Facultad del Ejército
Escuela Superior de Guerra
"TG Luis María Campos"

UNDEF
Universidad de la Defensa Nacional

**TRABAJO FINAL INTEGRADOR**

**Título: "La organización del Sistema de Inteligencia en apoyo al Componente Terrestre del Teatro de Operaciones en operaciones multidominio"**

**Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor HERNÁN RICARDO SALINAS.**

**Director del TFI: Coronel GABRIEL EDGARDO ROJO.**

Ciudad Autónoma de Buenos Aires,  de mayo de 2024.

**Resumen.**

El Componente Terrestre del Teatro de Operaciones, es un conjunto de organizaciones militares que forma parte de un todo, la cual va a desarrollar sus acciones militares en un determinado Teatro de Operaciones. En la actualidad, es muy difícil comprender a los conflictos sin mencionar la existencia de otros dominios "no clásicos" en donde el avance tecnológico, las amenazas que surgen producto de la globalización, intereses, otros tipos de actores y la aparición de tecnología disruptiva, impactan de manera directa sobre las operaciones militares.

Es así como el ciberespacio, el espacio, el espectro electromagnético y el dominio cognitivo/humano estarán presentes en toda operación, obligando a toda Fuerza Armada a hacer un cambio rotundo de perspectiva rompiendo paradigmas. La forma tradicional de hacer la guerra como lo era el combate aeroterrestre ya no es suficiente, existen otras variables que configurarán el campo de batalla, pero nunca dejando de lado los ambientes y factores "clásicos", los cuales van a interactuar con otros factores/dominios "no clásicos".

La inteligencia, juega un rol preponderante, ya que la misma debe cumplir sus tareas fundamentales en el nivel que corresponda, en este caso particular en el nivel táctico, pero dentro de la esfera conjunta. En consecuencia, el análisis de todos los factores del ambiente operacional, la incorporación de nuevas tecnologías, base informativa detallada, adecuado análisis de las posibles amenazas, la integración y el trabajo interagencial, facilitarán la toma de decisiones del comandante y evitará la sorpresa.

**Palabras claves*:*** Inteligencia, Operaciones Multidominio, Componente Terrestre del Teatro de Operaciones, Gran Unidad de Batalla.

# Índice

## Índice de tablas



## Índice de figuras

# Introducción

## Presentación del problema

La teoría general de los sistemas de Bertalanffy (1968), puesto en pocas palabras, define al sistema como un conjunto de partes o elementos interrelacionados que interactúan entre ellos. Este sistema tiene una entrada/input (insumo que necesita para su funcionamiento), luego tenemos un proceso (análisis, donde se convierten esos inputs en outputs) y finalmente en esta secuencia se presenta el output (salida, que sería el producto resultante del proceso).

Estos conceptos, llevados en al marco de las organizaciones del instrumento militar y específicamente al campo de la conducción de inteligencia, nos lleva a pensar en la metodología madre empleada que se resumen en el ciclo de la producción de la inteligencia. Allí, identificamos la obtención de la información (entrada), el proceso de la información (proceso) y la diseminación (salida).

Asimismo, en esta identificación de partes, también existe una retroalimentación que va actualizando el sistema propiamente dicho y el contexto/ambiente, el cual da marco y rodea al sistema donde va a desenvolverse e interactuar.

Llevado al campo de las estructuras que se conforman para dar vida a un teatro de operaciones, se entiende al componente terrestre como un subsistema, el cual podrá contener a una Gran Unidad de Batalla (en adelante GUB) ya sea formando parte del Componente Terrestre del Teatro de Operaciones (CTTO) o constituyéndose como tal.

El apoyo de inteligencia que se le proporciona a esa GUB, por ejemplo, es un sistema abierto y se materializa en el apoyo que le proporciona el Batallón de Inteligencia (en adelante B Icia) donde, la Compañía Centro Integrador de Inteligencia (en adelante CII) del B Icia apoya al órgano de dirección (G2) de la GUB. Su medio de ejecución, la Compañía de Inteligencia,

ejecuta procedimientos de obtención sobre las fuentes que existen en el campo de combate para dar vida al ciclo de inteligencia, en torno a la misión de la División.

Con este ejemplo se observa la interrelación de las partes y una propiedad de los sistemas abiertos, la homeostasis, que se entiende como la capacidad de un sistema para mantener su equilibrio y autorregularse. En efecto, esto lo lograría, por ejemplo, con un elemento de inteligencia, donde busca información, la procesa y la disemina; esta función brinda una de las herramientas necesarias para que el comandante lleve adelante sus acciones, por lo tanto, el sistema se va retroalimentando con información constante, manteniendo su equilibrio.

En definitiva, esta aproximación a lo que es un sistema, nos da la pauta que se debe observar a la organización como un todo, de manera holística, que va a interactuar con el contexto que lo rodea, interrelacionándose con todas sus partes en la consecución del logro de un fin determinado.

Por otra parte, hay que tener en cuenta que nos encontramos en un mundo donde las Tecnologías de la Información y Comunicación (en adelante TICs) y la evolución tecnológica tendrán un impacto directo en la forma de organizar y adiestrar a nuestras fuerzas militares. Estas y otras variables serán factores determinantes en los conflictos armados.

En ese mismo orden de cosas, la globalización también será parte de estas variables, ya que es un proceso que abarca a todo el mundo, con la finalidad de interconectar a los países. Esta integración fue poco a poco tomando mayor impulso y velocidad, debido al avance de la tecnología.

Es así, que gracias a la globalización se obtuvo grandes e importantes beneficios en diferentes aspectos, tales como en comercio, cultura, comunicaciones, etc, pero también trajo consigo diferentes desafíos y problemas a enfrentar.

Particularmente y centrando el tema en la defensa nacional, nuevas amenazas surgieron aprovechando este avance tecnológico e hicieron que muchos actores cobren una gran importancia utilizando nuevos dominios como, por ejemplo, el ciberespacio. (Oreglia, 2017)

Entendiendo a la guerra como un estadio del conflicto donde se enfrentan dos o más actores buscando imponer sus objetivos y que la misma va a evolucionar conforme a la tecnología, se genera una de las formas de clasificación de la guerra. (EMCO, 2018).

Esta clasificación, que nace con la primera y continúa hasta la quinta Generación, muestran un camino recorrido desde los conflictos de la antigüedad, la aparición de las armas de fuego, atravesando la primera guerra con la industrialización y la mecanización, la segunda guerra mundial, la guerra irregular, el uso de otros dominios y la tecnología nuclear. Es aquí donde nos encontramos con nuevas definiciones, tales como las operaciones multidominio.

Para identificar este concepto es necesario tener en cuenta que los conflictos armados se clasifican en: conflictos armados en ambiente convencional o regular, conflictos armados en ambientes no convencionales o irregulares, conflicto armado en ambiente compuesto y conflicto armado en ambiente híbrido (EMCO, 2018).

Es en este último tipo de conflicto, se opera en diferentes dominios, utilizando tácticas convencionales con acciones híbridas. Se puede observar claramente que, en los conflictos actuales, las fuerzas militares utilizan este tipo de metodología para hacer la guerra.

Por consiguiente, las organizaciones militares deben desarrollar capacidades que les permita abarcar la guerra en múltiples dominios (aéreo, terrestre, marítimo, espacio, ciberespacio, espectro electromagnético y humano) de una manera sistémica para lograr los fines trazados.

Cabe aclarar que nuestra doctrina no dispone de reglamentos específicos que desarrollen la temática. En efecto, en el reglamento conjunto se menciona la batalla multidominio definida de la siguiente manera:

> Un concepto de empleo de las fuerzas, sincronizado y convergente en el marco de la acción militar conjunta, a través de los cuatro ambientes operacionales (terrestre, naval, aeroespacial y cibernético), llevando a cabo operaciones para, evitar el aislamiento de los componentes y lograr la sinergia que permita obtener la superioridad sobre el enemigo en un momento y lugar determinado. (EMCO, 2019, pag 32)

Haciendo mención al menor nivel de la conducción táctica, la GUC, no dispone orgánicamente de medios que actúen en todos los dominios mencionados por su eminente naturaleza terrestre y específica, pero si deben crear los enlaces necesarios para poder incluirlos teniendo en cuenta factores de éxitos tales como la modularidad y la interoperabilidad (EMCO, 2023).

La misma no actuará de forma aislada ni independiente, sino en el marco de la campaña en un ámbito conjunto, conteniendo operaciones multidominio planificadas por el nivel operacional y llevadas adelante por los componentes que se conformen para un determinado Teatro de Operaciones (en adelante TO). Este nivel, el operacional, establecerá diversas capacidades para las organizaciones que actuarán de forma modular en ámbitos físicos y no físicos en un espacio multidimensional.

En definitiva y relacionado al tema en cuestión, dentro de los elementos del diseño operacional tradicionales se considerará el concepto de maniobra operacional multidominio, la cual se basa en ejecutar permanentes movimientos para evitar que el adversario utilice una variedad de elementos para la adquisición y observación a fin de detectar nuestra presencia y así, aplicar su poder de combate. Por lo tanto, es necesario tener en cuenta que los recursos a

emplear en nuestras organizaciones para contrarrestar lo anteriormente mencionado, deben responder al uso de medios tales como: Vehículos Aéreos No Tripulados (en adelante VANT), radares, sensores, armas antitanques, capacidad de comando y control y defensa antiaérea (EMCO, 2023).

En base a ello, y colocando un hipotético escenario bélico, podemos inferir que las actividades que desarrollarán, en la actualidad, las organizaciones militares serán de gran complejidad con múltiples variables y situaciones que deberán ser afrontadas por los diferentes niveles de toma de decisiones.

Esta creciente complejidad y los distintos factores del ambiente operacional que se presentan en el campo de batalla, requieren del desarrollo de ciertas capacidades para las organizaciones militares que les permita cumplir misiones con mayor especificidad. La especialización en cada organización, hacen a la eficiencia del elemento, pero nunca perdiendo de vista los factores de éxito anteriormente nombrados: la interoperabilidad y la modularidad.

En cuanto a los antecedentes del tema, existen diferentes investigaciones, estudios y trabajos relacionados a las operaciones multidominio y su relación con la inteligencia.

En primer lugar, voy a citar un Trabajo Final Integrador (en adelante TFI) de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, referido sobre al multidominio, visto como un desafío para las Fuerzas Armadas Argentinas. Este documento trata sobre la distinción, vinculación y empleo de los dominios en el ambiente operacional llevando adelante la batalla multidominio. Particularmente marca la influencia que tienen los nuevos dominios en las operaciones militares de las Fuerzas Armadas de la República Argentina (Angulo Molina, 2019).

El segundo TFI a mencionar, se refiere al sistema de inteligencia del componente terrestre y la guerra de la información, el autor hace mención sobre las capacidades que debe

desarrollar el sistema de inteligencia en este nivel para hacer frente a las actividades de la guerra de la información, ya que se entiende que la función de inteligencia es la principal responsable de la obtención de información y del proceso de la misma, generando productos que sirvan para el asesoramiento y la asistencia. Este trabajo se toma como antecedente e información relevante ya que las operaciones de información transitan dentro del ámbito de las operaciones multidominio. (D'Agata, 2021).

Asimismo, otro TFI de la Escuela Superior de Guerra expone sobre el CII en apoyo al Departamento Inteligencia del CTTO. El autor trata de demostrar los inconvenientes que existen en este nivel de la conducción y al apoyo de este al órgano de dirección, remarcando un vacío en la doctrina y por supuesto la importancia de este en apoyo al Componente Terrestre. Se toma como un importante antecedente, obteniendo información relacionada al sistema de inteligencia en general, comparaciones que se realizan con países de la región y las capacidades y limitaciones que existen dentro del órgano de dirección de estos niveles (Páez, 2021).

Finalmente, un cuarto trabajo que citaré está referido a la organización de la jefatura de inteligencia del Comando Operacional de las Fuerzas Armadas en las operaciones multidominio. El autor explica la importancia de conformar un órgano de dirección de inteligencia de un comando estratégico operacional a fin de brindar las bases necesarias para la toma de decisiones en ámbitos físicos y no físicos. Además, se infiere que esta organización se podrá utilizar tanto en la paz como en el desarrollo de operaciones militares cuando se conforme el comando de un teatro de operaciones, nivel donde se desarrollarán la mayor parte de las operaciones multidominio (Arenas, 2021).

Para finalizar con este primer bloque, y haciendo una conclusión parcial, podemos inferir que los conflictos actuales hacen de la función inteligencia un subsistema primordial, que junto con las demás funciones de combate permitirán un desarrollo sistémico durante las

operaciones militares facilitando la conducción de estas. Por lo tanto, la evolución de los conflictos armados, el uso de diferentes dominios y el vertiginoso avance de la tecnología obliga a que la inteligencia se especialice, conformando un sistema idóneo, capacitado, integrado y adiestrado para brindar un adecuado apoyo de inteligencia al CTTO.

Como segundo bloque de la presente investigación y como parte de los antecedentes y justificación del problema, nos centraremos en conceptos generales de la inteligencia en apoyo a la GUB/CTTO, materializado por el sistema de inteligencia (Batallón de Inteligencia / Destacamento de Inteligencia de Combate).

El CTTO, es un conjunto de fuerzas específicas que forma parte de una fuerza conjunta (el teatro de operaciones), estos son puestos a disposición de un comandante para el cumplimiento de una misión (EMCO, 2018, pag 52)

Asimismo, podrá ser conformado por algunas de las siguientes organizaciones: Grandes Unidades de Batalla - Grandes Unidades de Combate - otras grandes unidades de nivel brigada - Centro de Apoyo Logístico - Centro Regional de Apoyo Logístico - Agrupaciones, Destacamentos, Unidades y Subunidades (EA, 2015, Cap II-40).

Entre las características más sobresalientes del CTTO podemos mencionar que: cuenta con Orden de Batalla (en adelante OB), se materializa en este nivel un elevado grado de incertidumbre relacionado a las intenciones del enemigo, enfrenta problemas militares operativos complejos y futuros, se caracteriza por desarrollar sus acciones en amplios espacios, por lo tanto, existe una dificultad para identificar flancos, frente y retaguardia. En definitiva, da como resultado un problema para el apoyo mutuo entre los elementos dependientes.

Razón por la cual, la coordinación entre los comandos que participen en el TO será un factor determinante para alcanzar una coherente y sistémica acción común, como así también contar con un eficiente sistema de comando y control vinculado con plataformas militares o

sensores que permitan obtener información y comunicar de forma segura facilitando la transmisión de información en tiempo real y su posterior procesamiento impactando positivamente en la conciencia situacional que debe poseer el comandante, el estado mayor y todo el sistema propiamente dicho.

La GUB es una organización operacional que podrá integrar el CTTO, algunas características más importantes son: la de no poseer una organización fija (sino que dispone de OB), opera en grandes espacios, conduce operaciones complejas atendiendo varias direcciones de operaciones en forma simultánea, dispondrá de un número variable de formaciones y de GGUUCC, desarrollará sus acciones en zonas lineales, contiguas y no contiguas, tiene la estructura para constituirse como Comando del CTTO, llevando a complejizarse aún más la conducción (EA, 2015, Cap II, 41-42).

El comandante de la GUB/CTTO, como así también su estado mayor, durante el planeamiento y ejecución de las operaciones militares, necesitarán llenar vacíos de información o interrogantes que se presenten.

Estos interrogantes, que se transformarán en requerimientos, no estarán solamente relacionados al terreno, enemigo, condiciones meteorológicas y otros aspectos particularizados del ambiente geográfico, sino también a requerimientos relacionados al ambiente operacional (factores sociales, demografía, geografía económica, infraestructuras, medios de comunicación social, sistemas de armas, etc).

Por lo tanto, podemos inferir que, al enfrentarnos a numerosos factores tales como la extensión del terreno, el tiempo disponible y la voluntad inteligente de otro actor/actores, la población, el uso de tecnologías disruptivas, hace indispensable contar con un sistema de inteligencia flexible, integral, especializado, con información básica, tecnología y

técnicas/capacidades específicas (a desarrollar) para enfrentar las operaciones multidominio que se desarrollan en los conflictos actuales.

En definitiva, nos centraremos en el empleo de las organizaciones de inteligencia en apoyo a la GUB y CTTO, materializado por el B Icia y el Destacamento de Inteligencia de Combate (en adelante DIC) formando parte del Sistema de Inteligencia del Ejército (en adelante SIE).

Relacionado al apoyo a la GUB, se considera un gran desafío para la inteligencia lograr el apoyo pertinente a las operaciones profundas, al empleo de la reserva por parte de la GUB y en la detección del centro de gravedad del enemigo (EA, 2017, Cap I, 3-4).

El sistema de inteligencia en este nivel (GUB) estará conformado por el B Icia, los Subsistemas de Inteligencia de Combate (en adelante SIC) y Subsistemas Territoriales de Apoyo de Inteligencia (en adelante STAI). Este nivel debe estar en perfecta armonía con los niveles de inteligencia superior (operacional), para integrar los esfuerzos necesarios a fin de brindar información e inteligencia detallada.

El B Icia, es una unidad que conforma un agrupamiento de medios de obtención y medios en apoyo al órgano de dirección que brindaran apoyo integral de inteligencia a la GUB dentro de una zona determinada (EA, 2017, Cap II – 1).

Particularmente, el CII es la organización que orientará el sistema de inteligencia de la GUB, junto con el G2 de la GUB conformarán el órgano de dirección de inteligencia (EA, 2017, Cap I, 5-7).

Los medios de obtención específicos del B Icia, materializados por la Compañía de Inteligencia de Combate, se basarán en medios de Inteligencia Humana (en adelante INTHUM) y en medios de Inteligencia de Emisiones (en adelante INTEM) para satisfacer necesidades de información provenientes de la GUB.

Por otro lado, el Destacamento de Inteligencia de Combate (DIC) será el elemento que brindará el apoyo de inteligencia al CTTO y en su doctrina marca la importancia de contar con información en tiempo real (análisis inmediato mientras es obtenida) o casi real (análisis en un corto período luego de ser obtenida).

El DIC, es la mayor unidad táctica de inteligencia de combate, para obtener información en la zona de interés de un comando de nivel estratégico operacional (sería el nivel operacional el comando del TO) o táctico superior (termino en desuso, hoy se refiere a la conducción nivel táctico, específicamente las GGUUBB y los Comandos de Componentes (CTTO). Básicamente sus misiones estarán orientadas a brindar apoyo de inteligencia al Comando del Teatro de Operaciones (CTO), al CTTO, o a una GUB. Aclarando que hoy en día, el DIC apoya al nivel CTTO.

Su organización depende de un cuadro de organización y su estructura será variable según al tipo de comando que apoye y el ambiente operacional donde se encuentre enmarcado. Contará con organizaciones del tipo Subunidad y estas son netamente elementos de ejecución, tales como: Compañía de Inteligencia de Combate, Geográfica, Obtención Aérea y Obtención Electrónica (EA, 2007 Pag 3 y 22).

El CII formará parte del Puesto Comando del DIC y básicamente el DIC actuará sobre el área de combate a través de la inteligencia de combate.

En consecuencia, se presentan varios interrogantes, los que se intentarán dar respuesta en el presente trabajo. Así, por ejemplo, algunos de ellos son:

¿Cuáles son los dominios preponderantes en el nivel CTTO?

¿Cómo puede enfrentar el órgano de dirección de inteligencia del CTTO la complejidad que presenta este tipo de operaciones? ¿Cuáles serían las capacidades que deben poseer los especialistas para enfrentar este tipo de operaciones?

¿Los medios de obtención del sistema de inteligencia (B Icia y DIC) son acorde/afines para la ejecución de procedimientos de obtención en este tipo de operaciones? ¿Qué otros tipos de materiales, recursos, personal, tecnología se necesitan?

¿Cuáles son los tipos de especialistas del CII y del estado mayor del CTTO o GUB para el asesoramiento y asistencia en este tipo de escenarios? ¿Cuáles son las tecnologías, comunicaciones e infraestructuras para enfrentar estos desafíos?

El apoyo del DIC en el nivel CTTO, ¿Cómo se integra con el B Icia?, en el caso que se conforme un CTTO en base a una GUB, ¿cómo actúa el DIC? ¿A quién apoya? ¿Se complementan sus capacidades con las del B Icia? ¿O se integran formando un solo núcleo?

¿Qué otros tipos de requerimientos necesita un Cte CTTO durante este tipo de operaciones?

Finalmente, es necesario identificar y relacionar las funciones que cumplen las organizaciones existentes en este nivel, ya que hay tareas que pueden ser reorganizadas, distribuidas o crear algunos procesos de trabajo para darle eficiencia al sistema. Es parte de este trabajo investigar, y proponer soluciones afines para optimizar el empleo del Sistema de Inteligencia en apoyo al CTTO.

## Formulación del Problema

¿Cuál es el diseño organizacional, sus elementos constituyentes y los procesos de trabajo para brindar el apoyo de inteligencia al CTTO en el marco de las operaciones multidominio?

## Objetivo de la Investigación de Estado Mayor

### *Objetivo General*

Establecer y determinar la organización del elemento que proporcione el apoyo de inteligencia a un Componente Ejército del Teatro de Operaciones en la ejecución de operaciones multidominio.

### *Objetivo Particular Uno*

Analizar y describir las características de las operaciones multidominio para determinar su influencia en el apoyo de inteligencia en el nivel CTTO.

### *Objetivo Particular Dos*

Analizar y describir el actual Sistema de Inteligencia a nivel GUB y CTTO, para determinar el concepto de empleo y capacidades más adecuadas que debería disponer el sistema en el nivel CTTO, para afrontar las exigencias que imponen las operaciones multidominio.

## Metodología a Emplear

### *Explicación del Método:*

El método a emplear será el deductivo.

### Diseño de la Investigación:

El diseño de la investigación será de tipo explicativo.

### Técnicas de Validación:

Análisis bibliográfico, documental y lógico.

# Capítulo I.

## Características de las operaciones multidominio para determinar su influencia en el apoyo de inteligencia en el nivel CTTO.

El presente capítulo tiene por objetivo analizar y describir las características más significativas de las operaciones multidominio, para poder determinar su influencia en el apoyo de inteligencia en el nivel CTTO.

El capítulo se divide en cuatro secciones, donde me respaldaré en artículos y publicaciones de las fuerzas armadas de los Estados Unidos de América (en adelante EUA), Chile, y España. Como así también en un boletín informativo que emitió el Estado Mayor Conjunto de las Fuerzas Armadas referido a la concepción estratégica de capas, restricción de áreas y operaciones multidominio.

En la primera sección trataré sobre el marco legal vigente, los cuales proporcionan las bases necesarias para poder encuadrar el desarrollo de este tipo de operaciones y sobre las actividades de inteligencia a desarrollar.

En la segunda sección, mencionaré los conceptos y características de las operaciones multidominio desde el punto de vista de diferentes publicaciones extraídas de instituciones/organismos tales como academias de guerra, centros/institutos de estudios e investigación, revistas militares y la propia doctrina.

En la tercera sección haré referencia a la vinculación de las operaciones multidominio con estrategias de disuasión y restricción de áreas. Como así también conceptos referidos a anti-acceso y negación de área (A2/AD) y el concepto de Network Enabled Capability (NEC), para posteriormente mencionar la preponderancia de la inteligencia en las operaciones multidominio. Para así, finalmente, en la cuarta sección, llegar a las conclusiones parciales del presente capítulo.

## Sección I

## Marco Legal.

**Ley de Defensa Nacional Nro 23.554**, expone en su artículo 2 que las Fuerzas Armadas solucionaran conflictos en forma disuasiva o efectiva para enfrentar las agresiones de origen externo (República Argentina, 1988).

A su vez, la ley de defensa nacional marca que dentro de las finalidades que tiene el sistema de defensa es asegurar la ejecución de operaciones militares conjuntas de las Fuerzas Armadas y eventualmente operaciones combinadas que pudieran llevarse a cabo (República Argentina, 1988).

En su artículo 15, menciona las actividades de inteligencia nacional y nivel estratégico militar, el cual se integrará con los organismos de inteligencia de las otras fuerzas.

En su artículo 21 describe que para la organización y despliegue de las fuerzas armadas dependerán del planeamiento militar conjunto logrando la eficiencia conjunta (República Argentina, 1988).

Y en su **reglamentación, decreto 727/2006**, cita en su artículo 1 que las Fuerzas Armadas serán empleadas ante agresiones de origen externo perpetradas por fuerzas armadas de otros Estados.

Con respecto a la **"ley de reestructuración de las Fuerzas Armadas" Nro 24.948**, en su artículo 2 menciona que se debe lograr una eficaz estrategia disuasiva. A su vez, en su artículo 5, expone que se dará prioridad al accionar conjunto y a la integración tanto con fuerzas de seguridad como del ámbito regional (República Argentina, 1998).

Específicamente en el artículo 8, expone:

“Dividir el territorio nacional en áreas estratégicas dotadas de un comando, de carácter conjunto, con la misión de realizar estudios y previsiones de carácter estratégico operacional y de elaborar las doctrinas aptas para el área estratégica correspondiente” (República Argentina, 1998, art 8 a))

Con ello también agrega que se debe potenciar el uso de medios informáticos, estandarizando los mismos para toda la fuerza.

Finalmente, en su artículo 19, haciendo referencia al equipamiento a incorporar, cita que se debe dar prioridad a aquellos que potencien la capacidad disuasiva.

En contra posición de la ley anteriormente expuesta, el **decreto 1691/2006 “Organización y funcionamiento de las FFAA”,** expone que el territorio nacional conformará una sola área estratégica hasta que el planeamiento estratégico no aconseje lo contrario.

Se menciona en la mayor parte del documento lo fundamental de entender al instrumento militar como una organización integrada, con acciones conjuntas para lograr la máxima capacidad. A su vez, se establece que se dispondrá de un Comando Operacional el cual será el responsable del adiestramiento militar conjunto, las ejercitaciones, el planeamiento y ejecución de operaciones militares con los medios que los Estados Mayores Generales de cada Fuerza designen.

Otro punto es el diseño de la fuerza en función de las “capacidades” en reemplazo al uso del instrumento militar basado en “hipótesis de conflicto”, disponiendo de una “capacidad suficiente” para desarrollar de forma sistémica y autónoma todas las operaciones inherentes a la potencialidad de que se trate (República Argentina, 2006)

Finalmente, prioriza las capacidades de vigilancia, comando y control, comunicaciones, informática e inteligencia, movilidad táctica y estratégica con su sostén logístico correspondiente.

Con relación a la **Ley de Inteligencia Nacional 25.520**, expone en su artículo 10 la creación de la Dirección Nacional de Inteligencia Estratégica Militar (DNIEM) a fin de producir inteligencia estratégica militar. Asimismo, los organismos de inteligencia integrantes de las Fuerzas Armadas serán los responsables de la inteligencia operacional, táctica y técnica específica (República Argentina, 2001).

Y en relación con las actividades de inteligencia la **resolución ministerial 381/06,** hace mención que los organismos de inteligencia de las Fuerzas Armadas realizaran inteligencia de nivel estratégico Operacional y táctico sobre el componente militar. Cuando estén relacionados al accionar militar se incluyen los componentes: geográfico, transporte, telecomunicaciones y científico-técnico. (República Argentina, 2006)

Finalmente, para cerrar la primera sección, resta mencionar la **Directiva de Política de Defensa Naciona**l (DPDN). En su primera parte, en el diagnóstico y apreciación del escenario de defensa global y regional (tablero transnacional), describe que resulta de importancia considerar las dimensiones de la defensa relacionadas al ciberespacio, porque este no es un espacio en sí mismo, sino que atraviesa a todos los espacios tradicionales (tierra, mar, aire y espacio), se explica que tiene un origen virtual, pero impacta en el mundo físico, particularmente sobre las infraestructuras críticas.

En su capítulo dos, marca que la República Argentina adopta una identidad (actitud) estratégica defensiva, renunciando a políticas ofensivas con proyección de poder sobre otros estados. Por lo tanto, la estrategia que debe llevar adelante el Sistema de Defensa esta apuntado hacia la disuasión de potenciales agresiones externas perpetradas por otros estados. A su vez, se indica que, para garantizar los intereses vitales, deben prevalecer los mecanismos de vigilancia, reconocimiento y producción de inteligencia militar de los espacios aeroespaciales, marítimos, terrestres y ciberespaciales.

La amenaza que afectaría el territorio orientaría su esfuerzo sobre espacios y recursos estratégicos como, por ejemplo, las cuencas hidrocarburíferas, sector agropecuario, cuencas hidrográficas, minería, etc.

En su capítulo tres, menciona que el planeamiento estratégico militar deberá elaborarse teniendo en cuenta el control efectivo de los espacios territoriales soberanos en sus ambientes terrestre, marítimo, aeroespacial y su transversal dimensión ciberespacial. Con lo cual hace énfasis sobre la capacidad de vigilancia, comando, control, comunicaciones, informática, inteligencia y guerra electrónica con el fin de contar con una adecuada alerta temprana estratégica.

En efecto, este planeamiento debe considerar el desarrollo de capacidades operacionales de ciberdefensa y de capacidades destinadas a proteger la seguridad de las redes pertenecientes al Sistema de Defensa Nacional con un eje en la soberanía nacional y el otro sobre el plano táctico.

Por lo tanto, se debe resguardar el entorno digital, ya que el ciberespacio será uno de los dominios donde la ciberdefensa debe minimizar el riesgo y contrarrestar eventos que afecten la disponibilidad del ciberespacio durante las operaciones militares. Asimismo, se hace hincapié en el empleo de la inteligencia artificial, la cibernética, acceso al espacio y la biotecnología.

Otra cuestión importante para tener en cuenta es la identificación de escenarios estratégicos: norte, centro y sur.

Por otro lado, y relacionado con la amplia gama de funciones del ministerio de defensa, particularmente en materia de investigación y política industrial para la defensa, debe potenciar los programas tecnológicos orientados a la vigilancia y control de los espacios soberanos, avances de sistemas de armas y la protección de infraestructuras críticas. Como punto importante menciona el desarrollo de una política de ciberdefensa.

En cuanto a las funciones del Estado Mayor Conjunto, debe delinear una estrategia militar que responda a algunas de las siguientes consideraciones: disponer de una concepción estratégica para desgastar en forma constante y progresiva un eventual avance de un agresor a través de operaciones de disuasión, resistencia y/o recuperación. La priorización del control efectivo de los espacios terrestres, marítimos, aeroespaciales y ciberespaciales de jurisdicción nacional, por lo que se deben intensificar las tareas de vigilancia, control y reconocimiento en las áreas de frontera.

Asimismo, el Estado Mayor Conjunto, intervendrá en lo que se refiere al presupuesto de las Fuerzas Armadas, referido a proyectos de inversión, por lo que se establece prioridades en las inversiones, reconociendo las siguientes: sistemas C4I2VR, sistemas de satélites de comunicaciones y observación, sistemas no tripulados (terrestres, marítimos, submarinos y aéreos) y sistemas de ciberdefensa.

Y finalmente, se menciona la responsabilidad de orientar y coordinar acerca de proyectos que tiendan a disponer de una arquitectura única de comando y control único, en todos los niveles para optimizar el conocimiento situacional y la toma de decisiones en tiempo y forma.

## Sección II

## Características de las operaciones multidominio.

Para poder llegar a una aproximación del concepto de multidominio, iniciaremos la presente sección citando un artículo del Centro de Estudios de Investigaciones Militares de Chile (CESIM), en donde podemos expresar que las operaciones multidominio buscan explotar sinérgicamente las capacidades militares existentes en los dominios físicos y no físicos/abstractos (tierra, mar, aire, espacio, ciberespacio, espectro electromagnético, ambiente de la información y cognitivo) y así generar las condiciones que permitan obtener un control

local y temporal en el campo de batalla, para entregar a los comandantes múltiples opciones para alcanzar la victoria (León, 2017).

Dentro del ámbito de las Fuerzas Armadas del Reino de España, según el jefe de Estado Mayor de la Defensa, tras un análisis para aclarar lo que se debe entender por las operaciones multidominio en las Fuerzas Armadas Españolas, expresa que son:

> Todas aquellas operaciones realizadas por la Fuerza Conjunta que, por su agilidad y complejidad, necesitan de una adecuada interoperabilidad y conectividad que posibiliten un control distribuido de los medios para permitir la integración de todas sus capacidades y así poder producir efectos en y desde cualquiera de los ámbitos de operación (Ministerio de Defensa de España, 2020).

Dentro del ámbito de las Fuerzas Armadas Argentinas, personal del Comando Operacional de las Fuerzas Armadas, durante una exposición en la Escuela Superior de Guerra durante el mes de setiembre del año 2023, expuso el siguiente concepto sobre 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, generando efectos sincronizados en momentos del ritmo operacional relacionados a la identificación de vulnerabilidades críticas y disponibilidad de recursos (Comando Operacional de las Fuerzas Armadas, 2023).

Algunas características que encontramos en la actualidad sobre este tipo de operaciones son las siguientes:

- Aproximación operacional indirecta en teatros de operaciones no lineales.

- Acciones integradas por dos grandes líneas, una del sistema de armas tradicionales y la otra a través de los dominios espacial, electromagnético y de la información, actuando como multiplicadores del poder de combate.
- Sistemas de comando y control interconectados en red donde el factor tiempo y velocidad son cruciales.
- Movilidad constante como medida de protección.
- Sistemas targeting, fuegos cinéticos y no cinéticos enlazados en red a centros integradores de inteligencia.
- Acciones de información de forma permanente – sostén logístico agiles y simplificados (EMCO, 2023).

Haciendo una breve explicación de los dominios podemos describir lo siguiente: dominio “tierra/terrestre” es el que se desarrolla sobre la superficie terrestre (zonas urbanas o rurales). Estas incluyen todas las tácticas y procedimientos de empleo de una maniobra operacional, ya sea con actitud defensiva (control de un objetivo) u ofensiva (conquista de un objetivo).

El dominio “mar”, se centrará en las operaciones navales, que incluyen las fuerzas de superficie, de submarinos, aeronaval, anfibia y la infantería de marina que proyectará el poder desde la superficie marítima hacia el interior del territorio.

El dominio “aire” va a comprender aquellas operaciones en el espacio aéreo (Interdicción Aérea Táctica (IAT), Apoyo de Fuego Aéreo Cercano (AFAC), Cobertura Aérea Defensiva (CAD), Exploración y Reconocimiento Aéreo Táctico (ERAT), Transporte Aéreo Táctico (TAT), Búsqueda y Salvamento Aéreo (BSA) y por supuesto el combate aéreo propiamente dicho.

El dominio “espacio”, comprende todas las actividades relacionadas a la defensa nacional en el espacio ultraterrestre. Utilizando satélites como medio fundamental, para operaciones tales como como el reconocimiento, la comunicación y la navegación.

El dominio “ciberespacial” esta referido a las operaciones que se llevan a cabo en el plano digital o sea que es un entorno virtual, utilizando infraestructuras de información y redes digitales a través del camino artificial del “ciberespacio”. Este dominio es uno de los más complejos de entender, ya que es difícil determinar la autoría de los responsables, llevando adelante por ejemplo operaciones de bandera falsa, con técnicas específicas que encubren y dificultan la atribución del actor.

El dominio “cognitivo” no es nuevo, pero podemos centrarnos en una etapa clave en el uso de este, por ejemplo, a través de la figura Lenin o Mao con la guerra política que llevaron adelante con la propaganda y la desinformación durante sus actuaciones. O como también Joseph Goebbels como ministro de Propaganda e Información de Adolf Hitler durante la IIda Guerra Mundial. La idea de esta “batalla de narrativas” es afectar e influir la mente humana a través de diversas técnicas tales como las operaciones de información, operaciones sicológicas y el uso/manejo de narrativas y percepciones sobre el ser humano.

Podríamos llegar a inferir que este dominio incluye las percepciones, creencias, comportamientos y toma de decisiones de los seres humanos, y la influencia externa que se puede ejercer sobre estos aspectos para modificarlos, mediante la gestión de la información de todas las personas que la utilizan (2022, García Servet, R y Calvo Alvero J L).

Continuando con la idea y para captar de una mejor manera el concepto “multidominio”, cabe aclarar, que el ejército de EUA menciona a la batalla aeroterrestre como puntapié y antecedente inicial de las mismas. Esta se introdujo durante los años 1980 en EUA para contrarrestar la amenaza que representaban las grandes fuerzas blindadas de la Unión Soviética, utilizando de manera sincronizada los medios aéreos en apoyo a las operaciones terrestres. A

su vez, nació de la experiencia de la guerra de Yom Kippur en 1973. Por lo que luego de unos años, esta doctrina vio materializado su éxito durante la primera Guerra del Golfo de 1991 con la maniobra aeroterrestre en Kuwait (León, 2017).

Para poder entender la batalla multidominio, hay que establecer un marco, así como los EUA establecieron en el combate aeroterrestre un marco de batalla profundo, cercano y de retaguardia, el marco de batalla multidominio es más extenso, atravesando todo el campo de batalla hasta inclusive la propia guarnición del adversario (Perkins, 2018).

Por lo tanto, podemos concluir parcialmente que la gran diferencia que existe entre el combate aeroterrestre (antecedente inmediato de las operaciones multidominio) y las operaciones multidominio, es que estas últimas, integra el espacio y el ciberespacio como nuevas dimensiones sin reconocer límites. Y que, además, influyen en todas las dimensiones, afectando los medios que existen en cada uno de ellos, por ejemplo, satélites.

El otro ítem para tener en cuenta, es que las operaciones no se concentran solamente en el conflicto armado, sino que pueden operar en la denominada “zona gris”, empleando el dominio cognitivo/humano y el ciberespacio (Alaníz Miranda, 2021).

Es esencial la combinación de los elementos del diseño operacional para finalmente poder llegar al centro de gravedad del adversario.

En relación con el centro de gravedad anteriormente mencionado, podemos decir que es la fuente de poder del enemigo, son las fortalezas que posee. En base a ello, a través de un análisis de los factores críticos, obtendremos fortalezas y debilidades críticas. Y, además, teniendo en cuenta este análisis se podrá diferenciar dos grandes núcleos: el interno donde se encuentra la potencia de fuego, maniobra o liderazgo del adversario y un núcleo externo, por ejemplo, la defensa aérea, los apoyos, la seguridad donde encontraremos las debilidades críticas que explotándolas llegaremos al centro de gravedad (Vego, 2000).

Asimismo, se utiliza el concepto de “operaciones” para abarcar todos los niveles de la conducción, entendiendo que todo parte de objetivos nacionales, políticos, que se transforman en estrategias para llevar adelante acciones y lograr efectos a fin de obtener la consecución del fin trazado. Es un trabajo conjunto, pero también interagencial e interdisciplinario en función del objetivo político trazado (Arce Ducassou, 2019).

Para finalizar con esta sección, podemos citar algunos claros ejemplos del uso de la tecnología y de la integración de algunos de los dominios, como por ejemplo la guerra que se libró entre Azerbaiyán y Armenia, por el conflicto de Nagorno Karabaj. Aquí quedo plasmado el uso intensivo de la tecnología dron que dio como resultado el triunfo de Azerbaiyán contra la incapacidad de Armenia para contrarrestar la superioridad en el dominio “aire”.

Es así como también durante el mencionado conflicto, se utilizaron los drones como instrumento de propaganda y guerra psicológica, utilizando las imágenes aéreas que brindaban los mismos para difundir ataques grabados desde las plataformas aéreas, publicando a través de medios y redes sociales tales como Twitter, Facebook, Telegram o You tube, dando un fuerte mensaje psicológico persiguiendo un objetivo claro: desmoralizar a las tropas enemigas (2021, Marín Delgado).

Otro claro ejemplo es lo que ocurre en la guerra Rusia-Ucrania, ya que podemos considerar que se está haciendo un amplio uso de todos los dominios, algunos en mayor o menor medida, pero todo dependiendo de las ventanas de oportunidades que se presenten. A su vez, claramente se puede identificar que el uso del ciberespacio inició mucho antes de la invasión de febrero de 2022, a través de ataques cibernéticos rusos a infraestructuras críticas ucranianas antes de la anexión de Crimea en el año 2014, los cuales prosiguieron durante la invasión en el 2022.

Otro ejemplo en este conflicto es el uso del espacio, a través de los satélites cedidos por la empresa Space X con la utilización de terminales satelitales Starlink lo cual facilitó a las

fuerzas ucranianas mantener el plano de la información y comunicaciones seguras impactando en la conciencia situacional durante la guerra. Pero durante el desarrollo del conflicto, se dice, que los mismos servicios de dicha empresa sabotearon un ataque contra la flota rusa, por no permitir a Ucrania el acceso a las redes de Starlink a fin de evitar una escalada en la guerra, esto también podría ser parte del juego de narrativas y mensajes, por lo tanto, el uso de otro dominio en la guerra: el cognitivo.

Referido a este último dominio, se vio utilizado antes de la anexión de Crimea por parte de rusia, utilizando la narrativa y el discurso, como por ejemplo el apoyo de los habitantes ruso-parlantes en el este de ucrania o también con el mensaje del presidente de Rusia, hablando de desnazificar Ucrania. Se utilizan estereotipos y realidades distorsionadas, utilizando una gran cantidad de medios de comunicación. Por consiguiente, el uso de las redes sociales es otro de los grandes problemas que tiene este conflicto.

Es claro que los dominios físicos durante la guerra se están explotando de una manera considerable, con operaciones ofensivas y defensivas clásicas. Por lo tanto, y de acuerdo con las ventanas de oportunidades que se presenten a los actores enfrentados, los dominios se están ejecutando de una manera simultánea, con mayor prominencia en algunos de ellos y atravesando todos los ámbitos y espacios, exigiendo a su vez, hacer un uso intensivo del arte y ciencia de la guerra.

## Sección III

## Vinculación de las operaciones multidominio con estrategias de disuasión, restricción de áreas y con la inteligencia.

### Disuasión Estratégica.

De acuerdo con un artículo publicado por la revista digital Global Strategy (2023), se menciona que EUA desarrolló desde el año 2021 un concepto conocido como la disuasión estratégica y la disuasión integrada, que buscan hacer frente a amenazas y riesgos en un entorno

multidominio, son herramientas del Estado para mantener la paz utilizando las capacidades de sus aliados de manera integral, logrando una disuasión estratégica efectiva.

El concepto “disuasión integrada” nace en el año 2015, como la prevención de la acción del adversario a través de capacidades físicas, cognitivas, morales creíbles y proactivas para disuadir a otros actores haciendo que se enfrente a potenciales y arriesgadas consecuencias cuando lleve adelante sus probables acciones.

Podemos también hacer una comparación con el concepto estratégico que utiliza la Organización del Tratado del Atlántico Norte (en adelante OTAN), que fue aprobado en la cumbre de Madrid (España), durante junio de 2022. El propósito principal de la OTAN es garantizar la defensa colectiva con un enfoque de 360 grados que a su vez definen tres tareas fundamentales: la disuasión y defensa, la prevención y gestión de crisis y la seguridad cooperativa. Es así como remarcan que la disuasión y la defensa es la columna vertebral de la alianza en el compromiso de defensa mutua (Ministerio de Defensa, 2022).

En la disuasión descentralizada, los EUA buscan redistribuirse por toda la región para proteger de forma efectiva sus intereses nacionales a través de una disuasión creíble. Esta doctrina tiene como objetivo ampliar la red de socios militares regionales de los EUA y prevenir posibles ataques.

Por lo tanto, se intenta conformar una fuerza integral con estos dos tipos de disuasiones en defensa de los intereses y seguridad del hemisferio occidental combinando tecnología y capacidades con otras naciones para enfrentar amenazas en distintos ámbitos tales como el convencional, cibernético e informacional.

La creación de una fuerza integral tendría implicancias de todo tipo, ya sea en el ámbito político como en el presupuestario. Obligando a definir retos en común que impactarían en el marco legal, política de defensa, doctrina, adiestramiento y recursos financieros. Tendiendo a

la interoperabilidad y estandarización de procedimientos, cuestión que se hace muy difícil de lograr.

Otro punto a tener en cuenta, producto de la creación de esta fuerza integral, está relacionada a la logística que implicaría la necesidad de incorporar nuevos procedimientos y conceptos de empleo, equipos y recursos, procedimientos para el mantenimiento, etc.

Por otro lado, el desarrollo de capacidades se incrementaría progresivamente en la interoperabilidad que se logre entre los integrantes de la fuerza integral, intercambiando información y generando inteligencia en todos los niveles tanto para las amenazas externas y riesgos internos (Barrera y Carranza, 2023).

Hay que analizar las políticas de defensa de cada país de la región ya que, aplicar este tipo de estrategia conlleva diversas aristas que se deben analizar detalladamente, las cuales impactarían de manera positiva en la seguridad nacional, pero traen consigo ciertos aspectos muy difíciles de coordinar, sincronizar y planificar.

**Restricción de áreas.**

Haciendo una comparación con lo anteriormente expuesto, podemos mencionar el concepto de capas y restricción de áreas, las cuales actuarán para **anticipar, prevenir, conjurar y repeler** toda acción perpetrada por el adversario, básicamente para negar el acceso a un espacio y si lo hace, negar el uso efectivo del mismo. Las Fuerzas Armadas Argentinas, serán empleadas en este concepto, mediante operaciones multidominio planificadas por el nivel Operacional. Me centraré básicamente en las dos primeras capas: anticipar y prevenir (EMCO, 2023, pag 3).

Relacionado a la capa “anticipar”, se trabajará sobre la alerta temprana, esta es una función importante para la inteligencia estratégica, la cual asesorará sobre futuros riesgos y amenazas a fin de prevenir ataques sorpresivos al territorio nacional.

Esta alerta proporcionará beneficios a la seguridad nacional ya que en nuestros días nos encontramos con un marco internacional fluctuante, incierto, nuevos actores y riesgos multidimensionales y transnacionales.

Para enfrentar estas estas amenazas, la tarea debe ser encarada de forma multidisciplinaria e interagencial, ya que, con una única organización dedicada a ello, dificultará el apoyo de inteligencia.

Esta capa, además, buscará de manera constante disponer de vigilancia y control de los espacios soberanos, en esta capa se iniciarán con ciertas operaciones multidominio en los espacios físicos (soberanía en el mar, tierra y aire) y en los no físicos (búsqueda permanente de posibles ataques a las propias redes informáticas y sistemas satelitales). Con el último fin de lograr profundidad estratégica (EMCO, 2023, pag 6,7).

La tecnología cobra gran importancia en esta capa, ya que diversos equipos tales como sistemas no tripulados, satélites, plataformas con sensores, la exploración y la tecnología en la protección de datos e infraestructura facilitarán la protección de los propios recursos y proporcionarán información para identificar oportunidades.

Finalmente, cabe destacar que adquiere una gran relevancia entender las relaciones de poder entre los actores. Básicamente, los medios que dispone un estado/actor son la base objetiva del poder y las relaciones entre ellos se manifiestan a través de dos maneras: la “comunicación”, donde un actor expone sus medios (base de poder) o la “interacción”, por medio de la cual el actor orienta sus medios a los fines, amenazando los intereses del otro (Campos, 2003, pag 205). La comunicación es la relación más preponderante que se llevará a cabo en esta instancia, en la capa “anticipar y prevenir”.

La segunda capa que hare referencia es la de “prevenir” la que tendrá preeminencia el dominio informacional/cognitivo, el cual se trabajará sobre la comunicación para enviar el mensaje al adversario de desistir ante su iniciativa de perpetrar la agresión.

Asimismo, en el ámbito/dominio físico (instrumento militar terrestre, aéreo y naval) deben disponer de un adecuado alistamiento, conocimiento del ambiente operacional y un apropiado plan de velo y engaño, todo ello demostrando al otro actor/es el potencial de la Fuerza ante posibles agresiones. Quiere decir con ello, que la fuerza ejecutará despliegues "disuasivos" con los medios terrestres, navales y/o aéreos mostrando capacidades del poder disponible.

Por consiguiente, en esta capa la dialéctica de voluntades estará presente, porque el mensaje originado, ya sea por el nivel político o por la estratégica, diseñado y ejecutado por el nivel operacional provocará un mensaje de respuesta. En este juego de ida y vuelta, encontraremos incertidumbre, por ende, será difícil anticipar exactamente la respuesta del otro (Campos, 2003, Anexo 2).

Si necesitamos entender ese mensaje, requiere de un profundo análisis y evaluación comunicacional que permita diferenciar la verdad del engaño, lo conocido de lo oculto de cada mensaje que se produce en esta dialéctica de voluntades.

Por tal motivo es que a través de una disertación que tuvo lugar en la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, el ministro de Defensa, el director nacional de planeamiento y estrategia del Ministerio y el jefe del Estado Mayor Conjunto de las Fuerzas Armadas, expusieron temas centrales refiriéndose al impacto de la revolución tecnología y el escenario internacional.

Finalizando el JEMCO nombró que la República Argentina se apoyará en una estrategia basada en las operaciones multidominio con sus respectivos dominios haciendo hincapié en el uso del espectro electromagnético, la preparación territorial, los sistemas aéreos no tripulados (SANT), fuerzas de operaciones especiales y las operaciones de restricción de áreas.

**Estrategia Anti-Acceso y Negación de Área (A2/AD).**

Ambos conceptos pueden ser considerados por separado, pero normalmente se asumen de manera integral. Las capacidades A2/AD buscan evitar que las fuerzas oponentes superiores

accedan o se desplacen dentro de un TO. Estas implican la capacidad de limitar la libertad de acción de una potencia militar en espacios cercanos o contiguos a una zona de interés propia.

Por lo tanto, no implica proyección de poder sino anular o limitar la capacidad de acceso del enemigo. En otras palabras, se logra generar una interrupción sostenida de las operaciones militares o incrementar sensiblemente el costo de estas (Battaleme, 2013).

La diferencia sustancial es que la capacidad A2 (anti-acceso) evita que el adversario ingrese a nuestro espacio, podemos traducirlo cuando estos están por iniciar su desplazamiento. Por lo tanto, la fuerza que quiere evitar ese acceso utiliza armamento de largo alcance, misiles cruceros, balísticos, submarinos, entre otros.

La capacidad AD (negación de área) es para limitar o dificultar su accionar una vez que iniciaron sus acciones militares e ingresaron en nuestro espacio, o sea no se pudo evitar el acceso, pero se utilizaran medios tales como Fuerzas Especiales, minado defensivo en las costas del país, uso de fuerzas irregulares, guerra hibrida, artillería para dificultar sus operaciones, entre otros.

Existen dos tipos de estrategias A2/AD, las directas y las indirectas. La primera de ella supone que se debe disponer de una capacidad militar no tan solo para disuadir sino impedir operar a un oponente superior que detente su poder contra nuestro espacio. La segunda, la indirecta, además del recurso militar se utiliza el recurso diplomático/político (Battalame, 2013).

De la misma forma que la estrategia A2/AD presenta ventajas, también demuestra limitaciones. Quiere decir que si se utiliza solamente como método defensivo no permitirá derrotar al enemigo, sino que solo lo inmovilizará, lo hará abandonar el área y desistir de su intento. En definitiva, para que derrotar al adversario, es necesario que ocurran en forma simultánea otros eventos fuera de las operaciones propias de antiacceso y negación de área (Castro Brahm, 2021).

Finalmente se exponen cinco elementos fundamentales que se combinan y son comunes en el desarrollo de las estrategias A2/AD.

1. La percepción de la superioridad estratégica del oponente. Describe a esta como la razón que motiva al defensor a desarrollar acciones de A2/AD.
2. El segundo explica sobre la ventaja de la geografía como el elemento que más influye en el tiempo y facilita el desgaste del enemigo. Se lo considera de gran importancia ya que facilita el desgaste del oponente.
3. El predominio general del dominio marítimo como espacio de conflicto.
4. La importancia de la información y la inteligencia ya sea la que se pueda obtener del enemigo, como la protección de la propia tropa (contrainteligencia).
5. Y como último elemento, expone sobre el impacto determinante de eventos extrínsecos, considerando las consecuencias de acciones fuera del teatro de operaciones, pero que afectan de manera considerable el desarrollo de las operaciones (Aquino, 2022).

**Sistemas integrados de comando y control en redes.**

Son estrategias utilizadas por países tales como EUA e integrantes de la OTAN. Por ejemplo, el sistema de mando y control conjunto en todos los dominios (Joint All-Domain Command and Control - JADC2), las Fuerzas Armadas de EUA se encuentran en proceso de desarrollo y se considera de vital interés e importancia para el instrumento militar a fin de enfrentar las amenazas que se están presentando en la actualidad.

El JADC2, es un concepto que conecta todos los sensores de datos, combatientes y los dispositivos de comunicación de las Fuerzas de EUA (Ejército, Armada, Fuerza Aérea, Infantería de Marina y Fuerza Espacial) y eventualmente aliados en una “red de redes” integrada.

El éxito de JADC2 comienza con la rápida obtención de datos, pero también exige una interpretación precisa de esos datos en tiempo real. Esa necesidad de velocidad con precisión informativa es la razón por la que JADC2 aplica Inteligencia Artificial a la gran cantidad de información obtenida en el proceso ISTAR (inteligencia, reconocimiento, vigilancia, adquisición de blancos) (JADC2 (s.f) recuperado el 23 de setiembre de 2023 de https://www.baesystems.com/en-us/definition/what-does-jadc2-stand-for).

Otro de los conceptos conocidos son los de Network Centric Warfare (guerra centrada en redes o NCW), también el sistema Network Enabled Capability (NEC) o simplemente conocido como Netwar (Fojon, 2019).

Son herramienta que tienen la capacidad de integrar sistemas, recursos y procesos en una red totalmente cohesionada, para mejorar la eficiencia y eficacia de las operaciones. Tiene la capacidad de integrar una variedad de plataformas que dispongan las Fuerzas Armadas en una única arquitectura C3I2 (Comando, Control, Comunicaciones, Informática e Inteligencia). La arquitectura se puede adaptar a cualquier tipo de plataforma, dentro de diferentes niveles (estratégico, operacional y táctico).

A su vez, se combina la información generada por los sensores para agilizar las decisiones, mejorar la sincronización, tomar conciencia de la situación y mejorar el ritmo, la letalidad y la supervivencia de las fuerzas en operaciones (Fojon, 2019).

Con esta digitalización y tecnología/ingeniería aplicada que fluirá en puestos comandos, vehículos no tripulados, equipos con sensores, dispositivos de comunicación para los soldados de primera línea, permitirá el intercambio de información segura y confiable.

Esto permite acelerar el propio ciclo OODA (observar, orientar, decidir y actuar) y así ganar tiempo, rompiendo al enemigo su ciclo. La red permite concentrar y focalizar los esfuerzos en donde es realmente necesario para lograr resultados decisivos.

La información es vital en el conflicto, de forma tal que la estrategia se centra en incrementar las necesidades de información del enemigo, aumentando su dependencia de ella y a su vez reducir su capacidad de acceso, mientras se fortalecen las capacidades propias de disponibilidad de información a través de eficientes infraestructuras.

**Inteligencia en las operaciones multidominio.**

Los niveles de la guerra (estratégico, operacional y el táctico), se relacionan con los niveles de la conducción (estratégico nacional, el estratégico militar, el operacional y el táctico), cada uno de ellos implica un problema de distinta naturaleza y un razonamiento particular y tendrá diferentes requerimientos informativos, procedimientos de trabajo y tiempos de planeamiento (EA, 2015, Cap I – 2).

Para cada uno de estos niveles, la inteligencia brindará el apoyo necesario, con la finalidad de satisfacer necesidades de conocimiento e información. En consecuencia, existirá la inteligencia estratégica nacional, la inteligencia estratégica militar, la inteligencia estratégica operacional y la inteligencia táctica.

La inteligencia es un sistema bidireccional porque cada uno de los niveles se nutre de información y conocimiento, ya sea a través de pedidos de información y ordenes de obtención para luego difundir la misma. No son compartimentos estancos, ya que es necesario el trabajo sistémico siempre en torno de la misión del elemento o nivel apoyado.

Existen factores que influirán sobre la actividad de inteligencia, el primero es la misión, ya que esta orientará las actividades de inteligencia para así desarrollar una eficiente dirección del esfuerzo de obtención (1er paso del ciclo). El segundo factor es el enemigo a través del conocimiento de los factores del orden de batalla, las actividades importantes recientes y actuales, peculiaridades y debilidades, y la eficiencia de empleo. El tercer factor es el ambiente geográfico, la información del terreno y de las condiciones meteorológicas que afectarán las operaciones propias y las del enemigo analizando los aspectos militares del terreno. Finalmente,

un cuarto factor, las propias tropas (o propios medios) esto en relación con los medios de obtención disponibles en la fuerza para las operaciones militares (EA, 2008)

Nos encontramos desarrollando el presente trabajo sobre el nivel táctico (CTTO / GUB), por ende, corresponde el apoyo de la inteligencia táctica. Pero al estar enmarcados en un TO, donde el accionar es conjunto, existirán otros factores para tener en cuenta y por supuesto las operaciones multidominio que analizamos anteriormente.

Por lo tanto, la inteligencia actuará como un sistema perfectamente cohesionado e integrado con medios de obtención y medios de apoyo al órgano de dirección de inteligencia en el CTTO, para ello se necesitan de especialistas, tal como se menciona en la doctrina propia (intérpretes de imágenes, analista de emisiones, de censura militar, entre otros) pero también con otros tipos de recursos humanos que puedan obtener, analizar y difundir aspectos relacionados al multidominio, particularmente para los dominios no físicos.

Uno de los conceptos que podría ser utilizado para potenciar el apoyo de inteligencia durante las operaciones a nivel CTTO es el proceso ISTAR (siglas en inglés que traducidas significan: Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimientos). El cual es utilizado por la OTAN y algunos países latinoamericanos, como el Ejército de Chile, por ejemplo.

El concepto ISTAR, se debe efectuar a través de “centros” o “células” (órganos de dirección, apoyados con los elementos de inteligencia (CII)), donde deben efectuar la máxima coordinación en la gestión de información, analizando todas las necesidades de informativas, vacíos e interrogantes que surjan del planeamiento en apoyo a determinada fuerza (Varela Sabando, 2014).

Esta organización es la que cumplirá con el control centralizado (principio propio de la OTAN referido a la inteligencia), que luego apoyado en un sistema automatizado de gestión y

transmisión de datos logre conectar eficientemente la información y la inteligencia producida con el usuario que tiene la necesidad de saber.

Además, en la propia doctrina del Ejército Argentino, expresa que el G2, dentro de sus funciones, en la producción de inteligencia incluirá el planeamiento para la exploración terrestre y aérea, la vigilancia de combate y la adquisición de objetivos y blancos, queda claro la relación que existe con el planeamiento y ejecución de las tareas ISTAR (EA, 2008).

Por consiguiente, el concepto ISTAR es definido por la OTAN como un "sistema de sistemas", que integra la inteligencia, la vigilancia, la adquisición de objetivos y el reconocimiento, para conseguir el máximo rendimiento de los órganos de obtención, en los pasos del ciclo de inteligencia y en el proceso de planeamiento (Varela Sabando, 2014).

Este concepto tiene una estrecha relación con el ciclo de inteligencia, ya que, durante el primer paso, en la dirección del esfuerzo de obtención, se establecen los vacíos de información y nacen los requerimientos de inteligencia mientras que en el concepto ISTAR se planificará el medio de obtención adecuado para explotar la fuente de información.

Durante el segundo paso del ciclo, obtención de la información, el concepto ISTAR llevará adelante los procedimientos para la recolección de la información pertinente ya sea el reconocimiento, vigilancia o la adquisición de objetivos.

En el tercer paso del ciclo, durante el proceso de la información, existirán momentos en donde el órgano de dirección puede diseminar información sin ser procesada, ya sea por la urgencia del usuario o del comandante. Por lo tanto, el proceso ISTAR una vez obtenida la información, los analistas de inteligencia comprueban su pertinencia y la diseminan directamente.

Y en el cuarto paso, durante la diseminación, este proceso participa de la difusión de la información o inteligencia necesaria, coadyuvando al ciclo de inteligencia. En definitiva, el proceso de inteligencia, que se llevará adelante en los centros integradores de inteligencia en

apoyo al órgano de dirección, centralizará la información y diseminarán inteligencia de acuerdo con su pertinencia, confiabilidad y exactitud, a fin de facilitar la futura toma de decisiones.

## Sección IV

## Conclusiones parciales del primer capítulo.

En base a lo expuesto y analizado en la introducción y en el desarrollo del presente capítulo, lo que se buscaba era determinar la influencia que tienen las operaciones multidominio sobre el apoyo de inteligencia en el CTTO. Por lo tanto, se pueden arribar a las siguientes conclusiones:

Tiendo en cuenta el marco legal de la República Argentina, especialmente lo estipulado en la DPDN 2021 sobre potenciales amenazas a recursos y zonas estratégicas que podrían configurar futuros escenarios complejos, sumado a la trascendencia del avance tecnológico y la capacidad de brindar alertas tempranas efectivas mediante una amplia variedad de sensores y plataformas adecuadas, integradas en un eficiente sistema de comando y control exige, una transformación en nuestras perspectivas, estrategias y conceptos de empleo que implicaría profundos cambios de mentalidades en todos los niveles de la conducción, desafiando paradigmas establecidos a fin de adoptar innovadores conceptos de empleo para las fuerzas armadas.

En relación con lo anterior y específicamente a ciertas restricciones que existen en el campo normativo, la inteligencia militar no podría actuar ante una amenaza híbrida o acciones que se desarrollen en la zona gris del conflicto, ya que tendrá mayoritariamente, connotaciones cibernéticas y operaciones de información, estaríamos en contra de la reglamentación de la Ley de Defensa. Otra cuestión es la resolución ministerial del año 2006, donde prohíbe el trabajo de los organismos de inteligencia para desarrollar actividades en el dominio cognitivo, siendo este el que atraviesa a todos los ámbitos de las operaciones multidominio. Por lo tanto, se deben revisar a conciencia este cuerpo legal para permitir a las Fuerzas Armadas estar preparadas ante

un eventual conflicto moderno donde, por supuesto, estos ámbitos estarán plenamente desarrollados.

En efecto, las operaciones multidominio están transformado el pensamiento militar de todo el mundo e impactando directamente sobre el campo de batalla. Ya que el avance disruptivo de la tecnología, sumado a la aparición de nuevas amenazas y actores no estatales, presentan un cambio que orienta a las altas esferas de la conducción a replantearse ciertas estrategias y tácticas para enfrentar las situaciones que se presentan en este tipo de operaciones.

En definitiva, podemos inferir que las operaciones multidominio están íntimamente vinculadas con la tecnología y básicamente se busca disponer e integrar de toda la información e inteligencia, aprovechando las ventanas de oportunidades y respondiendo de manera eficiente, veloz y asertiva sobre la amenaza que se presente en el TO.

En este contexto, la inteligencia juega un rol fundamental, y centrándonos en el nivel táctico, la misma debe disponer de ciertas capacidades tales como: la rapidez y flexibilidad ante las situaciones que se plantean, con una eficiente capacidad de obtención y análisis casi en tiempo real (debido a la velocidad de las operaciones), la interoperabilidad y el trabajo interagencial de la mano de la tecnología, en donde el concepto ISTAR cobra especial relevancia. Esta capacidad para integrar la vigilancia, el reconocimiento, la adquisición de objetivos con la inteligencia es esencial en las operaciones multidominio. En efecto facilita el comando y control del CTTO lo que permite a un comandante táctico no solo anticiparse, con la información e inteligencia necesaria, sino también a actuar frente a la amenaza configurada, adaptándose a situaciones en constante evolución propias de este tipo de conflicto.

Por lo tanto, el sistema de inteligencia debe ser integral, interconectado a través de sistemas afines en cada nivel de la conducción con ciertos especialistas (sobre todo en los dominios no físicos) para satisfacer a las necesidades informativas que se plantean, en este caso

en particular, del comandante y del estado mayor del CTTO, creando una consciencia situacional acorde, brindando el apoyo de inteligencia necesario para el proceso de toma de decisiones durante las acciones militares.

La inteligencia en este nivel tiene una exigencia muy grande, ya que se enfrenta a todos los dominios: físicos y no físicos. Debe obtener información con los diferentes tipos de inteligencia (inteligencia humana, de imágenes, de emisiones (en sus dos formas la inteligencia electrónica y de comunicaciones) para integrarla con otras fuentes y medios de obtención a fin de producir inteligencia. Por lo tanto, podemos apreciar la injerencia que tiene el dominio terrestre, aéreo, electromagnético y espacial lo que permite diferenciar y resaltar la falencia que existe en otros tipos de dominios en la actualidad.

En efecto, hay campos donde hoy la inteligencia táctica en apoyo al CTTO, no se encuentra en capacidad de asesorar y asistir. El claro ejemplo es en el ciberespacio y el cognitivo. Por consiguiente, nuestros especialistas deberían capacitarse en técnicas y procedimientos afines a dichos dominios (conforme a lo que dicten las normas) para disponer de nuevas capacidades abarcando así, todos los ámbitos físicos y no físicos, logrando con ello que los especialistas del CII y los medios de obtención del sistema de inteligencia respondan eficientemente a las exigencias que presenta el combate moderno.

Como se puede apreciar, las operaciones multidominio representan un ambiente VICA (volátil, incierto, complejo y ambiguo) donde el sistema de inteligencia debe identificar las amenazas, realizar una correcta apreciación de situación de inteligencia, analizando todas las variables del ambiente operacional (factor muy relevante a tener en cuenta), respondiendo los requerimientos que surjan de los vacíos de información del comandante y del estado mayor, especializarse, adquirir nuevas tecnologías e integrarse con todo el sistema, actuando de manera holística, anticipada y eficiente en pos del cumplimiento de la misión asignada.

## Capitulo II.

## El Sistema de Inteligencia a nivel GUB y CTTO, su actual y futuro empleo durante las operaciones multidominio.

El presente capítulo tiene por objetivo analizar y describir el actual concepto de empleo, capacidades y limitaciones del sistema de inteligencia en el nivel CTTO y GUB, para determinar un nuevo concepto de empleo y capacidades a fin de establecer características que debería disponer un sistema de inteligencia en el nivel CTTO a fin de enfrentar las exigencias que imponen las operaciones multidominio.

El capítulo se divide en cuatro secciones, donde me respaldaré en la doctrina propia, con los reglamentos de inteligencia específicos, reglamentos conjuntos, artículos y publicaciones de otras fuerzas armadas, tanto de la región como extrarregional.

La primera sección tratará sobre conceptos generales de la inteligencia táctica y el nivel de la conducción táctica, observando sus principales características y diferencias existentes dentro del mismo nivel, entre GUC, GUB y CTTO.

En la segunda sección, mencionaré los conceptos y características del sistema actual de inteligencia materializado por el B Icia y el DIC. Sus capacidades y características distintivas como así también algunas limitaciones prioritarias, lo cual dará pie a la posible organización de un sistema de inteligencia multidominio.

En la tercera sección haré referencia a las disciplinas que son utilizadas mayoritariamente en los dominios no físicos que pueden afectar este nivel de la conducción y que son necesarias dentro de un elemento de apoyo de inteligencia para la toma de decisiones en las operaciones multidominio, como así también algunos medios fundamentales que debería disponer dicho sistema.

Finalmente, en la cuarta sección, presentaré las conclusiones parciales del presente capítulo.

## Sección 1

## Conceptos Generales.

### Principios de la inteligencia.

Existen ocho principios que la OTAN utiliza para desarrollar la función inteligencia durante las operaciones militares, a su vez, se expresa que son tan genéricos que tienen un valor universal para cualquier tipo de inteligencia. Estos principios son los siguientes: control centralizado, oportunidad, explotación sistemática de las fuentes, objetividad, accesibilidad, satisfacción de las necesidades del comandante, protección de la fuente y revisión continua (Instituto Español de Estudios Estratégicos, 1991).

Asimismo, nuestra doctrina marca principios y normas para la inteligencia que van a influir tanto en la organización y dirección como en la propia inteligencia producida. Podemos hacer una analogía con las anteriormente nombradas, las cuales van a ser necesarias para el proceso de planeamiento y ejecución de la función inteligencia. Las mismas se detallan a continuación:

Normas para la organización y dirección: seguridad (secreto en el accionar) flexibilidad (adaptación a situaciones cambiantes), iniciativa (adelantarse a las acciones del enemigo), especialización (conocimiento específico, logrando eficacia) y autonomía (contar en todo momento con los recursos necesarios) (EA, 2008, pag 3-5).

Normas para la inteligencia producida: oportunidad (disponible en el momento preciso), continuidad (acción ininterrumpida tanto en la paz como en la guerra), objetividad (imparcialidad y neutralidad en las actividades de inteligencia, mediante el uso de la ciencia, evitando sesgos y prejuicios), claridad (cualidad en el texto, redacciones sencillas y concretas, empleando la lógica y evitar ambigüedades), reserva (tiene que ver con la necesidad de saber y la conciencia de contrainteligencia) e integridad (la inteligencia producida debe ser lo más

completa posible, esta norma debe ser balanceada con la norma de la oportunidad) (EA, 2008, pag 3-5).

Claramente podemos distinguir que hay normas/principios que se repiten tales como la "objetividad" y la "oportunidad", también se puede relacionar la "continuidad" con la "revisión continua" y finalmente un principio fundamental es el "control centralizado".

Cabe destacar que, si bien los principios utilizados por la OTAN son nombrados para su uso en la inteligencia operacional, pueden materializarse en la inteligencia táctica en combinación con los principios y normas anteriormente detallados. Se destaca la importancia del "control centralizado", ya que evitará/disminuirá las duplicaciones y esfuerzos innecesarios, asegurando el uso eficaz de los medios. En efecto, durante la guerra de Malvinas este principio no se tuvo en cuenta, ya que al no haberse conformado un órgano de dirección a nivel TO, cada fuerza disponía de sus elementos y realizaban todos los procedimientos y actividades propios de la obtención de información y su posterior análisis en compartimentos estancos.

**Inteligencia táctica y el nivel táctico.**

La inteligencia táctica será el nivel de inteligencia que proporcionará el conocimiento, sobre el enemigo real (capacidades y debilidades) y el ambiente geográfico donde se desarrollarán las acciones militares durante el planeamiento y el desarrollo de estas, a fin de satisfacer necesidades del comandante para adoptar resoluciones afines que coadyuven el planeamiento y la conducción de las operaciones (EA, 2008, pag 5 – Anexo 1).

Con respecto a sus características, la inteligencia táctica se identifica por la rapidez en la elaboración de productos afines a la toma de decisión, por lo tanto, la inteligencia actual y básica son las que estarán en permanente acción, compartiendo la misma con todo el sistema de inteligencia.

Espacialmente, la inteligencia, está delimitada a la Zona de Responsabilidad e Interés de la fuerza que apoya. En este contexto, la extensión de la zona variará según el tipo de fuerzas

involucradas, su dimensión y las particularidades de las operaciones planificadas. Teniendo en cuenta el espacio que ocupará el CTTO dentro del TO que se establezca oportunamente.

Temporalmente, la inteligencia táctica trabaja en el corto plazo, no así la inteligencia Operacional que debe enfocar su trabajo en el mediano plazo para enfrentar los tiempos de guerra y durante la paz, trabajar en el mediano y largo plazo.

En este nivel, la información e inteligencia debe ser lo más detallada y completa posible, en este ambiente nos encontramos en el plano de las "probabilidades", donde nos enfrentamos a futuros alternativos porque estamos en contacto con las fuentes. Si hacemos una breve comparación con el plano Operacional podemos inferir que existe un abanico de futuros (orden de "posibilidades"), por lo tanto, es un ambiente con mayor incertidumbre.

Justamente, la ventaja más grande que tiene la inteligencia táctica es que mantiene permanente contacto con las fuentes o sea con la realidad del conflicto en desarrollo, pero con un gran inconveniente, la falta de tiempo, en consecuencia, necesitamos un sistema de inteligencia rápido, eficiente, tecnológico y especializado, que apoye el proceso de toma de decisión para cumplir con el objetivo de adelantarnos al ciclo OODA del enemigo a fin de obtener una ventaja táctica sobre el mismo.

Finalmente, debe existir una recurrencia e intercambio de información/inteligencia entre la inteligencia estratégica y la táctica esto permitirá dar mayor fluidez y flexibilidad al sistema. Particularmente, dentro del ámbito táctico, los sistemas de inteligencia deben conectar e integrarse, es uno de los objetivos del multidominio, disponer en un tiempo perentorio de la información/inteligencia para apoyar la toma de decisiones e influir sobre el enemigo. Esto se logrará con un adecuado elemento de apoyo al órgano de dirección de inteligencia que a través de su G2/C2, expondrá, en un "tablero" digital táctico, los fundamentos y elementos de juicio necesarios al estado mayor y al comandante para la resolución de un problema militar.

Por otro lado, y relacionado a los niveles de la conducción, particularmente el nivel táctico abarcará desde los niveles superiores, hasta los inferiores (conocidos anteriormente como táctica superior y táctica inferior respectivamente, términos en desuso dentro de la doctrina del EA). En los niveles superiores de la táctica, se encontrará el CTTO y la GUB. En los niveles inferiores de la táctica, el nivel GUC (Páez, 2022).

Por lo que resulta esencial establecer, como primera medida, la diferencia entre estos dos grandes niveles dentro de la táctica, dejando en claro que la inteligencia tendrá diferentes actividades y enfoques en cada uno de ellos.

Para hacer una rápida diferenciación entre la GUC y la GUB, podemos resumir que en el nivel GUC los espacios utilizados son menores, la naturaleza del problema es diferente, la situación será más organizada y estructurada, es un ámbito específico, un riesgo calculado mínimo y un escenario con mayores certezas gracias a la planificación de los niveles superiores. Finalmente, este nivel es apoyado por una Ca Icia con sus elementos de obtención y su elemento de apoyo (CII) al órgano de dirección de inteligencia (Div II – Icia, materializado por el G2) de la GUC.

Mientras que, en el nivel GUB, se puede apreciar que el problema se complejiza considerablemente, los tiempos de planeamiento serán mayores, existirán espacios vacíos (si se conforman TO no lineales) y no hay definición exacta, por lo tanto, los espacios serán mayores a los que se manejan en el nivel GUC. En consecuencia, se necesita de un importante intercambio de información entre todo el sistema de inteligencia, particularmente el proveniente desde los niveles más bajos, que disponen de mayor grado de detalle. Esto estará dado por las Compañías y las Secciones Inteligencia que gracias a la cohesión que existe dentro del sistema, facilitarán los futuros análisis que se presenten, por ejemplo, referido a los aspectos militares del terreno y los efectos, que servirán a la GUB para su intervención en el futuro TO que se designe.

El nivel CTTO, es la última instancia que representa el máximo nivel de conducción táctica previsto en la doctrina del Ejército Argentino. Las demandas de información crecerán en calidad y cantidad. Un rasgo distintivo de este nivel es su interacción con el nivel operacional de naturaleza conjunta y es muy claro el asesoramiento directo que realiza el comandante del CTTO al comandante del TO en el empleo de las fuerzas terrestres.

La información en este nivel será voluminosa y difícil de procesar, si no se cuenta un elemento preparado y adiestrado para tal fin, será un proceso complicado. Claramente los espacios serán aún mayores, debiendo atender todas las direcciones operacionales ordenadas por el comandante del TO. Asimismo, podrán recibirse responsabilidades fuera del área de combate, como en la zona de comunicaciones, zonas de seguridad, o comandos territoriales. (Páez, 2022)

Un factor distintivo y muy importante a tener en cuenta entre estos tres niveles de la táctica, es el análisis de los factores del ambiente operacional (ya mencionados) en donde la GUB y el CTTO deben realizar un exhaustivo estudio de estos, ya que es fundamental entender que los mismos son de vital interés para el futuro planeamiento y ejecución de las operaciones en estos niveles de la conducción.

En definitiva, a medida que incursionamos en los mayores niveles de la conducción, la inteligencia se ve particular e íntimamente relacionada con las características de las operaciones multidominio. Cuanto menor sea el nivel de la conducción menos dominios serán abordados y en consecuencia la simplicidad caracterizará a los órganos de dirección de inteligencia.

## Sección II

## El sistema de inteligencia en la GUB y en el CTTO.

**B Icia en apoyo a la GUB.**

Existen tareas principales de la inteligencia táctica, que un comandante en el nivel GUB debe tener en cuenta, tales como: la actualización permanente de la situación del enemigo y del ambiente geográfico de interés, la contribución al análisis de objetivos y la seguridad de la fuerza (EA, 2017).

En el mismo reglamento menciona la "batalla multidimensional", la cual se debe considerar para la organización del campo de combate, sea lineal (contiguo) o no. Donde se van a desarrollar las acciones en todas las dimensiones de forma coordinada y sincronizada.

Dentro de las capacidades del B Icia, se expresa que son la de obtener información de las áreas de proyección, territorial y de combate (pero en la zona de combate del teatro), producción de inteligencia, apoyar y reforzar elementos de las GGUUCC, obtener información a través de diferentes medios (VANT, humanos con interrogadores y examen de material y efectos, electrónicos (sensores terrestres y radares), interpretación de imágenes y apoyo meteorológico (EA, 2017, pag II – 2).

Por lo tanto, las capacidades del B Icia deben estar acorde a los mayores tiempos que necesita un CTTO para resolver los problemas militares complejos que se presenten, en definitiva, hacer que las acciones se ejecuten en tiempo y forma para que la recurrencia de información con dicho nivel sea llevada adelante sin complicaciones.

La organización para el combate del B Icia, se materializará a través del SIC (conformado por la compañía comando y servicio, el CII, una compañía de inteligencia de combate y una compañía de inteligencia) y el STAI (a través de la Ca Icia).

La GUB operará con grandes distancias a cubrir durante las operaciones, por lo que se organizarán, de manera transitoria dentro del SIC, equipos de sección o de compañía los cuales van a apoyar los esfuerzos de la división, ya que las Subunidades del B Icia difícilmente puedan brindar el apoyo necesario a dichos esfuerzos de manera reunida.

El concepto de empleo del B Icia se verá reflejado de la siguiente manera:

- A través de apoyo directo a una GUC con parte de sus medios.
- A través del apoyo directo de las fuerzas que se establezcan en la zona de seguridad estratégica, con parte de sus medios (integren o no la Z Comb).
- A través de apoyo general a la GUB con la totalidad o parte de sus medios.
- A través del refuerzo de los elementos de inteligencia orgánicos de las GUC integrantes del OB de la división, con parte de sus medios (EA, 2017, pag II – 9).

Referido a los medios de obtención, este nivel requerirá una estrecha integración y estructuración de todo el sistema, no solo con los medios del TO, sino también con aquellos que, externos, tengan responsabilidad de apoyo o aquellos que se encuentren dentro del TO pero que no sean orgánicos al mismo (EA, 2017, pag I - 6).

Esto se debe a la escasa cantidad de medios de obtención y la autonomía para operar. Ya que, el OB de la GUB se organizará con los elementos que estén a disposición para la actividad de obtención (exploración, artillería (Observadores Adelantados), Ingenieros (sección reconocimiento) y otros elementos de inteligencia puestos en apoyo.

El eje principal de apoyo de inteligencia estará dado por el CII, el cual va a guiar todas las actividades del sistema de inteligencia, conformando el elemento de apoyo al órgano de dirección, o sea el G2 de la GUB, recibiendo información e inteligencia del sistema de inteligencia subordinado (Ca Icia) y produciendo/diseminando inteligencia al nivel GUB, escalones adyacentes y superiores.

Existe una particularidad que hay que resaltar, y es que, cuando la GUB deba operar como CTTO, el B Icia solo estarán en capacidad de apoyar la zona de combate. En la zona del interior, el apoyo lo brindarían elementos de inteligencia no empeñados dentro del TO y en la zona de seguridad estratégica, se recibirá la agregación de Secciones de Inteligencia conformando un CII disminuido. Como así también se podrá recibir fracciones en apoyo al B

Icia, referidas a cuestiones de inteligencia técnica, de señales, logística o geoespacial (EA, 2017, pag I-7)

**DIC en apoyo al CTTO.**

Como se señaló anteriormente, es el elemento de inteligencia que apoyará al CTTO. Dentro de sus tareas, una de la más importantes es proporcionar información e inteligencia sobre los grandes espacios cuando se conforme el TO e identificando, a su vez, como el enemigo empleará sus tácticas y procedimientos para alcanzar sus objetivos, materializando así sus intenciones e intereses.

Para el concepto de empleo del DIC, podrán diferenciarse las siguientes variantes de empleo:

- En apoyo del CTO (Comando Teatro de Operaciones) como un todo (nivel Operacional).
- En apoyo del CETO (Componente Ejército Teatro de Operaciones, hoy Componente Terrestre del Teatro de Operaciones) como un todo (misión táctica superior).
- En apoyo de una GUB (misión táctica superior).

Cabe aclarar, que en la actualidad el concepto de empleo del DIC estará dirigido a brindar el apoyo de inteligencia al nivel CTTO (anteriormente nombrado CETO).

Asimismo, se establece que el fin último del apoyo de inteligencia a las operaciones de combate están dirigidas a blancos de inteligencia de alta prioridad, es por ello que se establece que para el nivel táctico superior (hoy el nivel CTTO), la obtención de información estará centrada a la reunión de fuerzas y sus desplazamientos, dispositivos enemigos, instalaciones logísticas, trabajos de organización del terreno, dispositivos de defensa aérea y la ubicación de puestos comandos (EA, 2007, pag 22 y 23).

Dentro de sus capacidades, y relacionado a los medios de ejecución, el DIC podrá ejecutar: exploración, reconocimiento, vigilancia de combate, adquisición de objetivos, a través de patrullas, VANT, y radares de vigilancia. Como así también, escucha radioeléctrica, interrogatorios de prisioneros de guerra, interpretación de imágenes, apoyo meteorológico básico e inteligencia del terreno a través de Sistemas de Información Geográfico (en adelante SIG) (EA, 2007 pag. 1 y 2).

A continuación, se expone un cuadro comparativo para resumir las capacidades actuales del B Icia y del DIC, lo que daría pie a la propuesta de nuevas capacidades para enfrentar los dominios actuales de este tipo de operación.

**Tabla 1**

***Cuadro Comparativo de las capacidades actuales de los elementos de inteligencia.***

| Dominio | DIC | B Icia | Nueva capacidad |
|---|---|---|---|
| Terrestre | Exploración, reconocimiento, adquisición de objetivos y vigilancia de combate con patrullas de largo alcance.<br>Interpretación de imágenes | Implementación de MSCI.<br>Interpretación de imágenes | Incorporación del concepto ISTAR con tecnología para el hombre y plataformas terrestres |
| Aéreo | Exploración, reconocimiento, adquisición de objetivos y vigilancia de combate con VANT<br>Interpretación de imágenes | Obtener información con VANT<br>Interpretación de imágenes | Incorporación del concepto ISTAR con tecnología para plataformas aéreas |
| Marítimo | -- | -- | Incorporación y/o coordinación con un especialista en el dominio marítimo para integrar información pertinente para el CTTO |
| Espacial | Empleos de Sistemas de Información Geográfica (SIG)<br>Interpretación de imágenes | Empleo del nodo SIGEA<br>Interpretación de imágenes. | Empleo de inteligencia artificial junto con los programas SIG para potenciar capacidades |
| Electro-magnético | Escucha radioeléctrica. | Escucha radioeléctrica. | Puestos móviles de escucha.<br>Inteligencia artificial para facilitar el análisis |

| | | | |
|---|---|---|---|
| | | | y la toma de decisiones. |
| Ciber espacial | -- | -- | Analistas de ciberinteligencia<br>Inteligencia de Fuentes Abiertas |
| Cognitivo | - Interrogatorios de prisioneros de guerra.<br>- Examen de documentos y materiales<br>- Análisis y apoyo meteorológico | - Interrogatorios de prisioneros de guerra.<br>- Examen de documentos e inteligencia técnica.<br>- Seguridad PMI<br>- Análisis y apoyo meteorológico | Medios de ejecución y analistas COSACO<br>Analistas específicos sobre factores del ambiente operacional (sobre todo influencia de la política, medios de comunicación y factores sociales) |

Fuente: elaboración propia.

Se puede apreciar que estas capacidades están mayoritariamente relacionadas con los dominios físicos (terrestre, aéreo) o a procedimientos clásicos. Sin embargo, se deduce que existirían otras capacidades no especificadas, posiblemente debido a la fecha de publicación del reglamento citado, otras tecnologías existentes de la época o por la falta de doctrina sobre las operaciones multidominio. Con lo anteriormente expresado, no se está observando como una crítica al reglamento sino todo lo contrario, se está investigando para reforzar los conceptos y adaptarlos a la realidad de nuestros tiempos.

Por lo tanto, es importante resaltar que el único elemento de inteligencia a nivel CTTO, debe actualizar ciertas capacidades relacionadas al uso de la tecnología y particularmente a los dominios no físicos.

Relacionado con el medio de apoyo al órgano de dirección de inteligencia (Departamento Inteligencia del CTTO), no se encuentra estipulado en este nivel de la conducción, ya que el CII tiene otro concepto de empleo. En primer lugar, se establece que el jefe del CII será el oficial de operaciones ya que dentro de sus funciones es la de integrar la

información producida por los medios del DIC. Otra cuestión para tener en cuenta es que la responsabilidad primaria de instalar y operar el CII es de la Compañía Comando del DIC.

Además, cuando el puesto comando del DIC se divida en un puesto comando táctico y en un secundario, el CII funcionará en el táctico donde se llevará el comando y control del DIC, básicamente, se planificarán, recibirán e impartirán ordenes de obtención y pedidos, se ejecutará la supervisión y actualizará la situación de la propia fuerza y del enemigo. Aquí se configurarán dos módulos, en uno de ellos se llevará a cabo la tarea de asesoramiento y asistencia al jefe del DIC y en el otro se encontrarán los operadores de las terminales de ambiente geográfico y orden de batalla llevando la carta de situación de forma actualizada (EA, 2017, pag 16 - 17).

En este nivel, el responsable de procesar la información recibida y diseminar inteligencia resultante, lo realizará el Puesto Comando del DIC, a través del CII que formará parte de dicho puesto comando.

Por lo tanto, y a diferencia del CII del B Icia, no está definida claramente la misión, función y capacidades del CII en este nivel. El CII del B Icia esta divido por grupos de trabajo (situación y análisis de combate) con analistas en ambiente geográfico, orden de batalla, interpretación de imágenes, meteorología, medidas de seguridad contrainteligencia, operaciones en desarrollo y futuras con listas de capacidades y actividades. En este nivel se infiere que el CII debe actualizar y agregar capacidades.

En definitiva, en este nivel, hay un quiebre en el sistema de inteligencia debido a que, el apoyo al órgano de dirección se viene materializando desde los niveles más bajos (CII de la Ca Icia en apoyo a la Div II – Icia de la GUC y el CII del B Icia en apoyo al Dpto II – Icia de la GUB) y en este nivel no se ve materializado eficientemente. Este hilo conductor que une los escalones de los sistemas de inteligencia del menor al mayor nivel facilita la recurrencia, la integración y el apoyo a la toma de decisiones en cada nivel de la conducción.

## Sección III

## Disciplinas y medios de inteligencia.

### OSINT.

Inteligencia de Fuentes Abiertas (en adelante OSINT), también conocida en la OTAN y EUA como Open Source Intelligence. Como una primera aproximación a la definición citaremos lo que expresa el Departamento del cuartel general del Ejército de los EUA a través de un Manual de Campo y que es el siguiente:

> La Inteligencia de fuentes abiertas es una inteligencia que se produce partiendo de información pública disponible y es obtenida, utilizada y difundida de manera oportuna a una audiencia adecuada con la finalidad de responder y abordar un requisito de inteligencia específico (Ejército de Estados Unidos, 2023).

Se puede considerar que la OSINT es mucho más eficiente, económico y seguro en comparación con otros tipos de inteligencia. En la actualidad, basta con algún equipo informático, una conexión a internet y por supuesto como muy importante, la capacitación del analista OSINT.

En relación con las fuentes OSINT, se puede considerar todo tipo de publicaciones en formato papel (diarios, revistas, folletos), medios tradicionales de información y comunicación (radio, televisión), fotografías, vídeos, imágenes, especialmente útiles si son en directo y geolocalizadas, información geoespacial, imágenes y vídeos tomados desde el espacio o el aire mediante drones o satélites y por supuesto internet, la Deep Web y la Dark Web consideradas la fuente de información por excelencia (foros, redes sociales, repositorios de video, motores de búsqueda, blogs, etc) (Lisa Institute, 2020).

Según lo publicado por la página de LISA Institute, existen tres métodos para la obtención: la obtención pasiva (obtener la información sin que se detecte nuestra presencia, sin

interactuar con el objetivo), la obtención semi-pasiva (aquí se genera tráfico a través de consultas, pero con una mayor discreción) y la obtención activa (hay interacción con el objetivo de la búsqueda, por lo tanto, la discrecionalidad se pierde) (Lisa Institute, 2020).

Por supuesto, hay que tener en cuenta en el momento de implementar ciertos tipos de búsqueda, el marco legal vigente en el propio territorio con respecto a ello. Pero inicialmente para una búsqueda de información pública no reviste problemas.

Los órganos de inteligencia siempre han utilizado las fuentes abiertas en la producción de inteligencia. Internet ha proporcionado un rápido crecimiento de las fuentes de información y un fácil acceso a las mismas.

El uso de las redes sociales, programas y plataformas de todo tipo, influyen en este tipo de inteligencia porque se nutren de las mismas, un claro ejemplo es el uso de Google Maps (solo para mencionar un programa) durante la invasión de Rusia a Ucrania en febrero de 2022, el cual brindó información de los movimientos rusos gracias a diversos análisis que realizó la inteligencia occidental, además en ese entonces Google deshabilitó algunas funciones para no poder acceder al monitoreo del tráfico en rutas ucranianas en tiempo real.

A su vez, existen diferentes tipos de programas los cuales se usan de manera integrada para cruzar datos, por ejemplo, programas de reconocimiento facial que también fueron utilizados durante el conflicto mencionado para identificar soldados rusos gracias a información existentes en las redes sociales, esto potenciado con inteligencia artificial, facilita el trabajo de la inteligencia.

Por lo tanto, podemos inferir que este tipo de inteligencia es un instrumento muy importante para poder entender el TO donde se llevarán a cabo las operaciones, ya que es a menudo más útil que cualquier otra disciplina para observar, obtener analizar y entender actitudes públicas y el apoyo de la población (en redes sociales, por ejemplo) hacia el instrumento militar propio o del adversario.

Pero hay que tener en cuenta que para esta disciplina se presentarán diversos problemas: en primer lugar, ofrece demasiada información (volumen de datos importante) como segundo aspecto es fundamental asegurarse de la fiabilidad de las fuentes, realizando un exhaustivo y correcto análisis y valorización de la información, trabajo clave del analista de inteligencia (Cárdenas, 2022).

En definitiva y a modo de cierre de la disciplina OSINT, podemos inferir que la tecnología nuevamente tiene una influencia directa, porque pone a disposición diversas fuentes gracias a la hiperconectividad que existe en el mundo. Asimismo, permite anticipar amenazas dado que, con un monitoreo constante de redes sociales, blogs, foros, publicaciones y/o discursos, se logrará entender el contexto. Sirve tanto para la paz como en la guerra, por lo tanto, es necesario preparar analistas OSINT dentro de la Fuerza y particularmente en un órgano en apoyo al G2 de un CTTO, donde enfrentará diversos factores.

**Ciberinteligencia.**

En primer lugar, debemos tener en claro que este concepto se desarrolla en el ámbito del ciberespacio, el cual podemos decir que el mismo es un ámbito virtual, pero tiene su parte física, en donde se llevan a cabo diversas actividades de procesamiento, almacenamiento digital que a través de las redes, software y dispositivos electrónicos el cual se da gracias al empleo de las TICs (EMCO, 2019).

El ciberespacio dispone de tres capas a saber: la capa social (personas físicas e información), la capa física (componentes de red física) y la capa lógica (servicios y arquitecturas de redes), por consiguiente, es un dominio no físico con impacto directo en el dominio físico.

A su vez, hay que diferenciar entre ciberseguridad y ciberdefensa, la primera de ellas es una política nacional enfocada en la protección de las infraestructuras críticas (IICC) con el fin último de obtener la libertad de acción en el ciberespacio, mientras que el segundo concepto se

refiere a lograr esa ciberseguridad para prevenir y contrarrestar las acciones que provienen del ciberespacio que afecten las infraestructuras críticas. Estas y otras IICC serán asignadas al ministerio de defensa para su protección (Comando Conjunto de Ciberdefensa, 2023).

A su vez se deben preservar las propias infraestructuras del instrumento militar las cuales son: sistemas de comando y control, sistemas de armas, sistemas de control, sistemas de comunicaciones y sistemas Informáticos.

Por otro lado, cabe destacar que esta disciplina está íntimamente relacionada con la anterior (OSINT), porque están atravesadas por las TICs y sobre todo porque operan en el dominio del ciberespacio, ya que los técnicos en ciberinteligencia aplicaran métodos de distinta índole y uno de ellos será empleando la OSINT.

Nos aproximaremos a su definición; en el reglamento conjunto menciona que la ciberinteligencia está relacionada a aquellas actividades de inteligencia realizadas en o desde el ciberespacio (EMCO, 2019).

Otra definición según un artículo de un Centro de Estudios Chileno expresa que, la ciberinteligencia es un conjunto de actividades que apuntan a obtener conocimiento previo de amenazas y vulnerabilidades a los sistemas de comunicación de información a través de una variedad de medios técnicos (Centro de Investigaciones y Estudios Estratégicos, 2018).

En un TFI de la Escuela de Guerra del Ejército Argentino (Organización Militar de Inteligencia como elemento de asesoramiento y asistencia a la toma de decisiones antes los ciberataques a nivel componente Ejército), menciona que la ciberinteligencia es un proceso de obtención y análisis de información dentro del ciberespacio, para localizar y predecir capacidades, intenciones y acciones cibernéticas que ejecuta el ciberatacante, con la finalidad de apoyar la toma de decisiones (Escribano, 2022).

En un trabajo expuesto en la revista Visión Conjunta de la Escuela de Guerra Conjunta de las Fuerzas Armadas de la República Argentina (la ciberdefensa y la ciberinteligencia

militar), mencionan diversas interpretaciones del término ciberinteligencia (CYBINT), y a continuación expondré algunos de ellos para un mejor entendimiento de la disciplina:

> Se entiende como la proyección en el ciberespacio de las funciones tradicionales de captación de datos que lleva a cabo un servicio de inteligencia, situándola en el mismo plano que otras actividades de obtención como, por ejemplo, la inteligencia de señales (SIGINT) o la inteligencia de fuentes abiertas (OSINT) (Casarino y Ortiz, 2019, pag 50).

Desde el punto de vista organizacional se refiere al conjunto de acciones que una organización de inteligencia ejecuta para impedir que adversarios, servicios de inteligencia hostiles o grupos delictivos/criminales obtengan datos digitales valiosos/sensibles o inteligencia mediante sistemas informáticos, redes y equipos (Casarino y Ortiz, 2019)

> Considerado desde el punto de vista operacional, se refiere a las operaciones de ciberinteligencia, vigilancia y reconocimiento que comprenden actividades en el espacio cibernético para reunir inteligencia activa de los sistemas del blanco y del adversario requeridos para apoyar las operaciones militares (Casarino y Ortiz, 2019, pag 51).

Es una disciplina muy técnica y específica, que requiere una especialización particular. Por lo cual, basándome en un Trabajo Final de Carrera de Especialización en Seguridad Informática (2020), se mencionarán algunos de los métodos que utilizan en esta disciplina, para así demostrar su grado de detalle, especificidad y tecnicismo que esta demanda:

Modelo de diamante: El modelo proporciona oportunidades para integrar la inteligencia en tiempo real para la defensa de la red, consta de cuatro fases, las cuales coinciden con las cuatro puntas de un diamante, el atacante (quien ataca, como es su modus operandi, su motivación), las capacidades (vectores de infección, técnicas, tácticas y procedimientos (TTP)), las infraestructuras (vectores, nodos, dominios) y las victimas (aquellos sectores que afectan).

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) o sea Tácticas, técnicas y conocimiento común del adversario: categoriza y describe tácticas, técnicas y procedimientos (TTP) utilizados por adversarios contra sistemas específicos, como así también amenazas y la identificación de las vulnerabilidades de los sistemas informáticos (Martínez, 2020).

Por lo tanto, la ciberinteligencia militar es un conocimiento esencial que se debe tener en cuenta para planificar y llevar a cabo eficazmente todas las misiones y tareas que las fuerzas desempeñan en cada nivel de la conducción, ya que es muy difícil que un solo nivel, el estratégico, pueda llevar adelante todo el esfuerzo para planificar, desarrollar y defenderse de toda amenaza cibernética durante las operaciones militares. Queda claro que no es suficiente reaccionar o defenderse ante un ataque, sino que es necesario anticiparse a ellos, por eso la ciberinteligencia es fundamental.

**Comunicación Social Aplicativa al Combate (COSACO).**

Esta operación complementaria está prevista que se lleve a cabo por organizaciones de asuntos civiles, fuerzas especiales en el cumplimiento de sus misiones contribuyentes a las operaciones tácticas y eventualmente por organizaciones de inteligencia. A su vez, este tipo de operación, integran la guerra de la información (EA, 2015, pag VII – 30).

Dentro de sus finalidades, y colocando una como prioritaria, podemos mencionar que: se buscará lograr un cambio de conducta (percepciones) ya sean propias, del enemigo y de la población local. Y otro punto importante que se considera vital es: lograr el apoyo de la población en la zona de operaciones.

En mi opinión, basándonos en la doctrina actual del EA, los factores del ambiente operacional, las operaciones multidominio y la influencia de estas sobre las acciones militares, se debería conformar un elemento COSACO bajo la conducción del DIC que opere de acuerdo

con las ordenes emitidas por el Nivel Operacional, a fin de brindar el apoyo de inteligencia necesario, integral y específico antes, durante y después de las operaciones militares.

El mismo debe ser capacitado junto con las Fuerzas Especiales. Esto a su vez incrementará la capacidad COSACO para ser utilizado en apoyo a niveles superiores al CTTO, o sea para las operaciones a nivel operacional.

A su vez, la inteligencia, a través de un grupo especializado de analistas que se dediquen a los factores del ambiente operacional y a las actividades de COSACO, debe disponer de una base de conocimiento y análisis importante sobre el área donde se realizarán las COSACO (demografía, audiencias, sociedad, terreno, economía, etc). Este grupo de analistas debería realizar una apreciación de situación específica enfocada netamente a este tipo de operaciones, las cuales tienen importancia los factores del terreno y condiciones meteorológicas, pero fundamentalmente es el estudio psicosocial del enemigo, los medios de comunicaciones social, sus métodos de propaganda y difusión de información.

Por lo tanto, al contar con un elemento COSACO dentro del DIC en apoyo al CTTO, facilita las operaciones en el dominio cognitivo. Además, al contar con un grupo de analistas específicos en esta área dentro del CII (análisis de COSACO) permite la rápida integración de información y la posterior coordinación y sincronización con los demás dominios físicos y no físicos, esto último tomado como finalidad de las operaciones multidominio.

**Medios para el Sistema de Inteligencia. Sistemas No Tripulados.**

Cabe destacar que el DIC debe ser reforzado con VANT de otras características de las actuales, para brindar el apoyo necesario a las acciones del CTTO. Siempre teniendo en cuenta el avance tecnológico y los tipos de VANT que existen en la región.

Es de gran importancia mencionar que, dentro de la variedad de estos tipos de equipos, son de gran utilidad los UAV de despegue y aterrizaje vertical por sus siglas en inglés VTOL

(Vertical Take-Off and Landing), ya que pueden ser utilizados desde cualquier lugar sin contar con una infraestructura adicional disponible.

Existe un VANT muy particular denominado **XP-4**, de la fábrica estadounidense Ptero Dynamics, la misma, presentó durante el año 2023 un equipo que tiene un sistema propio denominado “Transwing”, que permite que sus alas se plieguen para despegar, aterrizar y también realizar vuelo estacionario, pero lo más interesante es que las alas se despliegan una vez que se encuentra en el aire para operar como una aeronave de ala fija, lo que aumenta significativamente sus capacidades, tales como su rango de acción y su carga. (*Ptero Dynamics* (s.f) Recuperado de https://pterodynamics.com/)

**Figura 1**

***Vehículo Aéreo No Tripulado (VTOL) XP-4***

Otro de este tipo es el que presentó la empresa argentina INVAP. Es el **VTOL RUAS-160** En cuanto a sus dimensiones tiene 3,1 metros de longitud y 1,72 metros de altura, su motor le permite un alcance máximo de 600 kilómetros, tiene una autonomía de 5 horas, un techo operativo de 3.000 metros de altura y una velocidad máxima de 157 kilómetros por hora.

Cuenta con una estación de control portátil, un gimbal eléctrico óptico FHD, un sistema IR LWIR, un telémetro, un sistema de comunicaciones de medio y largo alcance, un sistema de transmisión satelital para video online de media baja definición.

Además, cuenta con una plataforma giroestabilizada con sensores EO/IR, LIDAR y un radar SAR en banda X, herramientas que le brindan la capacidad de detectar, reconocer e incluso identificar objetos móviles y fijos. (*Sistema de Helicóptero No Tripulado RUAS-160* (s.f). Recuperado de https://www.invap.com.ar/areas/defensa-seguridad-y-ambiente/sistema-de-helicoptero-no-tripulado/).

**Figura 2**

***Vehículo Aéreo No Tripulado (VTOL) RUAS-160***


Y un tercer VANT a mencionar es el **Orbiter 3** fabricado por Israel, por la industria Aeronautics. Entre sus características más importantes se encuentran que: es clase I, no necesita de una pista, sino que dispone de lanzador tipo catapulta que puede ir montado sobre un acoplado y es recuperado gracias a un paracaídas incorporado en el propio dron. Tiene propulsión eléctrica, con un peso de 50 Kg en el despegue, una longitud de 4,4 mts, velocidad máxima de 130 km/h y una autonomía de 7 hs y con un radio de 150 Km. Es de nivel táctico, se arma con 2 hombres y se transporta gracias a un camión y un remolque, el tiempo para desplegarlo consta de 7 minutos. Puede transportar cargas útiles de 5 Kg. Cada sistema cuenta estaciones control en tierra, estaciones de datos, cámara T-Stamp-XR, terminales de video

remoto, equipo de apoyo en tierra, kit vehicular y paquete de baterías, tiene enlace de datos digitales. Durante el vuelo, puede navegar incluso en zonas sin señal GPS. (*Aeronautics* (s.f). Recuperado de https://aeronautics-sys.com/systems/orbiter-3/)

**Figura 3**

***Vehículo Aéreo No Tripulado Orbiter 3***

Estos sistemas no tripulados, solo son a modo de ejemplo de entre tantos modelos que existe en el mercado internacional, la intención es reflejar la necesidad de estas aeronaves para el elemento de inteligencia en apoyo a este nivel de la conducción y estas en particular por su radio de acción, infraestructuras necesarias y autonomía para brindar un eficiente apoyo de inteligencia al CTTO, realizando reconocimiento, vigilancia y adquisición de objetivos. Siempre teniendo en cuenta la clasificación de los VANT según la OTAN: clase I (150 Kg al despegue), II (entre 150 Kg y 650 Kg) y III (más de 650 Kg).

**Medios para la obtención electrónica y humana.**

Es necesario incorporar mayor tecnología para los elementos de inteligencia de combate, materializado por la inteligencia humana y electrónica, lo cual dotará a dichas organizaciones con recursos fiables, veloces, flexibles y tecnológicos logrando esa rápida coordinación y sincronización que exigen las operaciones multidominio.

Por consiguiente, podemos mencionar como primer sistema tecnológico para tener en cuenta al **sistema de vigilancia LVSS**, el cual se encuentra montado en un vehículo ligero, este sistema convierte una camioneta convencional en un pequeño centro de comando y control. Con radar y cámaras electroópticas y de infrarrojos montadas en su torre de 5 metros de alto, el LVSS permite una eficaz cobertura de vigilancia durante cualquier tipo de operación. (*Teledine FLIR* (s.f). Recuperado de https://www.flir.com.mx/)

**Figura 4**

***Sistema de vigilancia LVSS***

El segundo equipo que se puede considerar es el **LTV-X Y y el Radar FLIR Ranger R6SS**, el primero es un vehículo ligero (el cual el EA dispone de los vehículos similares como los Polaris, por ejemplo) que combina sus medios de obtención para ofrecer vigilancia terrestre móvil. Con múltiples sensores integrados, como la torreta ISR multiespectral TacFLIR 280-HD y el radar de vigilancia terrestre Ranger R6SS, el LTV-X también incluye un sistema de comando y control a bordo que permite control, explotación y difusión total de imágenes y objetivos en tiempo real. Seguimiento entre activos móviles y fijos desplegados. (Rajowan, S. (2016). *FLIR lanza un vehículo táctico ligero con radar portátil,* de

https://aerobd.news/index.php/2016/05/29/flir-launches-light-tactical-vehicle-flir-portable-radar/)

**Figura 5**

***Sistema de vigilancia LTV-X Y y el Radar FLIR Ranger R6SS.***

Hay diversos equipos militares en el mercado internacional, como también el **Ranger HRC**, que es un sistema de termografía de onda media y alta resolución que identifica objetivos del tamaño de una persona a más de 10 km de distancia y vehículos a más de 20 km, entre otros modelos de la misma marca.

Una vez más, cabe aclarar, que la mención de ciertos equipamientos militares solo responden a demostrar la tecnología necesaria para lograr la flexibilidad, rapidez, eficiencia y la integración de los medios de obtención con el CII para su posterior análisis y difusión.

**Sistemas de Comando, Control, Comunicaciones e Inteligencia.**

Existen diversos tipos de equipamiento, tecnología, arquitecturas con sus modos y conceptos de empleo que facilitan la conciencia situacional de todo decisor táctico. En este caso y potenciando lo que se mencionó en el presente trabajo sobre los sistemas JADC2 y NEC, complementaré mencionando específicamente un producto que demuestra ciertas capacidades

que debe disponer un CII en apoyo al G2 dentro del Estado Mayor del CTTO. Pero existen también, equipos que son exclusivamente para el trabajo de inteligencia.

Sistema Torch–X C4ISR, de la empresa israelí Elbit Systems y el sistema Arkhe Intelligence, de la empresa Atech perteneciente a Embraer, son dos ejemplos claros de sistemas que apoyan el análisis y la toma de decisiones.

Ambas empresas ofrecen diferentes opciones para brindar eficiencia, eficacia, seguridad logrando la coordinación necesaria en el campo de batalla. Pero a modo de ejemplo, detallaré el primero de ellos: el sistema Torch-X.

Este equipo presenta un diseño avanzado, el cual es apto para numerosas tareas complejas de gran magnitud. Integra sensores, dispositivos y comunicaciones, adaptándose tanto a plataformas no tripuladas como a las convencionales. Estos sistemas de vanguardia optimizan la coordinación de las fuerzas, facilitan la planificación estratégica, administran el combate de forma exhaustiva y mejoran las operaciones tácticas. Las herramientas C4ISR de Torch-X incorporan inteligencia artificial en el apoyo a la toma de decisiones, aligerando el esfuerzo mental en todos los niveles y perfeccionando los procesos decisionales y de planificación (*Elbit Systems* (s.f). Recuperado de https://elbitsystems.com/products/c4i-systems/).

## Sección IV

## Conclusiones Parciales.

En base a lo anteriormente expuesto y teniendo en cuenta la complejidad que representa el apoyo de inteligencia en el nivel CTTO, podemos concluir lo siguiente:

Las características de la inteligencia táctica tal como la rapidez en la respuesta, la falta de tiempo, el detalle de la información, el contacto permanente con las fuentes de información sumado a las características propias del nivel CTTO, imponen al sistema de inteligencia (en

apoyo al CTTO), fluidez, integración, rapidez, coordinación y sincronización en las tareas a realizar enmarcadas por el ciclo de inteligencia.

El análisis de los factores del ambiente operacional reviste una gran importancia en este nivel, por esta razón es que merece toda la atención en la asignación de prioridades cuando el medio en apoyo al órgano de dirección (CII) deba ejecutar su análisis antes y durante la ejecución de las operaciones del CTTO. En consecuencia, debe existir un grupo dedicado al análisis exhaustivo de los mismos.

El sistema de inteligencia debe garantizar agilidad, incorporación tecnológica, conciencia situacional, recurrencia y cohesión en todo el sistema, lo que facilitará la ejecución del ciclo de inteligencia durante las operaciones multidominio logrando a su vez integrar y coordinar más de un dominio para cumplir con el objetivo de este tipo de operaciones.

El sistema de inteligencia en el nivel GUB se encuentra cohesionado al igual que el de la GUC, pero al existir el quiebre en el nivel CTTO por no contar con un CII en apoyo al órgano de dirección de dicho nivel, dificulta la recurrencia y agilidad en el traspaso y análisis de la información/inteligencia, por lo que impacta directamente en la conformación eficiente del órgano de dirección del CTTO ya que el G2 necesita de un elemento con analistas especializados que brinde la información/inteligencia relacionada a todos los factores que influyen en las operaciones multidominio.

Entendiendo el sistema de inteligencia como un conjunto de órganos de dirección y medios de ejecución, podemos materializar, en este caso en particular, al G2 del Departamento II-Icia y al DIC como integrantes de este. Este último debería cambiar su concepto de empleo y su organización, para estar acorde a las exigencias que imponen las operaciones multidominio. Ya que, con la incorporación de recursos tecnológicos, un concepto de empleo

y capacidades afines a las exigencias actuales, potenciarán el uso de dicho elemento de inteligencia.

Por lo tanto, su concepto de empleo podría ser el siguiente: el DIC será la mayor unidad táctica de inteligencia, el cual se encontrará organizado, equipado e instruido en las actividades que demande el ciclo de inteligencia para brindar apoyo de inteligencia al CTTO en las áreas de combate, territorial y proyección.

Creando e incorporando un CII "multidominio" con especialistas concretos, van a representar el recurso humano y tecnológico más idóneo y eficaz para los escenarios actuales. Esta creación y uso del CII, responde tanto a la multiplicidad de medios de obtención de información y de sensores en distintas plataformas que van a existir en este nivel, como la variedad de factores del ambiente operacional que influyen en las operaciones, lo cual representa una dificultad en el momento de la gestión de la información. Por lo tanto, es necesario centralizar y canalizar la información en un CII para optimizar la ejecución de las acciones a fin de permitir y facilitar el asesoramiento y asistencia al comandante para la toma de decisiones en un ambiente tan volátil y complejo como lo representa un futuro TO con las características que venimos mencionando.

Por consiguiente, el incremento de un CII como apoyo al órgano de dirección, las disciplinas descriptas tales como OSINT, ciberinteligencia, COSACO y los recursos tecnológicos para los medios de ejecución permiten al sistema de inteligencia reforzar sus capacidades actuales incrementando su poder de análisis, de obtención e integración de la información, transformándola luego en inteligencia para el comandante, a través de una manera expeditiva, asegurando al sistema de estar preparados ante cualquier escenario que se presenten durante las operaciones militares, específicamente en las operaciones multidominio.

Por otro lado, se debe tener en cuenta dos conceptos muy importantes para lograr cohesión y apoyo eficiente en este nivel. El primero de ellos es la creación de una comunidad de inteligencia y el segundo es el trabajo inter y multiagencial entre organizaciones civiles, de seguridad y militares.

Relacionado al primero de ellos, concretamente, es un conjunto de sistemas de inteligencia que se conforma por mutuo acuerdo y cooperación, no existe una relación orgánica entre los componentes del sistema, pero si objetivos comunes. Esto facilitará la obtención de información y su procesamiento, la cooperación, coordinación e integración entre las partes involucradas, logrando con esto un eficiente apoyo al proceso de toma de decisiones en el nivel CTTO y finalmente coadyuvando a la defensa nacional, fin último de toda organización armada y de seguridad. La experiencia de varios países del mundo da muestras de que contar con este tipo de estructura facilita el trabajo de inteligencia en pos de la seguridad y de la defensa.

En efecto, se debe poner a disposición todas las fuerzas del poder nacional al servicio de la defensa, integrando, esencialmente los medios de inteligencia de la seguridad interior y los de la defensa nacional.

Y relacionado al segundo concepto, las operaciones multidominio también atraviesan a las organizaciones de seguridad y civiles, con mayor preponderancia en ciertos dominios. Pero básicamente el ciberespacial y cognitivo afectan directamente a estas organizaciones. En definitiva, las fuerzas de seguridad (policía federal, policía aeroportuaria, gendarmería nacional, prefectura naval), junto con defensa civil, empresas relacionadas a las infraestructuras críticas, empresas de transporte (trenes argentinos, aviación civil), telecomunicaciones (Arsat, empresas telefónicas) y una cantidad importante de empresas estatales y civiles que podrían aportar su conocimiento técnico para la solución de problemas que afecten la vida y libertad de los habitantes.

Finalmente, es necesario la configuración, durante la paz, de equipos de trabajo (según los escenarios estratégicos que marca la DPDN: norte, centro y sur) que deben planificar, coordinar y ejecutar ejercicios, seminarios, transferencia de información, etc conformando un centro de operaciones conjunto multidominio, para que el día del conflicto se conforme ad hoc un elemento interagencial que trabaje a la par del CII integrando toda la información y experiencia para solucionar los problemas militares complejos que se vayan materializado. Pero esto se logrará a través de una regulación, con un cuerpo normativo, reglas, conceptos de empleo y responsabilidades y capacidades para cada una de las organizaciones civiles y de seguridad que participen del futuro conflicto.

## Conclusiones finales.

Después del análisis realizado durante el presente trabajo acerca de la organización del sistema de inteligencia en apoyo al CTTO durante las operaciones multidominio, se pretende destacar ciertos aspectos y reflexiones, las que se van a materializar a través de las siguientes conclusiones:

Como primer punto, cabe mencionar la importancia que cobra la tecnología y el avance de esta a través del paso del tiempo, por ese motivo las operaciones militares se ven atravesadas por el factor tecnológico que ha redefinido las estrategias y tácticas de la guerra. Esta tecnología disruptiva impactó en cada dominio existente logrando, a su vez, potenciar la integración y coordinación entre los mismos.

En base a la incorporación de tecnología a las organizaciones militares, debe acompañar la actualización doctrinaria lo que llevará a una instrucción diaria y posterior adiestramiento para lograr la eficiencia de los conjuntos.

Como segundo punto importante a destacar es la importancia de contar con un equipo interagencial y multidisciplinario, así como se explicó durante el trabajo, es fundamental para la etapa previa al conflicto, responde a cuestiones tales como la recolección de información, el procesamiento y la difusión, también jugarán un papel fundamental en la capa “anticipar” participando en la alerta estratégica, como así también en la alarma durante el conflicto. Esta integración de equipos conformado por personal civil, de seguridad y militar facilita el trabajo de la inteligencia antes y durante las operaciones que desarrollará el CTTO durante las operaciones multidominio, además dichas operaciones van a afectar de alguna manera, infraestructuras críticas relacionadas a la matriz energética del país, al sistema sanitario, al transporte y/o a la seguridad de la ciudadanía. El grado de confianza, la fluidez y el profesionalismo que se logrará a través de la instrucción, adiestramiento conjunto, las buenas

relaciones profesionales (compartiendo y analizando información) permitirá crear lazos de confianza y de profesionalismo. Siempre teniendo en cuenta la confidencialidad de la información que se maneje en ciertos ámbitos.

Por lo tanto, y relacionado a lo anteriormente descripto, la creación y desarrollo de una comunidad de inteligencia por escenarios estratégicos dentro del país facilitará la cohesión y fluidez en la obtención, procesamiento de la información y difusión, disponiendo de distintos medios y elementos que aporten a una causa y objetivo común: la defensa nacional.

Básicamente, debe existir una integración, cooperación y coordinación con las dos inteligencias más importantes de una nación, la inteligencia de la defensa nacional (Ministerio de Defensa) y la inteligencia de la seguridad interior (Ministerio de Seguridad) recurriendo a esta organización/comunidad, como un órgano consultivo para palear y contrarrestar todo lo que impone la estrategia de capas y restricción de áreas de la República Argentina. Por supuesto, integrándose con otros organismos de inteligencia civiles dentro de los escenarios estratégicos que establece la DPDN conformando grandes "órganos consultivos" disponiendo de información e inteligencia actualizada dando eficiencia al Sistema de Inteligencia del CTTO que se active para brindar apoyo dentro del TO.

Teniendo en cuenta el marco normativo de la República Argentina y la actitud estratégica defensiva adoptada en su política de defensa, demuestra que deben alcanzarse ciertas capacidades, desarrollando una estrategia disuasiva con tres aspectos a considerar: debe ser creíble, lograr comunicarla y por supuesto tener la capacidad de llevarla adelante. Esto exige en primer lugar disponer de tecnología e intenciones de llevarla a cabo mediante el uso de diversos equipos/recursos tales como VANT, satélites, radares, guerra electrónica, inteligencia artificial, C4I2, etc.

En definitiva, la República Argentina debe contar con alianzas estratégicas que respondan a una fuerza integral, tal como lo establece EUA, o simplemente desarrollarla de forma autónoma, pero se debería lograr a través de una política estratégica disuasiva haciendo que el adversario desista de realizar cualquier acción no deseada, haciéndolo percibir que los costos serán demasiado altos y/o que las posibilidades de éxito serán mínimas. En esencia, se puede utilizar diversos métodos, pero particularmente el concepto A2-AD.

Por lo tanto, y cerrando con la idea anterior, el contar con alianzas en el marco regional y la necesidad de trabajar de manera combinada para salvaguardar intereses y recursos estratégicos impulsa esta iniciativa. Así, se ve la importancia de analizar, planificar, desarrollar e incrementar el intercambio y futuro adiestramiento combinado con países de la región a fin de impulsar la estrategia disuasiva y el intercambio de información/inteligencia.

Es una responsabilidad de los más altos niveles de la conducción, reflexionar sobre este nuevo concepto estratégico para llevar adelante las operaciones militares y enfrentarse a un nuevo concepto de guerra, la guerra del futuro la cual nos encontramos transitando

En base lo descripto anteriormente y teniendo en cuenta algunos aspectos legales que se exponen en las distintas leyes, reglamentaciones y resoluciones dentro de la República Argentina, dificultan el pleno desarrollo de la función inteligencia en apoyo las operaciones que se desarrollen en el nivel CTTO, ya que las amenazas no solo serán del tipo convencional, perpetradas por fuerzas armadas de otro estado, sino que serán de diversos modos, a través de actores no estatales con tácticas y procedimientos conocidos tales como ciberataques, operaciones de información, operaciones encubiertas, terrorismo, lo cual sobrepasa el empleo único de métodos “clásicos”.

Por esta razón, la inteligencia debe desarrollar ciertas capacidades (que no se encuentran descriptas en nuestras doctrinas) para brindar un eficiente apoyo al nivel CTTO. Es por ello,

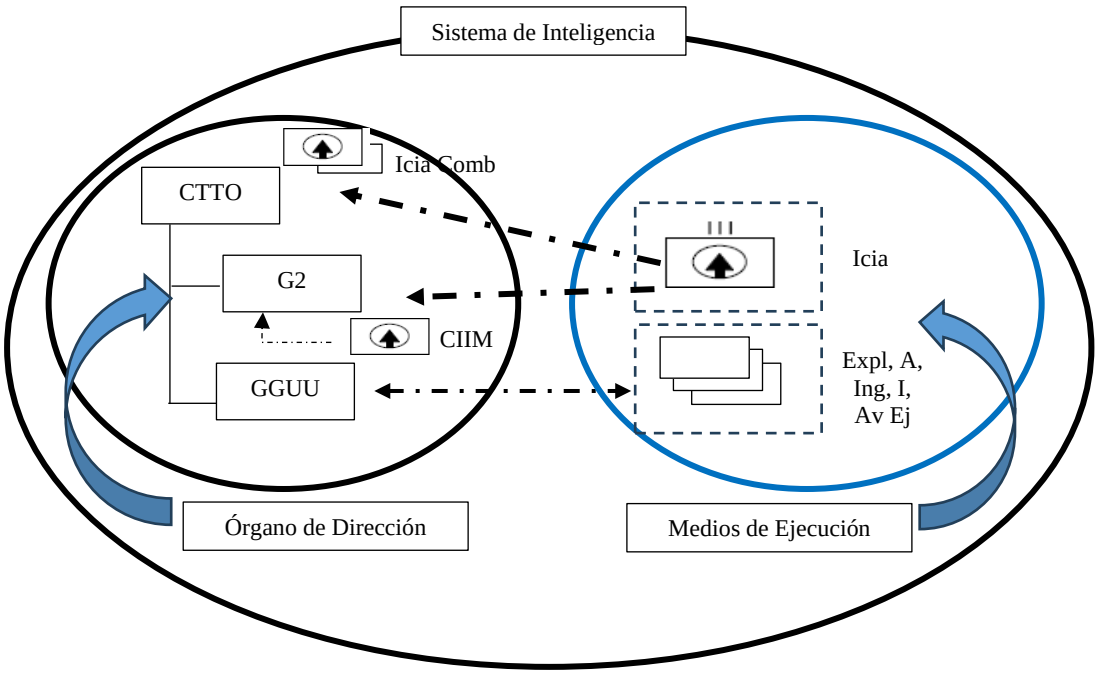
que lo podemos materializar a través de una organización “actualizada” del sistema de inteligencia. Dicho sistema contendrá: un elemento de ejecución (de inteligencia) y órgano de dirección con rasgos que responden al multidominio. No es más que adaptarse a la realidad que nos rodea, aceptando las nuevas amenazas, rompiendo paradigmas y, sobre todo, de nuestra forma de ver la defensa y entender el mundo (ya que somos una cultura occidental) para estar a la altura de países que están transitando este cambio en su pensamiento militar, teorías y doctrinas.

A continuación, y a modo de cierre de las conclusiones finales, se propone como aporte profesional, el Sistema de inteligencia en apoyo al CTTO.

## Aporte Profesional

**Figura 6**

***Sistema de Inteligencia nivel CTTO.***




**Fuente**: elaboración propia

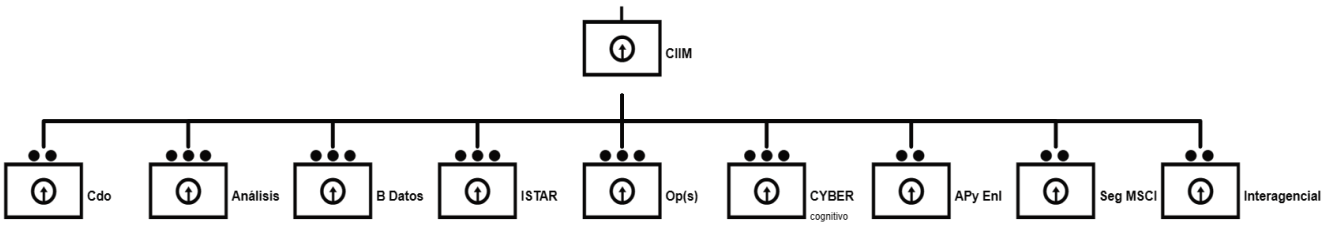
**Elemento en apoyo al Órgano de dirección:**

**Compañía Centro Integrador de Inteligencia Multidominio (CIIM).** En apoyo al G2 del Comando Componente Terrestre del Teatro de Operaciones, el cual estará integrado por los siguientes elementos:

- Un grupo comando
- Una sección Análisis
- Una Sección Base de Datos (grupo proyección, ambiente operacional, territorial)
- Sección Integración ISTAR
- Una Sección Operaciones (con un grupo operaciones Futuras y un Grupo Operaciones en desarrollo).
- Una Sección Inteligencia cibernética y cognitiva (grupo fuentes abiertas, grupo ciberinteligencia y guerra electrónica y grupo análisis COSACO)
- Un Grupo Apoyo y enlaces (con traductores, un grupo enlaces con otras fuerzas armadas, sicólogos, expertos en climatología)
- Un grupo seguridad a las operaciones (MSCI)
- Un grupo interagencial.

**Figura 7**

***Centro Integrador de Inteligencia Multidominio (CIIM).***




**Fuente**: elaboración propia

**Funciones de cada fracción integrante del CIIM:**

**Grupo Comando:** servirá como mesa de entrada, se encargará de las actividades administrativas y todo lo relacionado a documentación digital y papel que ingrese a la organización, y la distribución de la misma a las diferentes áreas/células de trabajo.

**Sección Análisis**: será la base de conocimiento de la Ca CIIM, proporcionará inteligencia. Aquí se encontrarán los analistas del Orden de Batalla, Ambiente Geográfico, Ambiente Operacional, condiciones meteorológicas e interpretación de imágenes los cuales van a ser asistidos por la Sección Apoyo y enlaces.

**Sección base de datos**: es el que dispondrá de la información básica y actual, no realizará el proceso de esta. El Grupo proyección trabajará sobre los componentes del o los actores: político, económico, geográfico, militar, transporte y telecomunicaciones, científico y tecnológico. Tendrá un grupo especial que se dedicará exclusivamente a la obtención de información de los factores del ambiente operacional de algunos de los escenarios estratégicos de la República Argentina. Y en forma de espejo dispondrá de un grupo territorial para realizar la misma tarea.

**Sección Integración ISTAR:** será el encargado de integrar la información obtenida por todos los sensores distribuidos en el TO que se encuentren ejecutando reconocimiento, vigilancia y exploración. Con la ayuda de un grupo denominado “apoyo situacional táctico”, que estará a cargo de los software y tableros tácticos para proyectar la información en tiempo real y con el soporte y apoyo de programas de inteligencia artificial junto con especialistas provenientes de la Sección Análisis, continuarán con el procesamiento de la información, mientras se está desarrollando la visualización y la futura toma de decisiones.

**Sección Operaciones:** compuesta por dos grupos, el de “operaciones en desarrollo” que llevará todo lo relacionado a la situación del enemigo y actualización de la información de los factores del ambiente operacional, recibiendo toda la información de los medios de obtención

y simultáneamente por el canal técnico de inteligencia proveniente de otras GUB, o Componentes. Por otro lado, el grupo “operaciones futuras”, deberá estar en capacidad de utilizar las técnicas de prospectivas y la confección de supuestos para desarrollar capacidades del enemigo, establecer intenciones y objetivos, escenarios futuros y probable evolución. Este grupo se verá apoyado especialmente con tecnología específica, a través de la inteligencia artificial, utilizando programas pertinentes que deberán ser desarrollados por especialistas a necesidad de la Sección Análisis y Operaciones.

**Sección Inteligencia Cibernética y cognitiva:** encargada de las operaciones de ciberinteligencia, estableciendo el planeamiento respectivo, realizará el monitoreo y vigilancia del ciberespacio en búsqueda de amenazas cibernéticas específicas que atenten contra objetivos de este nivel de la conducción, establecerá las medidas de protección de las infraestructuras críticas y de los sistemas de información del CTTO. Trabajará en enlace directo con el escalón superior (Nivel Operacional). El grupo cognitivo, estará a cargo del análisis de todos los factores que influyen en las operaciones COSACO, brindando información e inteligencia a las tropas en campaña que se encuentren desarrollando este tipo de operaciones. El grupo OSINT, tendrá la responsabilidad de obtener información con sus técnicas específicas, la validación y el análisis de esta, como así también el monitoreo constante para alertar de cualquier tipo de información sensible o crítica que afecten las propias operaciones.

**Grupo Apoyo y enlaces:** esta sección dispondrá de un grupo apoyo que contará con personal civil o militar especializado tales como traductores, psicólogos, expertos en relaciones internacionales, expertos en técnicas de prospectivas, meteorólogos, especialistas en comunicación social y, por otro lado, el grupo enlace, que contará (a orden) de oficiales de enlace de la Fuerza Aérea y Armada para coordinar actividades en los dominios respectivos.

**Grupo Seguridad a las Operaciones (MSCI)**: encargado de obtener y procesar la información de contrainteligencia, según su plan de obtención, incluirá todo tipo de medidas de seguridad para las operaciones en desarrollo a fin de proteger a la fuerza de la inteligencia del adversario. Ejecutará censura primaria y secundaria.

**Grupo Interagencial:** tendrá la responsabilidad de integrar la información que disponen desde la paz y las coordinaciones pertinentes que se deben efectuar para cada área específica que se vea afectada por las operaciones multidominio. Debe existir un grado de reserva y confidencialidad importante con la información que se trate, más allá de que el equipo ad-hoc cívico-militar ya se encuentra adiestrado y vienen desarrollando un trabajo conjunto y profesional.

**Medio de ejecución:**

**Destacamento de Inteligencia de Combate.** Principal unidad táctica de inteligencia en apoyo al CTTO, el cual brindará apoyo de inteligencia en las áreas de combate, territorial y proyección.

Además de sus compañías actuales, el DIC deberá incorporar: una compañía inteligencia COSACO (Ca Icia COSACO) y una compañía Centro Integrador Multidominio (CIIM). Esto, incrementará capacidades que no están comprendidas en algunos de los dominios, específicamente, en el domingo cognitivo/humano.

Además, se reforzará la capacidad ISTAR, en el ámbito terrestre a través de la obtención humana y electrónica (con medios tales como se mencionó, tecnología radar, FLIR, con medios livianos y ligeros que dispongan de conectividad y velocidad en la transmisión de datos) y en el ámbito aéreo, con los VANT (incorporando equipos VTOL, o equipamiento que responda específicamente al radio de acción que se utilizaría para este nivel de la conducción, autonomía y comunicaciones seguras). Finalmente, por medio de la Ca CIIM, se integrará la información

a través de la incorporación ISTAR brindando apoyo al órgano de dirección de inteligencia del CTTO, integrando también tecnología tal como los tableros tácticos e inteligencia artificial para facilitar el análisis, la integración y visualización de la información.

En definitiva, el incremento de elementos específicos a la orgánica del DIC, la incorporación de tecnología avanzada para los medios de obtención y el apoyo del CIIM, con sus nuevas capacidades, facilita el desarrollo del ciclo de inteligencia coadyuvando al proceso de toma de decisiones en el ámbito de las operaciones multidominio.

## Referencias

Alaniz Miranda, O (2021). O*peraciones multidominio: soluciones tácticas para desafíos estratégicos y operacionales.* Revista Ensayos Militares, Pag 111 – 125. República de Chile.

Angulo Molina, R. (2019) *Los multidominios, desafío de las Fuerzas Armadas Argentinas.* Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Buenos Aires.

Arce Ducassou, R. (2019) *Capacidades militares para enfrentar los desafíos de las operaciones multidominio*. Revista Ensayos Militares. (Vol. 5 – Nro 2 – 2019). Pag 57-81. Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile, República de Chile.

Arenas, E. (2021) *La organización de la jefatura de inteligencia del comando operacional de las fuerzas armadas en las operaciones multidominio*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Buenos Aires.

Aquino, C. (2022) *La implementación de una estrategia de Anti-Acceso y Negación de Área (A2/AD) en el triángulo Antártida, Tierra del Fuego e Islas Malvinas.* [Trabajo Integrador Final]. Especialización en Conducción Táctica y Operacional Naval. Escuela de Guerra Naval, Buenos Aires.

Barrera Franco, C. y Carranza Vázquez, M. (2023) *Disuasión estratégica en el hemisferio occidental: propuestas vigentes para el entorno multidominio*. (12/2023). Global Strategy Report.

Battaleme, J. (2013) *El acceso a los espacios comunes y las estrategias de negación de espacio y antiacceso*. Cuadernos de Geopolítica 1.

Campos, G. (2003) *Inteligencia Estratégica: aproximación conceptual y metodológica*. Compendio de clases de la materia inteligencia estratégica del ciclo de formación del Oficial de Estado Mayor del Ejército Argentino. Buenos Aires.

Cardenas, J. M. (2022). *OSINT en tiempos de guerra*. LISA News.

Casarino, P. y Ortiz, J. (2019). *La ciberdefensa y la ciberinteligencia militar*. Visión Conjunta. (Año 11. Nro 21). Pag 43 a 52. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de la República Argentina, Buenos Aires.

Castro Brahm, J. P. (2021) *Las operaciones de información en el comando del espacio común marítimo como parte de una estrategia A2/AD.* [Trabajo Integrador Final]. Escuela de Guerra Naval, Buenos Aires.

Comando Conjunto de Ciberdefensa (2023). La ciberdefensa en el nivel operacional y táctico. [Exposición basada en power point]. Escuela Superior de Guerra, Buenos Aires.

Comando Operacional de las Fuerzas Armadas (15 de setiembre de 2023). Estrategias de Capas y Multidominio. [Exposición basada en power point]. Escuela Superior de Guerra, Buenos Aires.

D'agata, D. (2021) *El sistema de inteligencia del componente terrestre y la guerra de información* [Tesis de Especialista en Conducción Superior de OOMMTT], Escuela Superior de Guerra, Buenos Aires.

Ejército Argentino (2007) *Destacamento de Inteligencia de Combate*. Buenos Aires. Estado Mayor General del Ejército.

Ejército Argentino (2008) *Inteligencia Táctica* – Buenos Aires. Estado Mayor General del Ejército.

Ejército Argentino (2014) *Conducción de la Compañía de Inteligencia de la Gran Unidad de Combate* – Buenos Aires. Estado Mayor General del Ejército.

Ejército Argentino (2015) *Conducción para las Fuerzas Terrestres* – Buenos Aires. Estado Mayor General del Ejército.

Ejército Argentino (2017). *Conducción del Batallón de Inteligencia* – Buenos Aires. Estado Mayor General del Ejército.

Ejército de Estados Unidos (2023). *FM 2-0 Inteligencia.* Washington. Departamento del Cuartel General del Ejército.

*Elbit Systems* (s.f). Recuperado de https://elbitsystems.com/products/c4i-systems/.

Escribano, D. (2022). *Organización Militar de Inteligencia como elemento de asesoramiento y asistencia a la toma de decisiones antes los ciberataques a nivel componente Ejército*. [Trabajo Final Integrador]. Escuela Superior de Guerra, Buenos Aires.

Estado Mayor Conjunto de las Fuerzas Armadas (2018) *Doctrina Básica para la Acción Militar Conjunta* – Buenos Aires. Estado Mayor Conjunto de las Fuerzas Armadas.

Estado Mayor Conjunto de las Fuerzas Armadas (2019) *Glosario de términos de empleo militar para la acción militar conjunta* – Buenos Aires. Estado Mayor Conjunto de las Fuerzas Armadas.

Estado Mayor Conjunto de las Fuerzas Armadas (2023) *Conceptos Generales sobre la concepción estratégica de capas, restricción de áreas y de operaciones multidominio* – Buenos Aires. Estado Mayor Conjunto de las Fuerzas Armadas

Fojón, E. (2019) *Desarrollos tecnológicos militares frente a nuevos conceptos operativos.* Real Instituto Elcano.

García Servet, R. y Calvo Alvero J. L. (2022). *El dominio cognitivo en las operaciones multidominio: concepto y problemática.* Academia de las Ciencias y las Artes Militares. España.

Instituto español de estudios estratégicos (1991). *Estudio de inteligencia operacional*, Madrid, España. Ministerio de Defensa.

León, P (2017). La Batalla Multidominio. Revista Escenarios Actuales. (Año 22, octubre,

Nro 2). Pag 39-56. Centro de Estudios e Investigaciones Militares. Santiago de Chile

Ludwig Von Bertalanffy (1976) *Teoría General de los Sistemas.* México. Fondo de Cultura Económica.

Marín Delgado, J. A. (2021). *Guerra de drones en el Cáucaso Sur: lecciones aprendidas de Nagorno Karabaj*. Instituto Español de Estudios Estratégicos (IEEE). España.

Martínez, G. (2020). *Inteligencia de Amenazas Cibernéticas.* [Trabajo Final de la Carrera de Especialización en Seguridad Informática]. Universidad de Buenos Aires Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería, Buenos Aires.

Ministerio de Defensa del Reino de España (2022). *Nuevo concepto estratégico de la OTAN* - Madrid 29 de junio de 2022.

Ministerio de Defensa del Reino de España (2020). Nota Conceptual: Operaciones Multidominio. Centro Conjunto de Desarrollo de Conceptos (CESEDEN). Madrid, España.

Oreglia, J. L. (2017). *Fuerzas Armadas y las amenazas transnacionales: su marco legal*. Visión Conjunta. (año 9, Nro 17). Pag 39-46. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Buenos Aires.

OSINT (inteligencia de fuentes abiertas). Recuperado de https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas

Páez, E. (2022) *El Centro Integrador de Inteligencia en apoyo al Departamento Inteligencia del Componente Terrestre del Teatro de Operaciones* [Investigación de Estado Mayor]. Escuela Superior de Guerra, Buenos Aires.

Perkins, D. G. (2018). *La batalla multidominio. Impulsando el cambio para ganar en el futuro*. Military Review.

Rajowan, S. (2016). *FLIR lanza un vehículo táctico ligero con radar portátil*, de https://aerobd.news/index.php/2016/05/29/flir-launches-light-tactical-vehicle-flir-portable-radar/

República Argentina (1988). *Ley de Defensa Nacional Nro 23.554.* http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

República Argentina (2006). *Decreto 727/06 Reglamentación de la Ley de Defensa.* http://servicios.infoleg.gob.ar/infolegInternet/anexos/115000-119999/116997/norma.htm

República Argentina (1988). *Ley de Reestructuración de las Fuerzas Armadas Nro 24.948*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/50000-54999/50229/norma.htm

República Argentina (2006). *Decreto 1691/2006. Organización y funcionamiento de las Fuerzas Armadas.* https://servicios.infoleg.gob.ar/infolegInternet/anexos/120000-124999/122503/norma.htm

República Argentina (2001). *Ley de Inteligencia Nacional Nro 25.520*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm

República Argentina (2006). *Resolución Ministerial Nro 381/06*

República Argentina (2021). *Decreto 457/2021 Directiva de Política de Defensa Nacional*

Skates, J. L. (2021). *Operaciones multidominio en los niveles de división e inferiores*. Military Review. Tercer trimestre 2021.

*Teledine FLIR* (s.f). Recuperado de https://www.flir.com.mx/

Varela Sabando, P. (2014). *Desarrollo e Integración del Concepto ISTAR (Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimientos) en el Campo de Batalla Táctico*. [Trabajo Final Integrador]. Escuela Superior de Guerra, Buenos Aires.

Vego, M. (2000) *Centro de Gravedad*. Military Review. Pag 23 -29.