre los diferentes niveles que se almacenan en la nube facilitando el almacenamiento y rápido acceso a los datos compartidos.

De esta forma, en los diferentes niveles se accede a la información integrada y en tiempo real permitiendo:

- Una coordinación más rápida y efectiva entre diferentes dominios, ya que la información se comparte instantáneamente.
- La toma de decisiones en tiempo real al proporcionar datos actualizados y relevantes para la operación.

- Una visión más completa de la situación que ayuda a comprender mejor el panorama general en todos los niveles.
- Una asignación más eficiente de recursos en base a la disponibilidad y demanda en las diferentes áreas, tanto de recursos como de elementos de combate, apoyo de fuego o logísticos.
- Una mejor capacidad de respuesta a través de una respuesta rápida y coordinada a eventos imprevistos o cambios en las condiciones de las operaciones.

Si bien presenta muchos beneficios, al igual que el resto de las herramientas, también presenta desventajas:

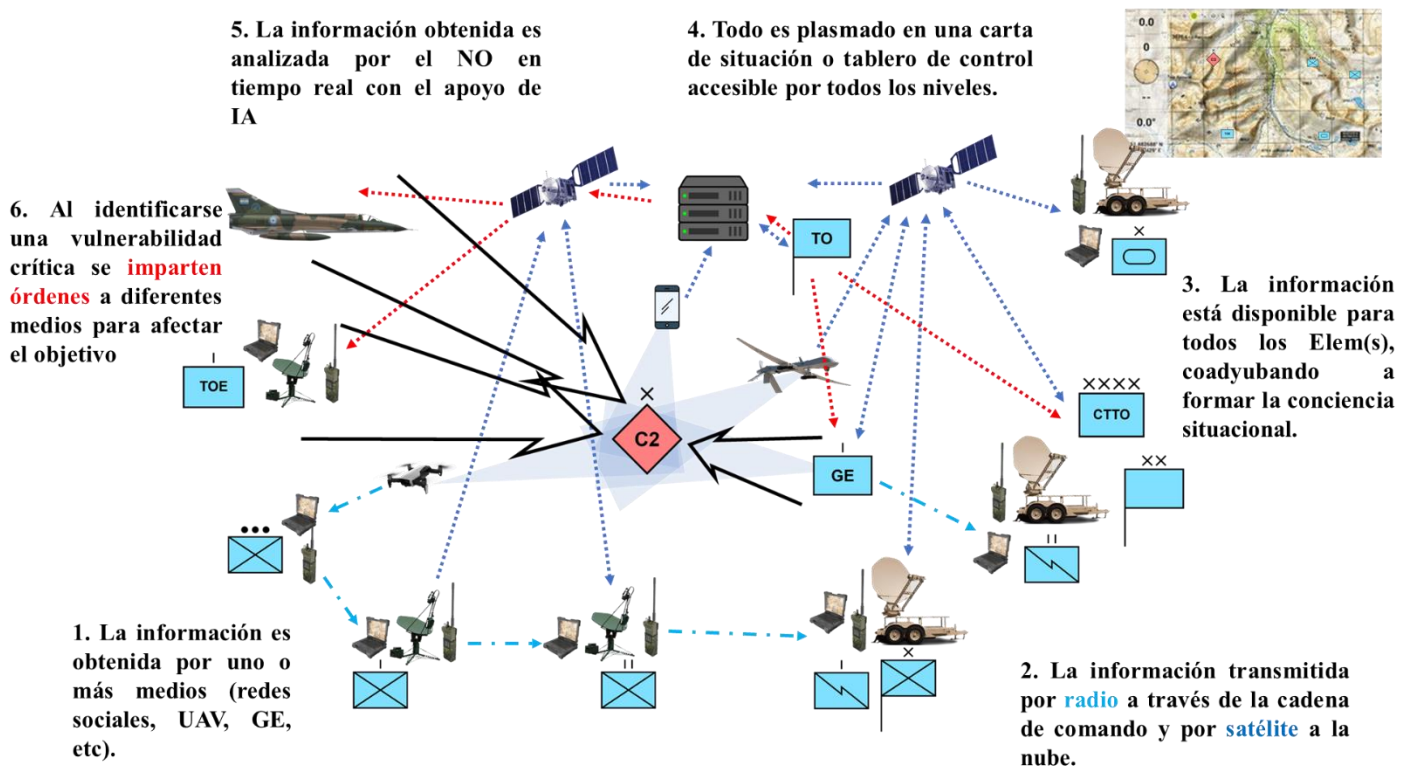
- Seguridad interna y externa: la transmisión en tiempo real puede aumentar los riesgos de seguridad, ya que la información sensible está más expuesta a posibles amenazas externas y vulnerabilidades internas.
- Complejidad técnica y costos elevados: la implementación de estos sistemas es técnicamente compleja, especialmente al integrar diferentes tecnologías y plataformas, derivando también en costos elevados.
- Plataformas interoperables: la sincronización de datos entre diferentes dominios puede ser un desafío especialmente si los sistemas operan en plataformas tecnológicas distintas, exigiendo que todas las fuerzas y niveles empleen el mismo sistema.

## **Sección 2 Integración de los Sistemas C4IG a las operaciones multidominio**

Teniendo en cuenta que, si bien las operaciones son planificadas y conducidas por el nivel operacional, su ejecución es táctica, ergo, todos los niveles de la conducción desde las menores fracciones deben estar interconectados a través de estas herramientas identificadas en la sección anterior.

Drones de reconocimiento y ataque, equipos de radio y satelitales portátiles que transmitan imágenes y video de forma segura y sistemas de ciberdefensa que permitan proteger sistemas de comunicaciones serán necesarios en todos los niveles y dependiendo el mismo, el alcance, potencia y capacidades necesarias de cada equipo, ver Apéndice A. En la Figura 2 se puede apreciar como cada nivel debe estar interconectado a través de diferentes medios de obtención, análisis y comunicación de la información para la identificación, análisis, impartición de órdenes y afectación de un blanco.

Figura 2



*Concepto de empleo del sistema de C4IG multidominio.*

## Conclusiones Parciales

Para integrar los sistemas de C4IG para el desarrollo de operaciones multidominio es necesario:

1. Que todos los niveles de la conducción estén interrelacionados a través de un sistema de C4IG ágil y seguro para transmitir la información disponible en tiempo real.
2. Esta información debe estar accesible a la mayor cantidad de elementos posible para aumentar la conciencia situacional de todos los presentes en el teatro de operaciones.

3. La tecnología a través de la conectividad, los satélites, la inteligencia artificial e internet son necesarios para la recepción, procesamiento, almacenamiento y diseminación de la información u órdenes en todos los niveles.
4. La seguridad y privacidad en el acceso a la información compartida requiere de elementos de ciberdefensa que operen y controlen de acuerdo con la magnitud de la información a emplear.

Si se posee un nivel operacional altamente tecnológico, ágil y moderno, poca utilidad va a tener si las fracciones que deben obtener la información o ejecutar las misiones decisivas no cuentan con los medios necesarios para transmitir información, recibir órdenes y ejecutarlas con la precisión y velocidad necesarias.

## Capítulo 3

### Diseño de la Brigada Multidominio

#### Propósito del Capítulo

Sintetizar las capacidades de C4IG multidominio para diseñar unidades en el marco de una Brigada Multidominio.

#### Sección 1 Diseño de la Red de C4IG de la Brigada Multidominio

De lo analizado hasta este capítulo podemos identificar que las diferentes grandes unidades de combate o batalla deben estar interconectadas desde sus menores niveles, con los otros componentes, con el estado mayor y elementos dependientes del nivel operacional.

Actualmente, en un sistema de comando y control, el flujo de información es gestionado por los elementos del arma de comunicaciones a través de sus sistemas de comunicación particulares integrados a los diferentes sistemas de comunicaciones del Ejército y de allí a las diferentes fuerzas armadas. Si bien es un sistema que funciona, el flujo de la información es relativamente lento para lo que se requiere en las operaciones multidominio.

El C4IG de la Brigada Multidominio debe estar compuesto por una combinación de medios y sistemas que permitan la transmisión de información rápida en todas direcciones y el acceso a toda la información disponible de acuerdo con el nivel de la conducción, como se aprecia en la Figura 2 del capítulo 2.

A continuación, se analiza cada parte componente del sistema de C4IG:

- Comando y control: se requiere un tablero de control que permita plasmar, de acuerdo con el elemento, la información necesaria para la toma de decisiones



pudiendo personalizarse de acuerdo con las necesidades operacionales. Por ejemplo: el comandante de la Brigada Multidominio podrá visualizar la situación de su fuerza y lo relacionado a otras adyacentes y superiores, como también diferentes factores del ambiente operacional necesarios para su operación.

- Comunicaciones: las diferentes redes de comunicaciones apoyado en medios satelitales (portátiles o remolcados), fijos, civiles y militares y radioeléctricos que permitan la transmisión de información digital, deben integrarse otorgando seguridad, confiabilidad y flexibilidad.
- Ciberdefensa: la defensa de los puestos comando de todos los niveles será necesaria y obligatoria, teniendo en cuenta las capacidades de ciberataque que se van desarrollando a nivel mundial. La protección cibernética no puede ser pensada y ejecutada sólo a nivel operacional o nivel componente. Cada elemento que posee acceso al sistema de comando y control debe poseer medios o sistemas (no solo medidas de seguridad) y el personal especializado para supervisarlos que lo protejan de diferentes ataques cibernéticos.
- Inteligencia y Guerra Electrónica: teniendo en cuenta que todos los elementos dentro y fuera del teatro de operaciones, civiles y militares, son fuentes y medios de obtención, es necesario poder acceder a la información que estos producen. Para ello, son fundamentales la inteligencia, la ciberdefensa, la guerra electrónica y los medios de obtención de largo alcance no tripulados. Todos estos elementos y medios deben entenderse como que tienen un doble propósito, el propio y el de completar el cuadro de situación del escalón superior, subalterno o adyacente según corresponda.

## **Sección 2 Diseño de los Elementos para Integrar las Capacidades C4IG a la Brigada Multidominio**

Las características de nuestro territorio no facilitan la conformación de elementos multidominio permanentes, por ende, hay que pensar en capacidades modulares basadas en relaciones funcionales y de comando. El Ejército Argentino (2017) para una situación similar plantea un esquema de organización por módulos como lo es el de la Fuerza de Despliegue Rápido, con un módulo orgánico y módulos variables asignados y de refuerzo, método que adoptará la Brigada Multidominio para su organización.

### **Módulo Orgánico.**

El módulo orgánico estará compuesto por los elementos que le dependan según la naturaleza del elemento. Teniendo en cuenta lo analizado durante esta investigación, se deberían incorporar de forma orgánica:

- De acuerdo al elemento o nivel, núcleos de instrucción o comandos de planeamiento temporales de forma permanente para facilitar la instrucción, planeamiento, adiestramiento y conocimiento de las funciones, capacidades y limitaciones de cada sistema.
- Tropas de operaciones especiales que facilitan la adaptación y participación en operaciones multidominio gracias a su flexibilidad, versatilidad y elevado grado de instrucción.
- Elementos de ciberdefensa para el nivel gran unidad de combate y de batalla.
- Elementos de aeronaves no tripuladas en todos los niveles de la conducción cuyas características estarán con relación al mismo.

**Módulo Interagencial.**

Contendrá todos los elementos que le son asignados de forma temporal para el cumplimiento de una misión particular (medios civiles, agencias, de otras fuerzas de seguridad propias o de otros países). Va a variar de acuerdo con la exigencia que se posea, y es por lo que es importante la presencia de forma permanente de como mínimo enlaces en los diferentes elementos o estados mayores, para acostumbrar a la organización a trabajar de forma conjunta combinada e interagencial.

La asignación de medios en base a este módulo va a depender completamente de la interoperabilidad de los elementos o fuerzas asignadas.

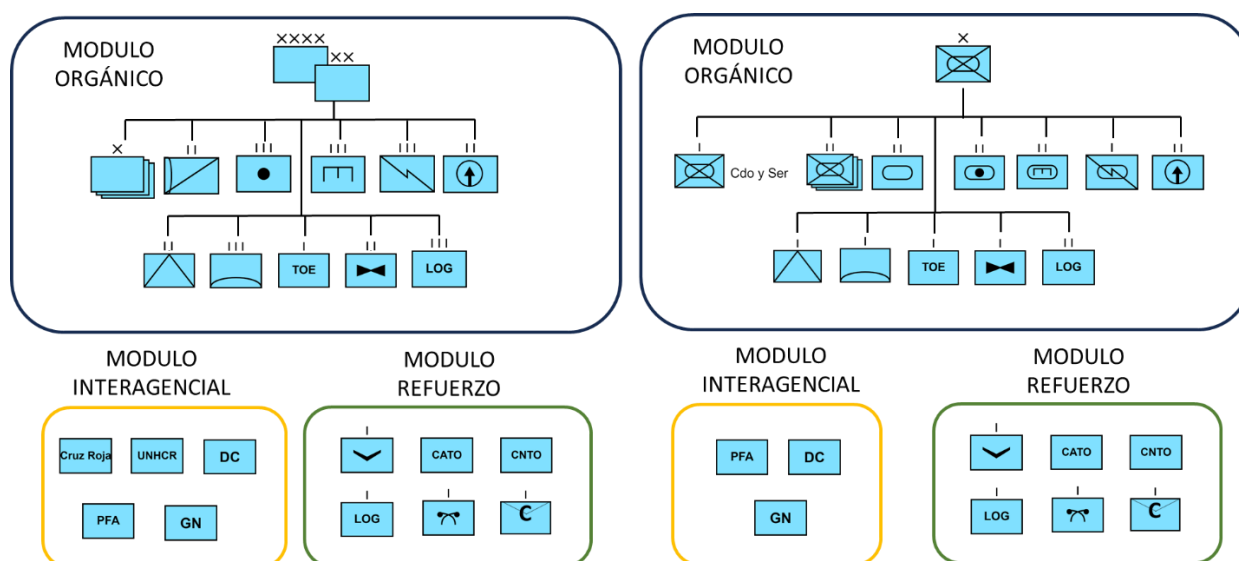
**Módulo Refuerzo.**

Serán todos los elementos básicos de combate, de apoyo de fuego, de apoyo de combate, tropas técnicas y de los servicios de apoyo para el combate que refuercen al elemento y que otorguen nuevas capacidades específicas para solucionar un problema particular de forma urgente o por un plazo breve y que signifiquen multiplicadores del poder de combate, lo cual amplía su capacidad de letalidad.

En la Figura 3 se puede apreciar una posible organización de un Componente Terrestre o GUB y una GUC, incorporando los elementos previamente desarrollados al módulo orgánico.

**Figura 3**

*Organización por módulos.*



*Nota.* Los elementos de los módulos interagencial y de refuerzo varían de acuerdo con las capacidades que necesite ese elemento para cumplir con la misión impuesta. El desglose esquemático de los elementos se encuentra en el Apéndice B.

### Conclusiones Parciales

Para que un elemento ejecute o participe de operaciones multidominio requiere de una capacidad tecnológica que le permita compartir y recibir información en tiempo real de forma rápida y segura, generándose un cuadro de situación en todos los niveles que facilite la toma de decisiones rápida para sincronizar los efectos necesarios, y así afectar las vulnerabilidades críticas del adversario logrando dislocar su centro de gravedad.

El otro factor necesario para un elemento multidominio es la capacidad modular y de interoperabilidad real, no solo a través de medios técnicos o doctrina unificada, sino mediante un alto grado de alistamiento y profesionalismo de sus integrantes, acostumbrados a operar de forma conjunta o combinada.

Basándonos en estos elementos, podemos concluir que los componentes que conformen una Brigada Multidominio deben estar completamente integrados en un sistema

de Comando, Control, Comunicaciones, Computación, Inteligencia y Guerra Electrónica (C4IG) que sea integral y abarque todos los niveles de comando. El cumplimiento de criterios esenciales como modularidad e interoperabilidad será fundamental para que la brigada pueda adaptarse con rapidez y eficacia a la ejecución de operaciones multidominio. Estos principios aseguran una respuesta ágil y coordinada ante las complejidades y dinámicas de los escenarios de combate actuales.

## Conclusiones

### Conclusiones Finales

A lo largo de este trabajo final integrador, se analizaron las diferentes características, herramientas y necesidades para el C4IG de un elemento que ejecute operaciones multidominio. De ello podemos concluir en:

- La modularidad como criterio organizacional es indispensable al momento de organizar un elemento para el cumplimiento de una misión en múltiples dominios. Esto se debe dar principalmente en lo que respecta a las comunicaciones y a los sistemas o plataformas de comando y control para facilitar, la transmisión de información y órdenes, la coordinación de acciones y sincronización de efectos.
- Todos los elementos dentro del teatro de operaciones deben estar interconectados entre sí gracias a una multiplicidad de medios de comunicaciones seguros como ser sistemas de comunicaciones de campaña con medios radioeléctricos y satelitales o sistemas subsidiarios o guarnicionales mediante telecomunicaciones o redes de fibra óptica. Todo elemento debe estar en condiciones de poder comunicarse de forma ágil y segura con otro, sin distinción del nivel, ya sea dependiente del mismo componente o no.
- La información e inteligencia compartida en tiempo real dará la ventaja por sobre el ciclo de toma de decisiones del adversario, al permitir visualizar la situación exacta de cada elemento propio o del enemigo, optimizando recursos y medios como así también facilitando la toma de decisiones. Esto logrado a través de sistemas de nube y transmisión en tiempo real.

- El desarrollo de tecnología relacionada al comando y control, su incorporación a los sistemas y su operación permitirá lograr la capacidad de contar con un sistema C4IG integrado, eficiente y seguro al ser de elaboración nacional.

La integración de sistemas, su modularidad, empleo y desarrollo se basarán en el principal factor a desarrollar para lograr una capacidad real de operar en múltiples espacios, este factor es un cambio de mentalidad.

Este cambio de mentalidad debe permitir ampliar la perspectiva de la situación que vive cada elemento que integra el teatro de operaciones para que estos interpreten correctamente que sólo son parte de un sistema mayor y que sus medios pueden quedar a disposición del comandante del teatro de operaciones si este los necesitara.

También esta nueva mentalidad debe orientar una interoperabilidad específica, conjunta y combinada real, no quedando en demostraciones o ejercicios esporádicos sino en relaciones de comando permanentes de acuerdo con cada nivel fomentando el profesionalismo y un alto grado de alistamiento.

### **Aporte Profesional del Autor**

La capacidad de la BMD de participar en operaciones multidominio no debe ser considerada una aptitud especial sino el incremento de capacidades a una OPC de forma permanente y a través de refuerzos modulares, buscando a futuro un cambio doctrinario y organizacional a aplicar a la masa de los elementos de las fuerzas armadas.

Dadas las características particulares de nuestro territorio y la distribución de nuestras fuerzas, es imperativo incorporar tecnologías que favorezcan la integración, interoperabilidad y versatilidad. Esto se hace necesario para estar preparados y capacitados para repeler cualquier amenaza estatal militar externa. Por esta razón, se propone la utilización de las cinco herramientas tecnológicas en combinación con organizaciones modulares, flexibles y

altamente profesionales. Este enfoque permitirá lograr un ciclo de toma de decisiones ágil, basado en la disponibilidad de información y la eficiente transmisión de órdenes.

Esta investigación ofrece las bases para la futura estructuración de los diferentes elementos de nivel GUC y eventual GUB del Ejército Argentino a través de su sistema de C4IG orientado a la ejecución de operaciones multidominio.



## Bibliografía

- Báez, G. (2022). *A primera vista: Grupos tácticos de batallón blindado mecanizado rusos en la guerra de Ucrania*. *Armor, the Professional Bulletin of the Armor Branch*, PB 17-22-3.
- Ceresoli, J. C. (2019). *Influencia del Ambiente Operacional para el planeamiento operacional en las Operaciones de Multidominio*. [Trabajo Final de Especialización]. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Buenos Aires.
- COFFAA (2023). *Concepción Estratégica de Restricción de Área y Operaciones Multidominio*. Boletín Informativo Conjunto. Buenos Aires.
- EMCFFAA (2023). *PC 00-02 Glosario de términos de empleo militar para la acción militar conjunta – Proyecto*.
- Ejército Argentino (2017). *ROD 80-01 Fuerza de Despliegue Rápido*.
- Ejército de Tierra de España (2019). *Fuerza 35*.
- Jefe del Estado Mayor del Ejército de los EEUU (2021). *Transformación a un ejército multidominio*.
- Grana, Lamb y O'Donoghue (2021). *Findings on Mosaic Warfare from a Colonel Blotto Game*. Rand. pp. 1-3.
- Lappin, Y. (20 de octubre de 2020). *A look into the IDF's mysterious new elite unit that could revolutionize the battlefield*. JNS. <https://www.jns.org/a-look-into-the-idfs-mysterious-new-elite-unit-that-could-revolutionize-the-battlefield/>
- Lind, W (1989). *The Changing Face of War: Into the Fourth Generation*. Marine Corps Gazette, pp. 22-26.
- McChrystal, S., Collins, T., Silverman, D., & Fussell, C. (2015). *Team of Teams: New Rules of Engagement for a Complex World*. Portfolio/Penguin.

Mercado, D (2023) *Combate antitanque a través de la conformación de Organizaciones Mosaico con capacidades modulares*. [Investigación de Estado Mayor]

Pulido, G. (2021). *Guerra multidominio y mosaico: el nuevo pensamiento militar estadounidense*, España: Editorial Catara.















## Apéndice A

El Apéndice A presenta por medio de tablas y figuras, los materiales y sistemas especiales necesarios para el desarrollo del C4IG en operaciones multidominio.

Algunos aspectos a tener en cuenta son:

- Las características y capacidades de estos materiales y sistemas son generales teniendo en cuenta la constante innovación y avances tecnológicos.
- Los medios actuales provistos en las diferentes fuerzas como ser equipos UHF, HF o VHF, equipos de GE, etc, poseen las capacidades necesarias para desempeñar su rol correctamente por eso no son tenidos en cuenta en este apéndice.

### Figura A1

Mat Esp	SNT x Clase				Eq(s) Com Especiales			
	Micro (5km)	Mini (25 km)	Pequeño (50 km)	Táctico (200 km)	Sat Port	RCD	TSC	Rad Banda Ae
	X							
		X			X			X
			X		X			X
		X	X		X			X
	X	X			X			X
					X			X
	X				X			
	X				X			
					X	X	X	X
	X	X	X		X			X
							X	X
				X	X			X
					X			
	X				X			X

*Materiales especiales que permiten el C4IG de una Brigada Multidominio.*

*Nota:* La tabla muestra los materiales disponibles o a incorporar por elemento para poder alcanzar las capacidades de C4IG necesarias para operaciones multidominio en el nivel GUC. Los primeros tres elementos representan los elementos básicos de combate.

Sat Port: Equipo satelital portátil de transmisión de datos.

RDC: Radioenlace digital de campaña.

TSC: Terminal satelital de campaña.

Rad Banda Ae: Radio banda aérea.

### Tabla A1

*Capacidades y empleo de las aeronaves no tripuladas necesarias para un C4IG Multidominio*

Clase	Categoría	Alcance	Elemento que lo emplea	Propósito
I (< 150 kg)	Micro	5 km	Sección	E - D

	Mini	25 km	Subunidad	E - D - F
	Pequeño	50 km	Regimiento	E - F
II (150 - 600 kg)	Táctico	200 km	GUC / GUB	E - F
III (> 600 kg)	MALE - HALE	> 200 km	GUB / CTTO	E - A

Nota. Adaptado de *Fuerza de Tareas 35*, de *Ejército de Tierra de España*, 2019.

E: Exploración y reconocimiento.

D: Conducción de los fuegos directos.

F: Conducción de los fuegos indirectos.

A: Ataque.

**Figura A2**

*Alcance del tablero o plataforma de comando y control de acuerdo con cada nivel y elemento*

		NIVEL DEL ELEMENTO							
		...	I	II	x	xx	xxxx	oooo	
NIVEL AL QUE PUEDE ACCEDER	...	Verde oscuro	Verde oscuro	Verde oscuro	Verde claro	Verde claro	Verde claro	Verde oscuro	
	I	Verde oscuro	Verde oscuro	Verde oscuro	Verde oscuro	Verde claro	Verde claro	Verde oscuro	
	II	Amarillo	Verde oscuro	Verde oscuro	Verde oscuro	Verde oscuro	Verde oscuro	Verde oscuro	
	x	Blanco	Blanco	Amarillo	Verde oscuro	Verde oscuro	Verde oscuro	Verde oscuro	
	xx	Blanco	Blanco	Blanco	Amarillo	Verde oscuro	Verde oscuro	Verde oscuro	
	xxxx	Blanco	Blanco	Blanco	Blanco	Amarillo	Verde oscuro	Verde oscuro	
	oooo	Blanco	Blanco	Blanco	Blanco	Blanco	Amarillo	Verde oscuro	

Nota. La imagen representa los diferentes niveles de acceso a la información de cada elemento. Las limitaciones están dadas para evitar la sobrecarga de información, tanto para el conductor como para el medio tecnológico que emplee (tableta, notebook, computadora, etc). Los colores significan:

Verde oscuro: acceso.

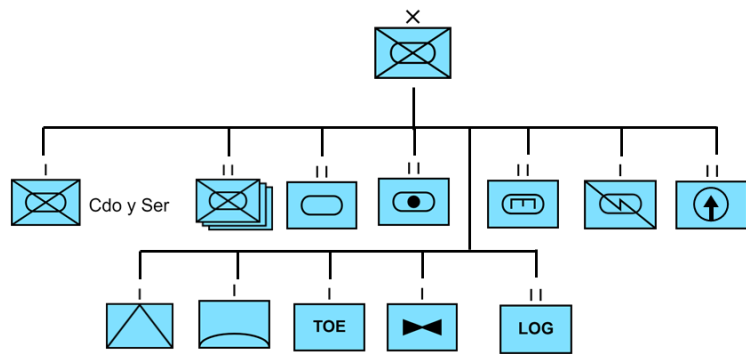
Verde claro: acceso sólo en caso de necesidad operacional.

Amarillo: acceso limitado o restringido.

### Apéndice B

En el Apéndice B se proporcionan los esquemas generales de organización de diversas GGUUC, los cuales están diseñados para llevar a cabo operaciones multidominio al integrarse en el sistema de C4IG Multidominio.

**Figura B1**



*Organización de una GUC Mecanizada y Blindada*

Las figuras B2 a B4 muestran los elementos constitutivos de una GUC Multidominio por funciones de combate.

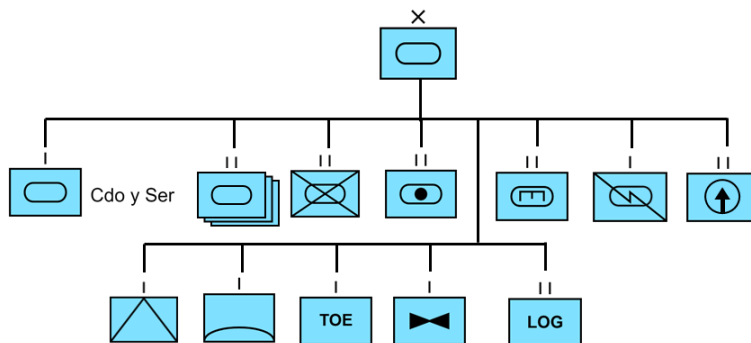
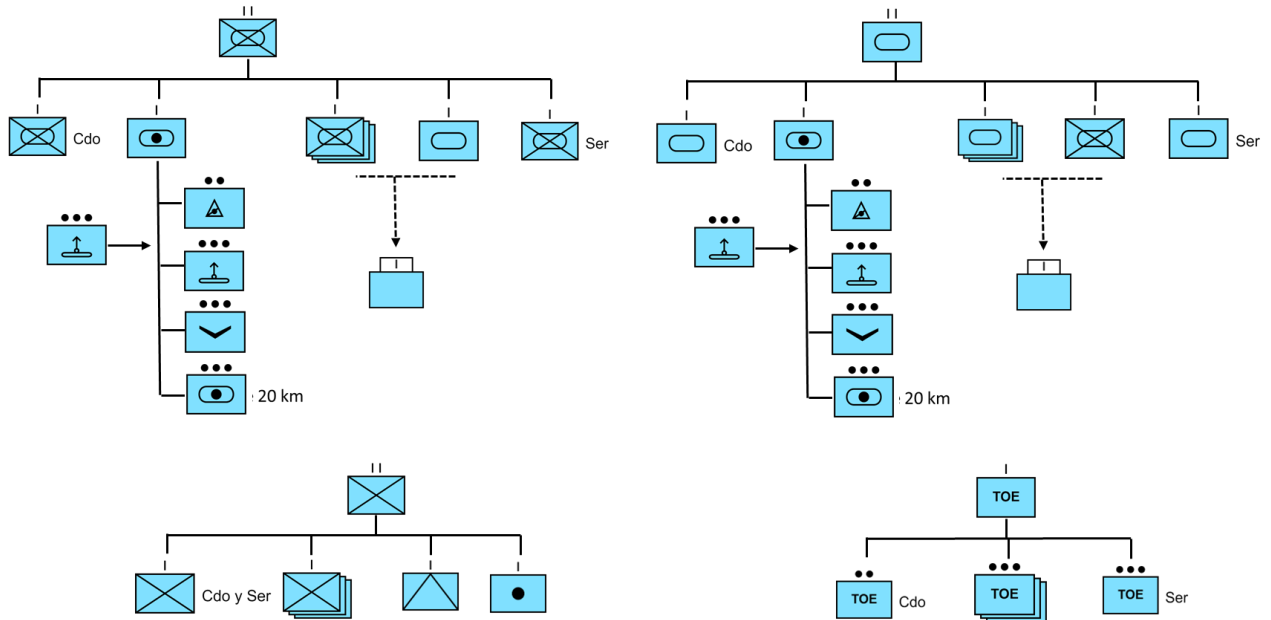


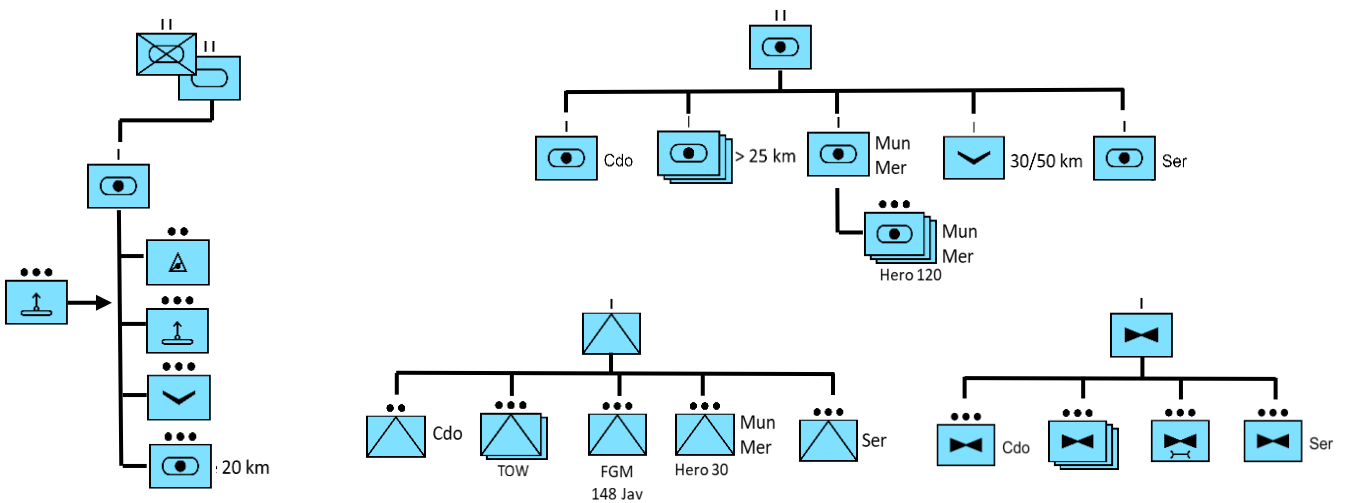
Figura B2



*Maniobra*

*Nota.* Los elementos de maniobra reciben una modificación principal a su organización, la Sección Morteros Pesados se modifica a una Batería de Artillería integrando morteros, ANT y piezas de un alcance de 20 km otorgándole versatilidad y flexibilidad a los elementos. En el caso de los elementos de infantería mecanizados se le agrega un escuadrón de tanques o una compañía antitanque aumentando su poder de fuego, letalidad e interoperabilidad. A todas las GGUUCC se les agrega una subunidad de Tropas de Operaciones Especiales.

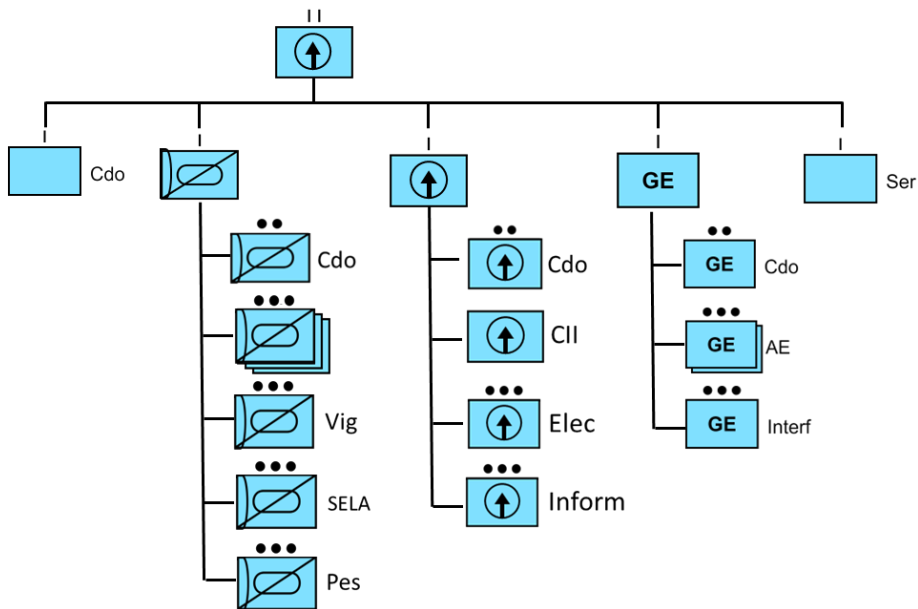
Figura B3



Apoyo de fuego

Nota. Además de las modificaciones ya desarrolladas en la Figura B2 y a las capacidades ya presenten, el Grupo de Artillería incorpora munición merodeadora y ANT con alcance entre 30 y 50 km, y sus cañones alcance mayor a 25 km; la Compañía Antitanque incorpora munición merodeadora y armas antitanque portátiles, adaptado de *Compañía Antitanque Multidominio*, de Mercado (2023).

Figura B4



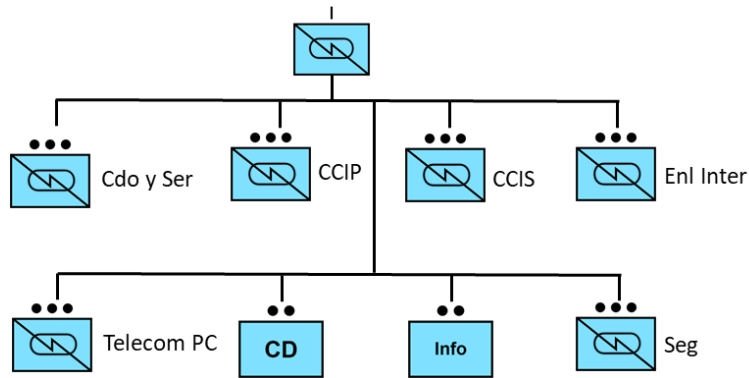
Inteligencia

Nota. Los elementos de exploración, inteligencia y guerra electrónica se organizan bajo un comando único en un Batallón de Inteligencia,



organizando sus elementos en obtención de información y análisis de información, evitando superponer esfuerzos y facilitando el planeamiento y ejecución de sus misiones.

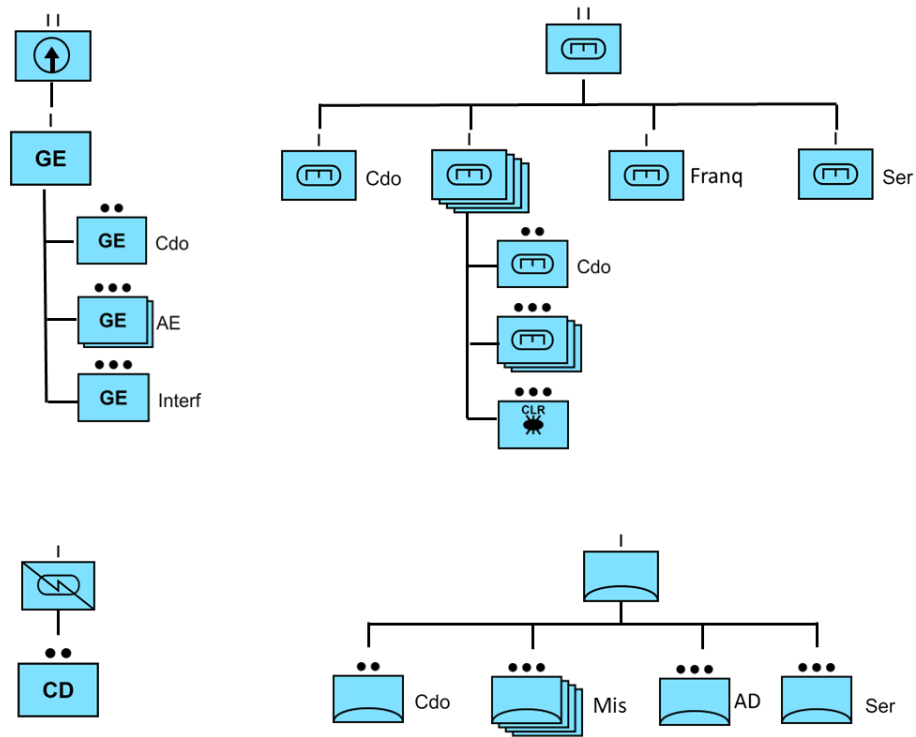
**Figura B5**



*Comando y Control*

*Nota.* La Compañía de Comunicaciones incorpora en grupo de Ciber Defensa y otro Informático para instalar, operar y mantener los tableros de mando y sistemas de comando y control multidominio, y brindar seguridad y defensa ante ataques cibernéticos.

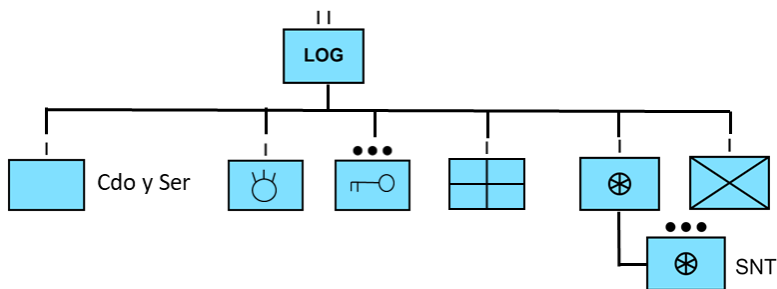
**Figura B6**



Protección

Nota. El principal cambio dentro de la función protección además de los elementos de guerra electrónica y ciberdefensa es la capacidad orgánica de desminado para las compañías de ingenieros de combate y la defensa aérea empleando sistemas de misiles.

Figura B7

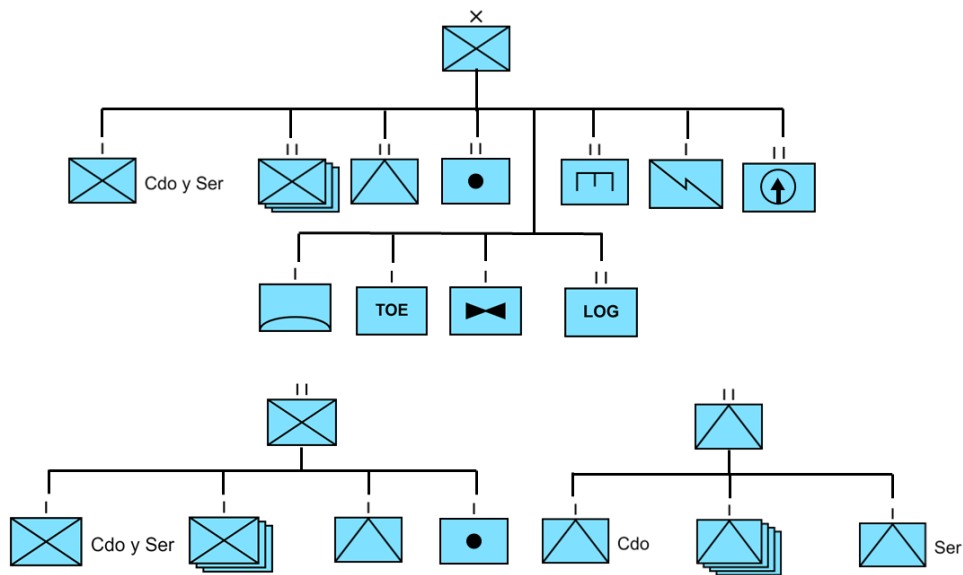


Sostenimiento

Nota. Los elementos logísticos dejan de funcionar a través de grandes centros logísticos o concentración de instalaciones en un solo lugar y pasan a operar a través de nodos o pequeños depósitos, haciendo uso de instalaciones fijas militares o civiles que funcionen como postas. Esto y la incorporación de sistemas no tripulados para transporte y evacuación permitirán aumentar la supervivencia de los medios y rutas logísticas.

Teniendo en cuenta la dificultad de adquisición o desarrollo, costos de diferentes materiales como ser los de GE, CD o SNT y el tiempo de adiestramiento del personal para operarlos, estos elementos como cualquier otro medio técnico y escaso debe operar con diferentes previsiones de empleo o misiones tácticas con orden preparatoria.

**Figura B8**



*Organización de una GUC Ligeras*

*Nota.* Las GGUUCC Ligeras incorporan a su organización un Regimiento Antitanque adaptado de *Regimiento Antitanque Multidominio*, de Mercado (2023).