



**ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y  
PLANEAMIENTO MILITAR CONJUNTO**

**TRABAJO FINAL INTEGRADOR**

**TÍTULO:** FUERZAS A DISPOSICIÓN DEL COMANDANTE DEL TEATRO DE OPERACIONES PARA LA EJECUCIÓN DE OPERACIONES MULTIDOMINIO EN LAS CAPAS CONJURAR Y REPELER.

**AUTOR:** MAYOR - EJÉRCITO ARGENTINO - DIEGO SEBASTIAN MERCADO

**TUTOR:** CORONEL JUAN PAULO BRITOS

**AÑO: 2024**

“Las ideas expuestas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia la opinión de la Escuela Superior de Guerra Conjunta de la Facultad Militar Conjunta de la Universidad de la Defensa Nacional

## **Resumen**

La concepción estratégica de “Capas, Restricción de Área y Operaciones Multidominio” prevé la defensa nacional a través de la ejecución de acciones agrupadas en cuatro capas. Las capas “anticipar y prevenir” materializarán los esfuerzos activos, permanentes y periódicos mediante la vigilancia y control del territorio nacional. En las capas “conjurar y repeler” se concretarán los esfuerzos reactivos, es decir, el empleo del poder militar contra un agresor estatal militar externo. En un primer momento se buscará degradar, desgastar y afectar la logística del agresor, para luego, destruirlo o neutralizarlo.

Las acciones reactivas se llevarán a cabo en uno o varios teatros de operaciones que podrán coincidir con las subáreas de interés estratégico. Al comandante del teatro de operaciones se le asignarán fuerzas militares que se organizarán en función de su misión específica impuesta.

La forma de ejecutar las operaciones militares, será a través de las operaciones multidominio. Las mismas han surgido como un enfoque estratégico crucial en el ámbito militar contemporáneo. Este concepto se refiere a la capacidad de las fuerzas armadas para operar de manera efectiva en múltiples dominios, terrestre, marítimo, aéreo, espacial, cognitivo, información y ciberespacial. El diseño de fuerzas para operaciones multidominio implica considerar una serie de parámetros clave, desde la interoperabilidad hasta la evaluación de amenazas y riesgos, así como la consideración de conceptos disruptivos como la guerra mosaico.

El presente trabajo final integrador tiene la finalidad de establecer, tras los análisis efectuados, los parámetros para diseñar las fuerzas que debería tener a disposición el Comandante del teatro de operaciones.

### **Palabras claves**

Multidominio – Mosaico – Interoperabilidad – Modularidad – Adaptabilidad

## Índice

Resumen.....	ii
Palabras claves .....	ii
Índice.....	iii
Introducción .....	1
Capítulo 1.....	5
Operaciones Multidominio y la Guerra Mosaico en el Marco de la Concepción Estratégica de Capas, Restricción de Área y Operaciones Multidominio.....	5
1.1.    Introducción a las Operaciones Multidominio .....	5
1.1.1.    Casos Relevantes .....	6
1.1.2.    Componentes Clave de las Operaciones Multidominio.....	6
1.1.3.    Aplicación en el Contexto de Defensa Nacional .....	7
1.2.    Definición y Principios de la Guerra Mosaico.....	8
1.2.1.    Fundamentos de la Guerra Mosaico .....	8
1.2.2.    Principios Clave de la Guerra Mosaico .....	8
1.2.3.    Ventajas Estratégicas de la Guerra Mosaico.....	10
1.3.    Capas Conjurar y Repeler .....	10
1.3.1.    Capa Conjurar .....	11
1.3.2.    Capa Repeler.....	11
1.3.3.    Sinergia entre las Capas Conjurar y Repeler .....	12
Capítulo 2.....	13
Parámetros para el Diseño de Fuerzas Multidominio para el Teatro de Operaciones.....	13
2.1.    Modularidad en el Diseño de Fuerzas Multidominio.....	13
2.1.1.    Fundamentos y Objetivos de la Modularidad .....	13
2.1.2.    Modularidad y Despliegue Rápido en el Teatro de Operaciones .....	13
2.1.3.    Integración de Tecnología Autónoma en Unidades.....	14
2.2.    Interoperabilidad en las Fuerzas Multidominio .....	14
2.2.1.    Fundamentos y Objetivos de la Interoperabilidad .....	15
2.2.2.    Interoperabilidad en la Capa Conjurar.....	15
2.2.3.    Interoperabilidad en la Capa Repeler.....	16
2.2.4.    Desafíos y Soluciones en la Interoperabilidad.....	16
2.3.    Escalabilidad y Adaptabilidad en el Teatro de Operaciones.....	17
2.3.1.    Escalabilidad en el Diseño de Fuerzas Multidominio.....	17

2.3.2.	Adaptabilidad en el Teatro de Operaciones .....	18
2.3.3.	Sinergia entre Escalabilidad y Adaptabilidad en el Teatro de Operaciones .....	19
2.4.	La Convergencia .....	19
2.4.1	Convergencia como Parámetro de Diseño .....	20
2.4.2.	Desafíos de la Convergencia.....	20
2.5.	Integración de Tecnología y Sistemas Autónomos en el Diseño de Fuerzas.....	20
2.5.1	Tecnología Autónoma y Operaciones en Múltiples Dominios.....	20
2.5.2.	Inteligencia Artificial y Análisis de Datos en Tiempo Real .....	21
2.5.3.	Sistemas de Mando y Control Avanzados .....	22
2.5.4.	Desafíos y Consideraciones en la Integración de Tecnología y Sist Autón .....	22
2.6.	Impacto Estratégico: Disuasión y Equilibrio Regional .....	23
2.6.1.	Disuasión y Preparación para Conflictos de Alta Intensidad.....	23
2.6.2.	Equilibrio de Poder Regional.....	23
2.7.	Desafíos Logísticos en Fuerzas Multidominio.....	23
2.7.1.	Costos de Implementación y Mantenimiento .....	23
2.7.2.	Infraestructura y Logística Descentralizada.....	23
2.7.3.	Desafíos en el Contexto Nacional.....	23
2.7.4.	Ventajas Logísticas de las Fuerzas Multidominio .....	24
2.8.	Propuesta para la Implementación de Fuerzas Multidominio.....	24
2.8.1.	Programas de Capacitación para Operaciones Multidominio.....	24
2.8.2.	Ejercicios de Simulación y Pruebas Operativas.....	24
2.9.	Evaluación de Riesgos y Limitaciones.....	25
2.10.	Coordinación con Agencias No Militares .....	26
2.10.1.	<i>Estrategias para Fomentar la Cooperación .....</i>	26
2.10.2.	<i>Beneficios de la Coordinación con Agencias No Militares .....</i>	26
	Conclusiones Finales .....	28
	Anexo 1 .....	31
	Anexo 2 .....	32
	Concepto de la Guerra Mosaico.....	32
	Anexo 3 .....	33
	El Mosaico de Combate .....	33
	Bibliografía .....	34

## Introducción

En el complejo escenario de las operaciones militares contemporáneas, la necesidad de una capacidad de respuesta efectiva y adaptativa ante amenazas multidimensionales se ha convertido en una prioridad estratégica. El comandante del Teatro de Operaciones, como responsable de las fuerzas desplegadas en un área geográfica específica, debe contar con una composición adecuada de fuerzas terrestres, aéreas y navales, así como de otras agencias no militares, para llevar a cabo operaciones multidominio de manera exitosa, que permita una respuesta integrada en diferentes frentes para accionar en los diferentes dominios.

Por esta razón, el comandante del teatro de operaciones debe comprender cómo estas amenazas multidominio interactúan y afectan la seguridad y estabilidad en su área de responsabilidad.

Según la concepción estratégica que rige la defensa nacional (Estado Mayor Conjunto [EMCO], 2023a), las fuerzas armadas se emplearán en las capas reactivas, es decir la capa conjurar y la capa repeler.

La Capa Conjurar se refiere a la capacidad de influir en la percepción y cognición del adversario. Aquí, las fuerzas deben utilizar medios como la guerra electrónica, la ciberdefensa y la información para afectar la toma de decisiones enemiga.

La Capa Repeler se centra en la protección y defensa contra amenazas. Las fuerzas deben estar preparadas para repeler ataques en todos los dominios, desde el ciberespacio hasta el terreno físico.

El comandante debe analizar cómo las fuerzas militares y agencias no militares a su disposición pueden operar en estas capas. ¿Cómo se integran los diferentes componentes militares y agencias no militares? ¿Cómo se sincronizan los efectos y cómo se coordinan las acciones en diferentes dominios?

La eficacia radica en la capacidad de las fuerzas para adaptarse rápidamente y coordinar acciones conjuntas. Esto implica el conocimiento profundo de los parámetros a tener en cuenta para diseñar las fuerzas que conformarán el orden de batalla.

La guerra en Ucrania en 2014 fue el punto de inflexión que obligó al Ejército de los Estados Unidos (en adelante US Army) a reevaluar su doctrina<sup>1</sup>. Durante las últimas décadas, el US Army estuvo a la vanguardia en el desarrollo de doctrinas para el empleo del poder militar,

---

<sup>1</sup> Conjunto de principios, conceptos y normas que guían la organización, el entrenamiento y el empleo de las fuerzas armadas en diferentes situaciones. Es un marco teórico y práctico que proporciona orientación sobre cómo deben llevarse a cabo las operaciones militares, asegurando coherencia y efectividad en el desempeño de las misiones asignadas.

desde la doctrina de *Active Defense*<sup>2</sup> en la década del 70, pasando por el *Airland Battle*<sup>3</sup> en la siguiente década, hasta la doctrina del *Full Spectrum Operations*<sup>4</sup> en los primeros años del presente milenio, orientado básicamente a operaciones militares de baja intensidad, producto de su intervención en Iraq y Afganistán.

Según Monge (2020), esta situación fue aprovechada por sus principales competidores, Rusia y China, quienes durante esos años habían estudiado cuidadosamente la forma de operar del US Army, desarrollando su propia doctrina, conocida como Anti-Acceso/Denegación de Área (en adelante A2/AD).

Esta doctrina, la A2/D2, se sustenta en generar las capacidades para impedir a un oponente ingresar en la zona de operaciones, buscando aislar sus componentes e imposibilitando su apoyo mutuo. Es decir, busca proyectar su poderío militar y al mismo tiempo evita que Estados Unidos y sus aliados hagan lo mismo (García, 2021). A partir de ese momento, las fuerzas armadas de Estados Unidos, luego de analizar que no estaban preparadas para un enfrentamiento de alta intensidad contra sus principales oponentes, vieron la necesidad de cambiar el paradigma en la forma de hacer la guerra vigente en ese momento, y transformarlo al desarrollo de operaciones multidominio.

El General David Perkins (2017), fue quien introdujo el concepto de *Multi-Domain Battle*. Este enfoque, que todavía no era doctrina, reconoce que las operaciones militares ya no se limitan a un solo dominio (como tierra, aire o mar), sino que se entrelazan en múltiples dominios.

Años más tarde, el US Army tomó este enfoque y lo convirtió en doctrina. Según la misma, las operaciones multidominio consisten en el empleo de las capacidades conjuntas de distintas armas, para crear y explotar ventajas relativas que logren objetivos, derroten a las fuerzas enemigas y consoliden ganancias (US Army, 2022).

Según el Estado Mayor Conjunto de las Fuerzas Armadas, las operaciones multidominio es un conjunto de operaciones militares que son planificadas por el nivel operacional, donde las capacidades modulares de cualquier dominio convergen en otro, lo que crea un dilema para el oponente y brinda una oportunidad para obtener el objetivo deseado. Estas operaciones se llevan a cabo a un ritmo y alcance elevados, con el objetivo de sincronizar

---

<sup>2</sup> Doctrina basada en la necesidad de producir gran desgaste y destrucción en un escenario definido y con un enemigo concreto. Busca la batalla decisiva.

<sup>3</sup> Doctrina basada en la maniobra. Busca la desarticulación del enemigo, no su destrucción.

<sup>4</sup> Doctrina basada en la idea de que las operaciones militares deben considerar todos los aspectos del conflicto, más allá de simplemente la lucha armada. Abordan una amplia gama de actividades, incluyendo operaciones ofensivas, defensivas, estabilización y apoyo a la sociedad civil.

sus efectos y generar un dilema cognitivo en el oponente que afecte su capacidad de tomar decisiones en un momento específico, impactando en sus vulnerabilidades críticas. Las capacidades modulares son reorganizadas y reconstituidas a medida que el comandante diseña la maniobra operacional para mantener la iniciativa (EMCO, 2023b).

Surge de este modo, un concepto disruptivo, que conjuga aspectos sobresalientes de las operaciones multidominio con los avances tecnológicos en materia de inteligencia artificial (IA) y empleo masivo de sistemas aéreos no tripulados (SANT). Este concepto es la guerra mosaico

La guerra mosaico, tiene sus antecedentes en la investigación del *Research and Development Corporation* (RAND) a través de sus investigadores Arquilla y Rostfield (2000) en su obra “*Swarming & The Future Conflict*”, donde estableció la utilización de tácticas tipo enjambre, donde pequeñas unidades, grupos e individuos pueden conectarse y actuar en forma conjunta mediante la adopción de formas de organización en red y doctrinas, estrategias y tecnologías relacionadas. (p. 2).

Una de las agencias que investigó esta tendencia, fue la *Defence Advanced Research Projects Agency* (DARPA), quién a través de Subdirector de la *Strategic Technology Office*, Dan Patt, define un nuevo concepto para operacionalizar una forma eficiente de llevar a cabo las operaciones multidominio, es decir la guerra mosaico.

De estos conceptos, se desprende la importancia de la interoperabilidad, la adaptabilidad y la modularidad con factores esenciales para el diseño de fuerzas que serán puesta a disposición de un comandante en un teatro de operaciones.

Los aportes al campo disciplinar son contribuir, desde el punto de vista del diseño y organización de fuerzas, al proceso de planeamiento que se realiza en el nivel operacional en un conflicto de carácter multidominio.

El alcance de la presente investigación consistirá en analizar las operaciones multidominio y la implementación de estos conceptos doctrinales en la conformación de fuerzas en conflictos actuales e hipotéticos, con un enfoque en los próximos 10 años.

El interrogante de investigación es ¿Qué parámetros se deberán tener en cuenta para el diseño de fuerzas que tendrá el comandante del teatro de operaciones a disposición para la ejecución de operaciones multidominio?

Para la presente investigación se propone un enfoque cualitativo para analizar la conformación de las fuerzas disponibles para el comandante del teatro de operaciones durante las operaciones multidominio.

El diseño de la investigación será explicativo, con el objetivo de comprender y describir los parámetros esenciales en el diseño de fuerzas. Se utilizarán tres técnicas de validación: análisis bibliográfico, análisis documental y análisis lógico. Estas técnicas me permitirán evaluar la coherencia y validez de los argumentos y conclusiones.

El objetivo general es establecer los parámetros de diseño de fuerzas militares a disposición del comandante del teatro de operaciones para la ejecución de operaciones multidominio, y los objetivos específicos son a) describir las operaciones multidominio y la guerra mosaico en el marco de la concepción estratégica de Capas, Restricción de Área y Operaciones Multidominio y b) definir y sintetizar los parámetros para el diseño de las fuerzas a disposición del comandante del teatro de operaciones.

La hipótesis será: el análisis de los parámetros de diseño de las fuerzas a emplear en un teatro de operaciones facilitará el establecimiento de previsiones para la conformación de fuerzas interoperables, modulares y adaptables a los conflictos multidominio.

El presente trabajo está dividido en dos capítulos, el primero dedicado a la interpretación de las operaciones multidominio y guerra mosaico en el marco de la concepción estratégica de Capas, Restricción de Área y Operaciones Multidominio y el segundo dedicado al análisis de los parámetros de diseño de una fuerza multidominio.

## Capítulo 1

### Operaciones Multidominio y la Guerra Mosaico en el Marco de la Concepción Estratégica de Capas, Restricción de Área y Operaciones Multidominio

#### 1.1. Introducción a las Operaciones Multidominio

Las operaciones multidominio representan una de las evoluciones más significativas en la doctrina militar moderna. Este enfoque, al integrar las capacidades en dominios tradicionales y emergentes, busca asegurar una superioridad en el combate que permite adaptarse a escenarios operativos complejos y en cambio constante. Su aplicación abarca los dominios terrestre, marítimo, aéreo, espacial, ciberespacial y cognitivo, los cuales no solo son explotados de manera individual sino, principalmente, de manera sinérgica, logrando así maximizar los efectos de las operaciones militares de forma integrada y coordinada.

Este tipo de operaciones son especialmente relevantes en el contexto actual, donde las amenazas a la seguridad nacional se han vuelto cada vez más sofisticadas y requieren respuestas rápidas y adaptativas. La introducción del concepto multidominio responde a la necesidad de enfrentar adversarios que también emplean tácticas avanzadas, como las estrategias de denegación de área (A2/AD), que buscan limitar la libertad de acción en ciertos espacios estratégicos (Clark, Patt, & Walton, 2021). De acuerdo con Pulido (2021), la coordinación en múltiples dominios permite que las fuerzas se desplieguen de manera flexible, sincronizando los recursos de cada Fuerza Armada y diferentes agencias, lo que es crucial para optimizar la efectividad operativa en contextos de alta incertidumbre.

Las Fuerzas Armadas de Estados Unidos han liderado el desarrollo de las operaciones multidominio, integrando tecnologías avanzadas y doctrinas innovadoras. Su concepto de *Joint All-Domain Command and Control* (JADC2) (Department of Defense, 2022), busca una sincronización total de fuerzas terrestres, aéreas, marítimas, espaciales y cibernéticas. Este sistema emplea inteligencia artificial y análisis de datos en tiempo real para garantizar una toma de decisiones informada y descentralizada.

De la observación de estas Fuerzas Armadas de Estados Unidos, se pueden extraer que:

- La interoperabilidad tecnológica es crucial para la coordinación efectiva entre las diferentes Fuerzas Armadas.
- La descentralización en la toma de decisiones permite una respuesta ágil frente a amenazas dinámicas (Clark, Patt, & Walton, 2021).
- La utilización de inteligencia artificial y sistemas autónomos potencia la modularidad y adaptabilidad de las fuerzas.

Rusia ha implementado estrategias de negación A2/AD para proteger regiones clave como Kaliningrado y Crimea, utilizando una combinación de sistemas de defensa aérea de largo alcance (S-400), misiles antibuque y capacidades cibernéticas. Estas estrategias buscan limitar el acceso de fuerzas adversarias y establecer un control territorial estratégico (Pifer, 2022).

China ha desarrollado sus propias capacidades A2/AD avanzadas para proteger sus intereses en el Mar de China Meridional con sistemas de misiles balísticos antibuque, SANT de vigilancia y plataformas de IA para monitorear y responder a incursiones. Su doctrina multidominio incluye la integración de capacidades espaciales y cibernéticas que permite asegurar la superioridad en escenarios de conflicto regional.

Las estrategias chinas destacan la importancia de la modularidad y la escalabilidad en fuerzas multidominio para responder tanto a conflictos de baja como de alta intensidad (Grayson & Lilliu, 2021).

### ***1.1.1. Casos Relevantes***

Resulta de suma importancia, rescatar los aspectos más importantes de los conflictos en desarrollo, en lo cuales se puede observar la aplicación de los conceptos desarrollados precedentemente

**La Guerra entre Rusia y Ucrania.** Esta guerra en desarrollo esta demostrando cómo un adversario puede emplear tácticas multidominio para maximizar su efectividad. Rusia ha combinado desde operaciones terrestres tradicionales con ataques cibernéticos, el uso de SANT para reconocimiento y ataques hasta operaciones información.

Mientras que las fuerzas ucranianas han demostrado adaptabilidad al integrar SANT de uso civil masivamente para reconocimiento, el desarrollo de capacidades cibernéticas defensivas y la coordinación de sus operaciones terrestres y aéreas de manera descentralizada. Estas tácticas resaltan la importancia de la interoperabilidad y la modularidad para contrarrestar fuerzas superiores en número y tecnología (Pifer, 2022).

**Israel y el Conflicto Gaza.** Israel está empleando un enfoque multidominio en sus operaciones militares contra grupos insurgentes en Gaza, Siria y Libano. Un ejemplo destacado son los "beepers", dispositivos móviles utilizados para la coordinación y comunicación de operaciones militares. Este método combina el dominio cognitivo (protección de la narrativa y minimización de daños colaterales) con capacidades de ataque aéreo precisas.

### ***1.1.2. Componentes Clave de las Operaciones Multidominio***

Las operaciones multidominio requieren la integración de cinco componentes estratégicos fundamentales, que son los pilares de su efectividad:

- Sincronización de fuerzas y recursos que asegure que las diferentes Fuerzas Armadas actúen en conjunto para maximizar sus capacidades y minimizar las vulnerabilidades. Esto implica una cooperación operativa que se extiende a todos los niveles de la conducción, garantizando que los recursos se desplieguen de manera eficiente y que los objetivos se logren evitando la duplicación de esfuerzos.
- Interoperabilidad tecnológica que permita integrar sistemas de armas y plataformas de información entre las diferentes fuerzas. En este sentido, el desarrollo de tecnologías de comunicación seguras permitirá al comandante del teatro de operaciones recibir y compartir información crítica en cada dominio, facilitando la toma de decisiones informada y rápida.
- Flexibilidad y adaptabilidad en la estructura de fuerzas que permita reorganizarse según las necesidades de cada misión. Esto incluye la capacidad de responder a amenazas en tiempo real mediante el reagrupamiento de unidades y la asignación de recursos en diferentes áreas.
- La incorporación de tecnología avanzada juega un papel central en las operaciones multidominio, ya que permite el uso de SANT y sistemas autónomos en el campo de batalla. Estos sistemas se integran en cada uno de los dominios operativos y refuerzan las capacidades de vigilancia, reconocimiento y ataque. La incorporación de tecnologías de IA también facilita la toma de decisiones en situaciones complejas, al analizar grandes cantidades de datos en tiempo real y ofrecer recomendaciones basadas en algoritmos predictivos (Scharre, 2018).
- Toma de decisiones descentralizada que permita a los jefes y comandantes tomar decisiones en el momento, en función de la información disponible, sin tener que esperar órdenes de niveles superiores. La capacidad de operar con una toma de decisiones descentralizada permite que las operaciones se mantengan fluidas y dinámicas, adaptándose a condiciones cambiantes (Ver Anexo 1).

### ***1.1.3. Aplicación en el Contexto de Defensa Nacional***

En el marco de la defensa nacional, las operaciones multidominio brindan una ventaja significativa. Su implementación refuerza las capacidades de las capas Conjurar y Repeler, integrando los recursos de cada fuerza en una estructura unificada que permite respuestas rápidas y coordinadas frente a un potencial agresor. La capacidad de operar en varios dominios también mejora la efectividad de las fuerzas en situaciones de crisis, permitiendo una defensa efectiva y flexible de puntos estratégicos, como las fronteras, zonas marítimas y espacios aéreos.

Este marco permite que las fuerzas respondan no solo a amenazas convencionales, sino también a desafíos asimétricos, como el ciberterrorismo y los ataques en el ciberespacio. La implementación de una estrategia multidominio proporciona una capacidad disuasiva que incrementa la seguridad nacional frente a las amenazas emergentes.

## **1.2. Definición y Principios de la Guerra Mosaico**

La guerra mosaico (Anexo 2) es un concepto relativamente reciente que se basa en la creación de fuerzas modulares y adaptables, diseñadas para operar en redes de unidades pequeñas, autónomas y reconfigurables. A diferencia de las estrategias militares convencionales, que suelen depender de plataformas grandes y monolíticas, la guerra mosaico emplea múltiples nodos, más pequeños, distribuidos y conectados, que pueden reorganizarse y adaptarse según las necesidades tácticas del campo de batalla. Este enfoque ofrece una ventaja significativa frente a adversarios que utilizan sistemas de defensa centralizados, permitiendo que las fuerzas mosaico operen en un entorno descentralizado y flexible (Clark, Patt, & Walton, 2021).

### ***1.2.1. Fundamentos de la Guerra Mosaico***

La guerra mosaico se desarrolló en respuesta a la creciente sofisticación de las amenazas y la necesidad de aumentar la velocidad de adaptación en el campo de batalla. Este enfoque permite una mayor resiliencia y capacidad de respuesta en entornos de alta incertidumbre y volatilidad. El aprovechamiento de tecnologías avanzadas, como la IA, los sistemas autónomos y la comunicación segura en red, permiten a unidades individuales actuar de manera autónoma mientras se mantienen coordinadas en tiempo real con el resto de la estructura de combate (Grayson & Lilliu, 2021).

La naturaleza distribuida de la guerra mosaico proporciona una resistencia inherente a las vulnerabilidades, si una unidad o plataforma es neutralizada, el resto de la red puede continuar operando sin afectar significativamente la misión general. Esto se debe a que la guerra mosaico no depende de activos críticos individuales, sino que se basa en la redundancia y la adaptabilidad de las unidades en un sistema mosaico. Así, este modelo de organización descentralizada permite que los comandantes en el campo de batalla ajusten y modifiquen las configuraciones de las fuerzas en función de las amenazas y las oportunidades emergentes, sin depender de órdenes centralizadas.

### ***1.2.2. Principios Clave de la Guerra Mosaico***

La guerra mosaico se estructura en torno a varios principios clave, que optimizan su efectividad y flexibilidad en el combate. Estos principios son los siguientes:

- Modularidad y reconfiguración rápida permitiendo que las unidades y sistemas se agrupen o separen de acuerdo con las necesidades del entorno operativo. Cada módulo puede funcionar de manera independiente o en combinación con otros, creando configuraciones adaptativas. Este principio es esencial para asegurar que las fuerzas puedan reconfigurarse rápidamente, incluso durante las operaciones, permitiendo ajustes constantes ante el cambio de condiciones en el campo de batalla (Pulido, 2021).
- La guerra mosaico permite una mayor autonomía y descentralización para los comandantes de menor rango y las unidades individuales. Esta autonomía es posible gracias a sistemas avanzados de IA y comunicación en tiempo real, que proporcionan a las unidades acceso a información clave sin depender de niveles superiores. La descentralización facilita una toma de decisiones más ágil, donde las unidades pueden actuar de forma inmediata y adaptarse según las circunstancias tácticas sin esperar directrices centralizadas (Clark, Patt, & Schramm, 2020).
- Interoperabilidad y conectividad en red. La guerra mosaico requiere que los sistemas de comunicación, sensores y plataformas de armas sean compatibles y capaces de intercambiar datos en tiempo real. Esta conectividad en red permite una coordinación que maximiza la efectividad de las operaciones, asegurando que los diferentes módulos puedan comunicarse entre sí y coordinar acciones en función de los cambios en el entorno (ESFAS, 2022).
- Redundancia y resiliencia operacional. La guerra mosaico no depende de activos únicos o críticos, sino que distribuye capacidades y responsabilidades en una red de unidades interconectadas. Esto crea una resiliencia significativa, ya que incluso si una parte del sistema es neutralizada, las unidades restantes pueden continuar operando sin interrupciones en la misión. La redundancia de funciones asegura que las capacidades críticas estén distribuidas en múltiples módulos, lo cual permite sostener las operaciones incluso en caso de pérdidas parciales de recursos (Fuerza 35, Ejército de Tierra, 2023).
- Adaptación continua a amenazas dinámicas, la guerra mosaico está diseñada para enfrentar amenazas cambiantes y dinámicas mediante una capacidad de adaptación constante. Las unidades pueden recibir actualizaciones de misión o reconfigurarse rápidamente para adaptarse a nuevas tácticas o tecnologías del adversario. La capacidad de adaptación es fundamental en el contexto actual, donde las amenazas evolucionan rápidamente y las fuerzas deben responder en tiempo real a cambios en el entorno (Grayson & Lilliu, 2021).

### ***1.2.3. Ventajas Estratégicas de la Guerra Mosaico***

La implementación de la guerra mosaico presenta ventajas estratégicas significativas en un escenario de operaciones multidominio. Estas ventajas particularmente relevantes son esenciales para enfrentar amenazas tanto convencionales como asimétricas (Anexo 3):

- Mayor resiliencia frente a la Negación de Área (A2/AD). La capacidad de las unidades mosaico para operar de manera dispersa y autónoma reduce su vulnerabilidad a sistemas de defensa de largo alcance. Además, la reconfiguración continua de las unidades impide que el enemigo logre una ventaja táctica al enfocarse en un objetivo fijo o concentrado (Pulido, 2021).
- Capacidad para generar dilemas operacionales al enemigo. La distribución de funciones entre nodos pequeños y autónomos genera una serie de objetivos que el enemigo debe enfrentar, lo cual diluye sus capacidades y aumenta el riesgo de saturación. Este efecto es particularmente útil para contrarrestar fuerzas superiores en número o tecnología, ya que la guerra mosaico obliga a los adversarios a dividir sus recursos en múltiples amenazas simultáneas (Clark, Patt, & Schramm, 2020).
- Flexibilidad para la adaptación rápida en el campo de batalla, clave para enfrentar amenazas asimétricas, como los ataques cibernéticos o las incursiones rápidas en áreas críticas, ya que permite que las fuerzas reconfiguren sus recursos sin necesidad de una reorganización extensa o prolongada. La capacidad de adaptación rápida también permite que los comandantes respondan de manera efectiva a amenazas emergentes y cambien las prioridades tácticas según sea necesario (ESFAS, 2022).
- Eficiencia en el uso de recursos y reducción de costos operacionales. La estructura modular y descentralizada de la guerra mosaico ofrece una ventaja en términos de costos, ya que permite a las fuerzas optimizar el uso de recursos al reducir la dependencia de grandes plataformas de armas. Los nodos pequeños y autónomos requieren menos mantenimiento y son más económicos de operar y reemplazar en comparación con plataformas monolíticas (Fuerza 35, Ejército de Tierra, 2023).

### **1.3. Capas Conjurar y Repeler**

Las capas Conjurar y Repeler constituyen el núcleo de la defensa activa, siendo las encargadas de la respuesta militar frente a una agresión en progreso. Estas capas se alinean con los principios de las operaciones multidominio, que maximizan la integración y coordinación entre las diferentes fuerzas en múltiples dominios (terrestre, aéreo, marítimo, ciberespacial y

cognitivo), lo que permite que la defensa se ejecute de manera coordinada y efectiva en entornos complejos y cambiantes.

La concepción de las capas Conjurar y Repeler responde a la necesidad de organizar las fuerzas de manera flexible y adaptable para responder a una amplia gama de amenazas. En el contexto actual, donde los riesgos para la seguridad nacional incluyen no solo ataques convencionales sino también amenazas asimétricas y cibernéticas, estas capas estratégicas permiten estructurar una defensa activa, que anticipe y enfrente al enemigo de forma escalonada y decisiva (Pulido, 2021).

### ***1.3.1. Capa Conjurar***

La capa Conjurar se enfoca en el debilitamiento de las capacidades ofensivas del adversario mediante una estrategia de desgaste y contención. Su objetivo principal es degradar el poder militar del enemigo, obstaculizando sus avances y afectando su logística y cohesión de combate. En términos de operaciones multidominio, la capa Conjurar implica el uso de tecnologías avanzadas, como sistemas de vigilancia y reconocimiento en tiempo real, para detectar y neutralizar amenazas antes de que se acerquen a áreas críticas del territorio nacional.

La capa Conjurar utiliza una estrategia multidominio que combina los recursos en los dominios terrestre, aéreo y ciberespacial para generar una red de defensa que disuada y frustre los movimientos iniciales del enemigo. Esto implica el uso de tecnologías de mando y control que facilitan la comunicación entre las diferentes fuerzas en tiempo real, asegurando que las operaciones en los diversos dominios se sincronicen de manera efectiva.

En el marco de la guerra mosaico, la capa Conjurar se beneficia de la capacidad de emplear unidades modulares y autónomas que pueden ser desplegadas y reorganizadas rápidamente para adaptarse a la situación en tiempo real. Este enfoque fragmentado, que integra SANT, sensores y unidades de combate ligero, permite responder a incursiones y ataques en diversos dominios simultáneamente, generando un entorno de alto riesgo y complejidad para el adversario (Clark, Patt, & Schramm, 2020).

### ***1.3.2. Capa Repeler***

La capa Repeler está orientada a la defensa directa frente a un enemigo que ha logrado penetrar los niveles iniciales de la defensa nacional. Su objetivo es neutralizar la amenaza mediante el uso concentrado de poder militar, en una fase avanzada del conflicto. La estructura y despliegue de fuerzas en esta capa reflejan la necesidad de una respuesta decisiva y contundente, con un enfoque que privilegia la letalidad y la destrucción de las capacidades operativas del adversario. El objetivo principal de la capa Repeler es brindar una respuesta de alta intensidad en áreas donde el enemigo ha establecido posiciones o ha alcanzado líneas de

avance crítico. Este enfoque busca emplear fuerzas altamente preparadas y con un nivel de integración operacional avanzado, permitiendo el uso coordinado de las capacidades de fuego, ataque aéreo y maniobra terrestre para rechazar al adversario de territorio nacional. La capa Repeler puede involucrar operaciones complejas y de gran escala, diseñadas para recuperar rápidamente el control de áreas estratégicas (Pulido, 2021).

La estructura de las fuerzas en la capa Repeler aprovecha la modularidad que caracteriza a la guerra mosaico, permitiendo que las unidades se agrupen y reorganicen en función de la situación táctica. Esta flexibilidad es fundamental para ajustar los recursos y fuerzas en tiempo real, maximizando la efectividad de las operaciones en distintos dominios. La escalabilidad de las unidades permite que el comandante del teatro de operaciones dirija los recursos de forma dinámica, empleando configuraciones específicas según la fase de combate y la naturaleza del adversario (Mercado, 2024).

### ***1.3.3. Sinergia entre las Capas Conjurar y Repeler***

El modelo en capas, integrado con la doctrina de operaciones multidominio, asegura una continuidad operativa en el tiempo y espacio, maximizando la eficiencia de los recursos nacionales en cada fase del conflicto. La combinación de estas capas con un enfoque modular y escalable, apoyado por tecnología avanzada y sistemas autónomos, permite actuar con flexibilidad y velocidad, garantizando una defensa sólida y adaptable.

## Capítulo 2

### Parámetros para el Diseño de Fuerzas Multidominio para el Teatro de Operaciones

#### 2.1. Modularidad en el Diseño de Fuerzas Multidominio

La modularidad es uno de los parámetros centrales en el diseño de fuerzas multidominio. Este enfoque permite que los elementos de combate, inteligencia y apoyo logístico se organicen y reorganicen en configuraciones adaptativas, optimizando la capacidad de respuesta un contexto operativo complejo y dinámico. La modularidad implica la creación de unidades que pueden actuar de manera autónoma o en combinación con otras, facilitando la integración de diferentes capacidades en función de las necesidades tácticas y operacionales del teatro de operaciones. La guerra mosaico, en particular, aprovecha esta estructura modular para maximizar la flexibilidad y resistencia de las fuerzas, proporcionando a los comandantes una capacidad de respuesta rápida y ajustable en múltiples dominios (Clark, Patt, & Walton, 2021).

##### 2.1.1. *Fundamentos y Objetivos de la Modularidad*

El objetivo principal de la modularidad en las fuerzas multidominio es permitir la rápida adaptación y reorganización de los elementos según el tipo de misión y las condiciones del entorno. Según Grayson y Lilliu (2021), el diseño modular asegura que las fuerzas puedan fragmentarse en componentes más pequeños y especializarse para ejecutar tareas específicas, como exploración y reconocimiento, ataque o defensa, de manera autónoma y sin dependencia de plataformas centralizadas. Esta capacidad de reconfiguración no solo mejora la flexibilidad táctica, sino que también incrementa la resiliencia de las fuerzas, permitiendo una respuesta efectiva ante daños parciales o pérdidas de unidades.

Al operar en estructuras modulares, las fuerzas pueden maximizar la eficiencia de sus recursos, asignando capacidades específicas a cada misión sin necesidad de movilizar unidades de gran tamaño. Esto se alinea con la concepción estratégica en las capas Conjurar y Repeler, que exigen respuestas adaptativas y escalables frente a distintos niveles de amenaza (Pulido, 2021).

##### 2.1.2. *Modularidad y Despliegue Rápido en el Teatro de Operaciones*

La modularidad permite que los elementos dispongan de unidades que puedan desplegarse y adaptarse rápidamente en función de los requerimientos del entorno operativo. Durante la fase de Conjurar, unidades mosaico de exploración, reconocimiento y vigilancia pueden ser movilizadas de manera rápida para identificar y monitorear amenazas potenciales en áreas estratégicas. Estas unidades ligeras y flexibles permiten una respuesta ágil y eficaz, brindando al comandante del teatro de operaciones información en tiempo real para la toma de

decisiones. En la fase de Repeler, la modularidad facilita la agrupación de unidades de ataque en configuraciones de mayor escala, maximizando el impacto ofensivo y permitiendo una defensa integral en situaciones de alta intensidad (Mercado, 2024).

La capacidad de reorganizar las unidades de manera ágil y de ajustarlas a la intensidad del conflicto es crucial para enfrentar amenazas en varios dominios, como el ciberespacio, el aire y el terreno. Esta flexibilidad asegura que las fuerzas no solo se desplieguen rápidamente, sino que también se ajusten en función de los cambios en el entorno de combate, manteniendo una ventaja táctica y operativa en el teatro de operaciones (ESFAS, 2022).

### ***2.1.3. Integración de Tecnología Autónoma en Unidades con Capacidades Modulares***

La integración de tecnología autónoma, como SANT, robots y IA, optimiza aún más el rendimiento de las unidades con capacidades modulares. En el contexto de la guerra mosaico, la tecnología autónoma complementa la modularidad, permitiendo que cada unidad funcione como un nodo autónomo en una red interconectada, generando una resiliencia significativa ante pérdidas o daños. Scharre (2018) argumenta que los sistemas autónomos mejoran la capacidad de las fuerzas para operar en ambientes de riesgo elevado, minimizando la exposición de los soldados y reduciendo la dependencia de activos humanos para tareas de alta peligrosidad.

En la capa Conjurar, los SANT de vigilancia y reconocimiento pueden actuar de manera independiente o en conjunto con otras unidades mosaico para realizar tareas de observación y patrullaje en áreas de posible incursión. Estos sistemas autónomos permiten una supervisión continua y detallada, lo cual es especialmente relevante en el contexto nacional, donde la extensión territorial y la diversidad geográfica exigen una cobertura eficaz y económica (Pulido, 2021).

Durante las operaciones en la capa Repeler, la IA facilita el análisis y la coordinación de las unidades mosaico, optimizando la asignación de recursos y ajustando las tácticas en función de los movimientos del enemigo. La IA permite que las unidades autónomas colaboren entre sí, analicen patrones de comportamiento enemigo y anticipen acciones, brindando a los comandantes datos clave para realizar ajustes tácticos en tiempo real. Esta capacidad de integración tecnológica es fundamental para asegurar que las fuerzas puedan adaptarse de manera rápida y eficaz, maximizando su capacidad de respuesta en momentos críticos (Grayson & Lilliu, 2021).

## **2.2. Interoperabilidad en las Fuerzas Multidominio**

La interoperabilidad es un principio crucial para la efectividad de las fuerzas multidominio, ya que permite la coordinación y colaboración fluida entre las diferentes Fuerzas

Armadas con agencias de seguridad y defensa del Estado, así como con fuerzas de estados aliados. En un escenario de operaciones multidominio, la interoperabilidad asegura que las fuerzas puedan actuar de manera sinérgica en todos los dominios operativos: terrestre, marítimo, aéreo, espacial, cibernético y de información. Esta integración es fundamental para optimizar la efectividad de las operaciones en un entorno de alta complejidad y adaptarse a las exigencias de las capas estratégicas Conjurar y Repeler.

### **2.2.1. Fundamentos y Objetivos de la Interoperabilidad**

El objetivo de la interoperabilidad en el diseño de fuerzas multidominio es permitir una comunicación y coordinación efectiva entre todas las unidades y plataformas, independientemente de su dominio o fuerza. La interoperabilidad debe garantizar que los sistemas de armas, las plataformas de comunicación y las unidades operativas puedan integrarse y actuar en un marco conjunto, evitando duplicidades y maximizando la eficiencia de los recursos disponibles (ESFAS, 2022). Permite que el comandante del teatro de operaciones pueda dirigir las fuerzas de manera unificada y con una visión completa del campo de batalla. La interoperabilidad también es esencial para que las diferentes fuerzas y agencias puedan ejecutar misiones conjuntas y combinadas de manera fluida, adaptándose rápidamente a los cambios en el ambiente operacional, lo cual es fundamental para la ejecución de operaciones en las capas Conjurar y Repeler.

### **2.2.2. Interoperabilidad en la Capa Conjurar**

La interoperabilidad en esta fase asegura que las unidades de distintas fuerzas y agencias puedan coordinarse para realizar operaciones preventivas y defensivas en varios dominios, como el aéreo, terrestre y cibernético. Esta integración permite que las fuerzas respondan de manera ágil y sinérgica frente a una amenaza potencial, utilizando tanto sistemas de vigilancia aérea como ciberdefensa para anticipar y neutralizar posibles ataques. En esta capa, la interoperabilidad facilita el uso conjunto de unidades de reconocimiento de la Fuerza Aérea y la Armada para monitorear espacios aéreos y marítimos, mientras que el Ejército proporciona apoyo en tierra. De esta forma, las fuerzas pueden realizar una vigilancia constante y coordinada en áreas estratégicas. La interoperabilidad es clave para que las fuerzas puedan compartir información de inteligencia en tiempo real, lo cual es esencial para una disuasión efectiva.

La interoperabilidad también es crucial para la ciberdefensa, ya que permite la integración de sistemas de información y comunicación en una red segura y resiliente. Esto asegura que las fuerzas armadas y agencias puedan detectar y responder a ataques cibernéticos dirigidos a sus infraestructuras críticas. De acuerdo con Pulido (2021), la interoperabilidad en

el ciberespacio permite que los equipos de ciberseguridad de diferentes fuerzas actúen de manera coordinada para prevenir la infiltración del enemigo y proteger la infraestructura de comunicaciones.

### ***2.2.3. Interoperabilidad en la Capa Repeler***

La interoperabilidad en esta fase es vital para que las unidades de las diferentes fuerzas actúen como un solo conjunto y maximicen el poder de fuego y maniobra. En esta capa, la interoperabilidad garantiza que las unidades terrestres, marítimas y aéreas puedan actuar de manera sincronizada en operaciones de contraataque y expulsión del enemigo.

En esta fase, la interoperabilidad se manifiesta en el uso de plataformas de comunicación y sistemas de armas comunes que permiten a las unidades de artillería del ejército, las unidades navales y la fuerza aérea coordinar sus ataques para maximizar el impacto en el enemigo. La estandarización de plataformas y la compatibilidad de sistemas de armas son fundamentales para asegurar una respuesta rápida y eficiente en situaciones de combate intenso (ESFAS, 2022).

La interoperabilidad también es crucial en operaciones en espacios con restricciones físicas o de alta movilidad, donde la velocidad y precisión son esenciales. La capacidad de operar con fuerzas con capacidades modulares permite que las unidades aéreas y terrestres sincronicen sus movimientos para neutralizar rápidamente las posiciones enemigas. Esto asegura que las fuerzas puedan mantener una ventaja en situaciones de conflicto de alta intensidad, adaptando sus operaciones a los requerimientos específicos del entorno operacional (Mercado, 2024).

### ***2.2.4. Desafíos y Soluciones en la Interoperabilidad***

La implementación de la interoperabilidad en las fuerzas multidominio presenta desafíos logísticos, técnicos y doctrinales. Entre los principales obstáculos se encuentran la estandarización de sistemas de comunicación y armas, la integración de plataformas de información seguras que permitan una integración fluida entre las diferentes fuerzas y agencias y el desarrollo de una doctrina conjunta que unifique los procedimientos operativos. Según el documento Fuerza 35 del Ejército de Tierra de España (2019), la implementación de la interoperabilidad también exige una infraestructura de soporte técnico que permita el mantenimiento y actualización continua de los sistemas de mando y control. Por esta razón, es fundamental la adopción de una doctrina conjunta que fomente la estandarización de plataformas y la compatibilidad de sistemas de armas. Además, es necesario implementar programas de entrenamiento conjunto y ejercicios de simulación que permitan a las unidades diferentes, trabajar juntas en escenarios de conflicto simulado, mejorando así su capacidad de

coordinación y respuesta en tiempo real. La inversión en tecnologías de comunicación seguras y resilientes también es clave para asegurar la interoperabilidad en entornos de alta amenaza, especialmente en el dominio cibernético, donde la seguridad de la información es fundamental (Grayson & Lilliu, 2021).

### **2.3. Escalabilidad y Adaptabilidad en el Teatro de Operaciones**

La escalabilidad y adaptabilidad son dos principios fundamentales en el diseño de fuerzas multidominio, que aseguran la capacidad de ajuste de las unidades militares en función de la intensidad y evolución del conflicto. En el contexto de las operaciones multidominio, la escalabilidad permite ampliar o reducir el tamaño y alcance de las fuerzas desplegadas, mientras que la adaptabilidad permite modificar la estructura y el enfoque de las fuerzas para responder de manera eficiente a las amenazas cambiantes.

#### **2.3.1. Escalabilidad en el Diseño de Fuerzas Multidominio**

La escalabilidad permite que las fuerzas puedan ajustar su tamaño y capacidades de acuerdo con las necesidades del teatro de operaciones, adaptándose tanto a conflictos de baja intensidad como a situaciones de alta intensidad. Según Clark, Patt y Walton (2021), la escalabilidad es esencial para maximizar la eficiencia de los recursos en entornos de conflicto dinámicos, permitiendo que las fuerzas incrementen o disminuyan su tamaño según la demanda operativa y los objetivos operacionales.

En la capa Conjurar, la escalabilidad permite comenzar con unidades de vigilancia y reconocimiento de menor escala, adaptadas a las primeras fases de un conflicto o para tareas de disuasión. Si la situación se intensifica, estas unidades pueden reforzarse con otros módulos operativos, como sistemas de artillería ligera, SANT de ataque y plataformas de defensa aérea. Esta capacidad escalable asegura que los recursos se utilicen de manera eficiente, incrementando la fuerza solo cuando la amenaza lo requiere (Mercado, 2024).

En la capa Repeler, la escalabilidad permite que las fuerzas se expandan rápidamente para enfrentar una amenaza de gran magnitud. Esto incluye el despliegue de unidades de combate más grandes y sistemas de armas de mayor impacto, como misiles antiaéreos, artillería pesada y fuerzas de maniobra terrestre. La escalabilidad en esta capa asegura que las fuerzas puedan responder con decisión a incursiones significativas, utilizando los recursos disponibles de manera concentrada y efectiva (ESFAS, 2022).

La escalabilidad asignar recursos de manera proporcional a la intensidad de la amenaza, optimizando el uso de los activos de combate y minimizando el desgaste innecesario de las fuerzas. Además, en el contexto de guerra mosaico, la escalabilidad facilita la reconfiguración de módulos operativos, permitiendo una expansión o reducción rápida de las capacidades en

función de la situación táctica y las necesidades del teatro de operaciones (Grayson & Lilliu, 2021).

### **2.3.2. Adaptabilidad en el Teatro de Operaciones**

La adaptabilidad permite que las fuerzas ajusten su estructura y tácticas en tiempo real, respondiendo a cambios imprevistos en el entorno de combate. En el contexto de las operaciones multidominio, la adaptabilidad es esencial para asegurar que las unidades puedan operar eficazmente en dominios terrestres, aéreos, marítimos, cibernéticos y de información, enfrentando tanto amenazas convencionales como asimétricas. Según Scharre (2018), la adaptabilidad permite que las fuerzas integren nuevas tecnologías y se ajusten rápidamente a las tácticas del enemigo, manteniendo así una ventaja táctica y operativa en el campo de batalla.

En la capa Conjurar, la adaptabilidad permite que las fuerzas ajusten sus operaciones preventivas y de vigilancia en función de la naturaleza y evolución de la amenaza. Por ejemplo, si el enemigo emplea tácticas de guerra cibernética o tecnologías de interferencia de comunicaciones, las unidades de defensa cibernética y guerra electrónica pueden adaptar sus procedimientos para proteger los sistemas de mando y control y asegurar la continuidad de las comunicaciones. Esto es fundamental para la disuasión activa, ya que permite responder a las tácticas enemigas de forma flexible y eficaz (Pulido, 2021).

Durante la capa Repeler, la adaptabilidad es crucial para ajustar la configuración y tácticas de las unidades de combate en respuesta a las condiciones cambiantes del conflicto. Esto incluye la capacidad de reorganizar las fuerzas de manera rápida, adaptando su estructura y roles en función de la posición y acciones del enemigo. La adaptabilidad en esta capa asegura que las fuerzas puedan emplear contraataques coordinados, cambiando su enfoque de defensa a ofensiva según las oportunidades y necesidades en el campo de batalla. Este principio es vital para contrarrestar la escalada de un conflicto en curso y permite que las fuerzas maximicen su efectividad en situaciones de alta intensidad (Mercado, 2024).

La adaptabilidad también se beneficia de la integración de tecnologías avanzadas, como la IA y el análisis predictivo, que facilitan la anticipación de los movimientos y tácticas del enemigo. Estas herramientas permiten analizar grandes volúmenes de datos en tiempo real, brindando a los comandantes información crítica para realizar ajustes en las tácticas y configuraciones operativas de las unidades. Según Grayson y Lilliu (2021), el uso de IA en operaciones multidominio proporciona una ventaja significativa en términos de adaptabilidad, ya que permite una respuesta rápida y ajustada a las dinámicas cambiantes del conflicto.

### **2.3.3. Sinergia entre Escalabilidad y Adaptabilidad en el Teatro de Operaciones**

La combinación de escalabilidad y adaptabilidad en las fuerzas multidominio proporciona una ventaja estratégica y operativa considerable en el teatro de operaciones. Estos principios permiten que las fuerzas respondan de manera proporcional a las amenazas, ajustando tanto su tamaño como su estructura en función de la situación operativa. Esta sinergia es particularmente efectiva en las capas Conjurar y Repeler, donde es esencial una postura de defensa flexible y escalable que asegure una respuesta eficaz frente a distintos niveles de amenaza.

La capacidad de escalar y adaptar las fuerzas permite que los comandantes modifiquen la estructura y configuración de las unidades en tiempo real, agrupando o disgregando módulos operativos según la evolución del conflicto. Esta sinergia permite que las fuerzas mantengan una ventaja táctica frente al enemigo, optimizando la asignación de recursos y asegurando que las unidades se empleen de manera eficiente y efectiva en cada etapa del conflicto (Clark, Patt, & Walton, 2021).

En la capa Conjurar, la escalabilidad y adaptabilidad permite que las unidades de reconocimiento y defensa se desplieguen de manera limitada en las fases iniciales y se amplíen rápidamente si se detecta una intensificación de la amenaza. Esta capacidad asegura que los recursos se usen de manera eficiente, incrementando la fuerza solo cuando la situación lo exige y adaptando la estructura de las unidades en función de los movimientos del enemigo.

Durante la fase de Repeler, la escalabilidad y la adaptabilidad permiten que las unidades de combate se reconfiguren para realizar contraataques en múltiples frentes, empleando tácticas y formaciones flexibles. Esta combinación asegura que las fuerzas puedan aumentar rápidamente su presencia en áreas clave, adaptándose a los cambios en el campo de batalla y manteniendo la capacidad de neutralizar al enemigo de manera efectiva. Esta sinergia permite maximizar el impacto ofensivo y asegura que las fuerzas puedan ajustar su respuesta en función de la escalada del conflicto y la posición del enemigo.

### **2.4. La Convergencia**

La convergencia es un concepto emergente en el diseño de fuerzas multidominio que destaca la integración y sincronización de capacidades de múltiples dominios para lograr efectos combinados y decisivos en el campo de batalla. Este enfoque va más allá de la mera coordinación, promoviendo una integración simultánea y dinámica de recursos, tecnologías y estrategias en tiempo real para maximizar la eficacia operativa.

### **2.4.1 Convergencia como Parámetro de Diseño**

La convergencia busca reunir las capacidades de dominios como el terrestre, marítimo, aéreo, espacial, cibernético y cognitivo en un marco operativo único, eliminando las barreras entre ellos. Este principio se centra en generar efectos sinérgicos que no serían posibles mediante la acción aislada de cada dominio. Según Grayson y Lilliu (2021), la convergencia permite a las fuerzas multidominio adaptarse rápidamente a escenarios complejos y dinámicos, explotando vulnerabilidades del adversario mediante la sincronización de esfuerzos. Las ventajas operativas de la convergencia pueden sintetizarse en:

**Efectos Combinados.** La convergencia permite que las operaciones en un dominio potencien las acciones en otros. Por ejemplo, el uso de IA para procesar datos recopilados por satélites puede guiar ataques precisos en el dominio terrestre o aéreo, maximizando la efectividad de las fuerzas (Clark, Patt, & Walton, 2021).

**Adaptabilidad en Tiempo Real.** En un entorno operativo volátil, la convergencia facilita la transición fluida entre dominios según las necesidades tácticas. Esto permite a las fuerzas responder con rapidez y flexibilidad a los movimientos del enemigo, manteniendo la iniciativa en el conflicto (Pulido, 2021).

**Reducción de Barreras entre Dominios.** La eliminación de compartimentos entre dominios garantiza que las decisiones y recursos se distribuyan eficientemente, evitando redundancias y aprovechando al máximo las capacidades disponibles.

### **2.4.2 Desafíos de la Convergencia**

Aunque la convergencia ofrece beneficios significativos, también plantea desafíos en términos de interoperabilidad tecnológica, capacitación del personal y protección de redes críticas. Según Scharre (2018), las redes de mando y control que soportan la convergencia son especialmente vulnerables a ciberataques, lo que subraya la necesidad de sistemas resilientes y protocolos de seguridad avanzados.

## **2.5. Integración de Tecnología y Sistemas Autónomos en el Diseño de Fuerzas**

### **2.5.1 Tecnología Autónoma y Operaciones en Múltiples Dominios**

La tecnología autónoma permite a las fuerzas multidominio realizar tareas de vigilancia, reconocimiento y ataque en áreas de alto riesgo, minimizando la exposición del personal. Los sistemas autónomos, como SANT de vigilancia y robots de reconocimiento, permiten monitorear espacios aéreos, terrestres y marítimos sin comprometer la seguridad de las tropas. Este enfoque es fundamental en el contexto de operaciones multidominio, donde es necesario mantener un control constante en varios dominios simultáneamente. Según Scharre (2018), la tecnología autónoma proporciona a los comandantes una ventaja significativa en

términos de vigilancia continua y recopilación de datos en tiempo real, facilitando la toma de decisiones informada en un entorno de alta incertidumbre.

En la capa Conjurar, los SANT de reconocimiento permiten una vigilancia constante en zonas estratégicas y el monitoreo de las áreas donde se anticipa una posible incursión. Estos SANT recopilan datos en tiempo real sobre la presencia y movimientos del enemigo, proporcionando a los comandantes información crucial para evaluar la situación y activar las fuerzas preventivas si es necesario.

En la fase de Repeler, los SANT de ataque y los STNT (sistemas terrestres no tripulados) pueden utilizarse para realizar ataques selectivos y de precisión contra posiciones enemigas, maximizando la letalidad y minimizando la exposición de las tropas. La capacidad de estos sistemas autónomos para operar en conjunto y atacar desde múltiples frentes permite que las fuerzas saturen las defensas del enemigo y aumenten la efectividad de sus ofensivas. Además, estos sistemas permiten actuar rápidamente ante cualquier amenaza que haya superado las capas de disuasión y contención, asegurando que el poder de fuego se concentre en puntos estratégicos en el momento adecuado (Grayson & Lilliu, 2021).

### ***2.5.2. Inteligencia Artificial y Análisis de Datos en Tiempo Real***

La IA y el análisis de datos en tiempo real son componentes clave para optimizar la toma de decisiones en las fuerzas multidominio. La IA permite analizar grandes volúmenes de datos de manera rápida y eficiente, identificando patrones y tendencias que pueden anticipar las acciones del enemigo. Esta capacidad es especialmente importante en operaciones multidominio, donde los datos recopilados desde diversos sensores, drones y redes de comunicación deben procesarse de manera instantánea para apoyar las decisiones tácticas.

En la fase de Conjurar, la IA se utiliza para procesar datos de vigilancia y crear modelos predictivos que anticipen las tácticas y movimientos del enemigo. Por ejemplo, si los SANT de reconocimiento detectan patrones de movimiento sospechosos en las cercanías de una zona de interés estratégico, la IA puede analizar esos datos y alertar a los comandantes sobre la posible incursión. La capacidad de analizar y predecir amenazas es crucial para activar mecanismos de respuesta anticipada y evitar que el enemigo obtenga una ventaja inicial (ESFAS, 2022).

Durante las operaciones de Repeler, la IA proporciona a los comandantes análisis en tiempo real que les permiten ajustar sus estrategias y tácticas de manera dinámica. Por ejemplo, si las unidades de combate detectan cambios en la disposición o formación del enemigo, la IA puede sugerir ajustes en la configuración de las fuerzas para optimizar su impacto. Esta capacidad permite una adaptación inmediata en el campo de batalla, facilitando que las fuerzas

respondan con precisión a los movimientos del enemigo y mantengan la ventaja táctica en situaciones de combate de alta intensidad (Scharre, 2018).

### **2.5.3. *Sistemas de Mando y Control Avanzados***

Los sistemas de mando y control avanzados son esenciales para la coordinación de las fuerzas en un entorno multidominio. Estos sistemas permiten una comunicación fluida y encriptada entre las unidades en distintos dominios, garantizando que los comandantes tengan acceso a información en tiempo real y puedan coordinar operaciones conjuntas de manera eficiente. En el contexto de la guerra mosaico, los sistemas de mando y control deben ser altamente flexibles y capaces de integrar diversas plataformas y unidades modulares.

En la capa Conjurar, los sistemas de mando y control avanzados facilitan la coordinación de las unidades de vigilancia y defensa en múltiples frentes. Estos sistemas permiten que las unidades de reconocimiento aéreo, terrestre y cibernético compartan datos y operen de manera integrada, optimizando la capacidad de respuesta ante cualquier amenaza potencial. De acuerdo con Grayson y Lilliu (2021), la integración de estos sistemas asegura una comunicación continua y segura entre las unidades, lo cual es fundamental para mantener la disuasión y prevenir incursiones en el territorio.

En la capa Repeler, los sistemas de mando y control avanzados permiten una coordinación precisa en la ejecución de contraataques. Estos sistemas brindan a los comandantes la capacidad de dirigir ataques de precisión en múltiples frentes, utilizando datos de sensores y sistemas de vigilancia para seleccionar objetivos y optimizar el despliegue de las fuerzas. La capacidad de realizar ajustes tácticos en tiempo real garantiza que las fuerzas argentinas puedan mantener una postura ofensiva eficaz y responder de manera inmediata a los cambios en el campo de batalla (Pulido, 2021).

### **2.5.4. *Desafíos y Consideraciones en la Integración de Tecnología y Sistemas Autónomos***

Aunque la tecnología avanzada y los sistemas autónomos ofrecen ventajas significativas, su integración también presenta desafíos. Entre estos, la necesidad de una infraestructura robusta y segura para la comunicación, así como la capacitación del personal en el uso y mantenimiento de estas tecnologías. Además, la dependencia de la IA y los sistemas autónomos plantea riesgos en términos de ciberseguridad, especialmente en un entorno de guerra multidominio donde los ataques cibernéticos pueden comprometer la efectividad de las operaciones.

La ciberseguridad es esencial para proteger los sistemas de mando y control avanzados y los datos recopilados por los sistemas autónomos. En el contexto de las operaciones multidominio, es fundamental que las redes de comunicación y los sistemas de mando estén

protegidos contra posibles ataques de interferencia y ciberataques. Según el Fuerza 35 del Ejército de Tierra de España (2019), la ciberseguridad es una prioridad para mantener la integridad de los datos y asegurar que las fuerzas puedan operar sin interrupciones en un entorno de alta amenaza.

## **2.6. Impacto Estratégico: Disuasión y Equilibrio Regional**

### ***2.6.1. Disuasión y Preparación para Conflictos de Alta Intensidad***

Las fuerzas multidominio fortalecen la postura defensiva nacional al proporcionar una capacidad de respuesta integrada en múltiples dominios. Esta integración disuade a potenciales agresores, al aumentar la incertidumbre sobre la capacidad de respuesta propia y dificultar la planificación de un ataque. En el contexto regional, esto posiciona a Argentina como un actor con una estrategia defensiva moderna y adaptable, alineada con las doctrinas más avanzadas de defensa global.

### ***2.6.2. Equilibrio de Poder Regional***

La implementación de fuerzas multidominio también contribuye a equilibrar las asimetrías militares en la región. Países del marco regional con mayores recursos, han avanzado en la modernización de sus capacidades militares, lo que podría generar una brecha estratégica. Al adoptar un enfoque multidominio, la defensa nacional no solo moderniza sus fuerzas, sino que también aumenta su capacidad de actuar como un actor estabilizador en la región.

## **2.7. Desafíos Logísticos en Fuerzas Multidominio**

### ***2.7.1. Costos de Implementación y Mantenimiento***

La modularidad, la interoperabilidad y escalabilidad de las fuerzas multidominio requieren una inversión inicial significativa en tecnología avanzada, como SANT, sistemas autónomos e infraestructura de comunicación segura. A largo plazo, estos costos pueden optimizarse mediante una reducción en la dependencia de plataformas monolíticas y de alto costo.

### ***2.7.2. Infraestructura y Logística Descentralizada***

Las fuerzas multidominio necesitan una red de infraestructura descentralizada que permita el despliegue rápido de unidades en diferentes dominios. Esto incluye bases logísticas avanzadas, lugares de mantenimiento en zonas estratégicas y sistemas de transporte ágil.

### ***2.7.3. Desafíos en el Contexto Nacional***

La extensión territorial de Argentina presenta dificultades logísticas, como la necesidad de mantener una red operativa en regiones remotas o de difícil acceso, como la Patagonia. Esto resalta la importancia de una planificación logística adaptativa y un enfoque modular para garantizar la autosuficiencia táctica.

#### **2.7.4. Ventajas Logísticas de las Fuerzas Multidominio**

A pesar de los desafíos, las fuerzas multidominio ofrecen ciertas ventajas logísticas que optimizan el uso de recursos y aumentan la eficiencia operativa.

**Reducción de la Dependencia en Grandes Infraestructuras.** Al emplear módulos autónomos y escalables, las fuerzas multidominio minimizan la necesidad de grandes bases y sistemas centralizados. Esto permite una mayor flexibilidad y capacidad de adaptación en entornos operativos volátiles.

**Eficiencia en el Uso de Recursos.** La modularidad permite ajustar la magnitud y el alcance de las fuerzas desplegadas según la intensidad del conflicto. Esto reduce el desgaste de recursos y evita el despliegue innecesario de unidades.

**Resiliencia Logística.** Las fuerzas modulares y descentralizadas son más resilientes frente a interrupciones logísticas. Si una parte de la red es neutralizada, el resto puede continuar operando sin afectar significativamente la misión global (Fuerza 35, Ejército de Tierra, 2023).

#### **2.8. Propuesta para la Implementación de Fuerzas Multidominio**

Para garantizar la implementación exitosa de fuerzas multidominio, es fundamental desarrollar una doctrina adaptable que permite que las Fuerzas Armadas se ajusten rápidamente a cambios en el entorno operacional, lo que permitirá operar en contextos de alta incertidumbre, como ciberataques o conflictos híbridos.

Incorporar la modularidad como base de la doctrina asegura que las unidades puedan reorganizarse rápidamente según las necesidades del conflicto. Esto también facilita la interoperabilidad entre las diferentes Fuerzas Armadas.

##### **2.8.1. Programas de Capacitación para Operaciones Multidominio**

La capacitación es fundamental para garantizar que el personal militar esté preparado para manejar tecnologías avanzadas y coordinar operaciones en múltiples dominios. Esto incluye no solo el uso de herramientas como los SANT, la inteligencia artificial y otros sistemas avanzados, sino también su mantenimiento y optimización.

Además, el personal debe ser entrenado en la coordinación efectiva de operaciones multidominio, lo que implica la capacidad de comunicarse en tiempo real con otras unidades y agencias, asegurando una respuesta integrada y eficiente. La capacitación técnica debe complementarse con ejercicios prácticos que simulen escenarios reales, permitiendo al personal adaptarse a condiciones dinámicas y desafiantes.

##### **2.8.2. Ejercicios de Simulación y Pruebas Operativas**

Los ejercicios de simulación son herramientas esenciales para probar y perfeccionar los conceptos y principios de las operaciones multidominio, especialmente en contextos de alta

incertidumbre y complejidad. Realizar simulaciones en tiempo real permite evaluar la capacidad de las fuerzas multidominio para responder de manera efectiva a ataques combinados, como ciberataques y operaciones terrestres simultáneas.

Las simulaciones deben incluir variables inesperadas, como cambios abruptos en las condiciones del campo de batalla o fallas tecnológicas, con el objetivo de identificar y corregir debilidades en la estructura de las fuerzas y los procedimientos operativos.

En este contexto, resulta prioritario crear centros de simulación y capacitación dedicados exclusivamente a las operaciones multidominio. Estos centros deberían estar equipados con tecnología avanzada, como simuladores de realidad virtual e inteligencia artificial, para replicar escenarios complejos de manera realista y efectiva.

Asimismo, la participación en ejercicios multinacionales con países que ya aplican operaciones multidominio resulta vital para aprender de sus experiencias y mejorar la interoperabilidad entre fuerzas. Finalmente, establecer un sistema de monitoreo permitirá evaluar el desempeño de las fuerzas en simulaciones y operaciones reales, ajustando la doctrina y los programas de capacitación según los resultados obtenidos.

## **2.9. Evaluación de Riesgos y Limitaciones**

La ejecución de operaciones multidominio presenta riesgos y limitaciones relacionados con la dependencia tecnológica, vulnerabilidades en la interoperabilidad y amenazas cibernéticas.

La dependencia de sistemas avanzados, como SANT, inteligencia artificial y redes de comunicación, introduce vulnerabilidades si estas tecnologías fallan o son neutralizadas. En conflictos en desarrollo, como en Ucrania, los SANT han sido vulnerables a interferencias electrónicas y ciberataques que limitan su efectividad operativa (Pifer, 2022).

- El ritmo acelerado del desarrollo tecnológico puede hacer que ciertos sistemas se vuelvan obsoletos rápidamente, lo que genera costos adicionales en mantenimiento y actualización.
- La interoperabilidad limitada entre las Fuerzas Armadas puede dificultar la coordinación en operaciones multidominio. Esto es especialmente crítico cuando se emplean plataformas tecnológicas que no comparten estándares comunes.
- La complejidad de coordinar operaciones en múltiples dominios aumenta el riesgo de errores operativos o falta de cohesión entre unidades.
- Las redes de comunicación y mando, fundamentales para las operaciones multidominio, son objetivos prioritarios para adversarios que emplean tácticas de guerra cibernética.

- La centralización excesiva de las operaciones en redes digitales aumenta el riesgo de colapsos operativos si estas redes son comprometidas.
- La descentralización en la toma de decisiones, aunque beneficiosa en escenarios dinámicos, puede generar problemas de coordinación si no se implementan protocolos claros.
- La implementación de fuerzas multidominio depende del entrenamiento adecuado del personal, que debe estar capacitado para manejar tecnologías avanzadas y coordinarse en múltiples dominios.

## **2.10. Coordinación con Agencias No Militares**

La naturaleza multidimensional de las amenazas actuales requiere una respuesta integrada que trascienda los límites de las Fuerzas Armadas. La coordinación con agencias no militares, como Fuerzas de Seguridad, organismos gubernamentales, entidades civiles y el sector privado, es crucial para abordar crisis complejas de manera efectiva. Este enfoque permite aprovechar recursos y capacidades adicionales para fortalecer la respuesta nacional ante desafíos de seguridad multidominio.

Las agencias no militares desempeñan un papel clave en la protección de infraestructuras críticas, la gestión de emergencias y la provisión de apoyo logístico. Al integrar sus capacidades en las operaciones multidominio permite una respuesta más completa y eficiente.

### ***2.10.1. Estrategias para Fomentar la Cooperación***

**Desarrollo de Protocolos de Interoperabilidad.** La creación de protocolos claros que definan roles, responsabilidades y procesos entre las Fuerzas Armadas y las agencias civiles es esencial para garantizar una coordinación efectiva. La realización de ejercicios conjuntos en escenarios multidominio permite identificar áreas de mejora en la coordinación y fortalecer la capacidad de respuesta integrada.

**Establecimiento de Redes de Cooperación Permanente.** La creación de redes y foros permanentes de cooperación facilita el intercambio de información y recursos entre sectores. Estas redes también fomentan la confianza mutua y la preparación conjunta.

### ***2.10.2. Beneficios de la Coordinación con Agencias No Militares***

**Eficiencia Operativa.** Aprovechar los recursos y capacidades de las agencias no militares mejora la eficiencia de las operaciones multidominio, optimizando el uso de los recursos disponibles.

**Mayor Capacidad de Respuesta.** La integración de actores civiles y privados amplía la capacidad de respuesta ante amenazas, garantizando una cobertura más amplia y efectiva.

**Fortalecimiento de la Seguridad Nacional.** Una respuesta integrada y coordinada refuerza la resiliencia del país frente a amenazas multidominio, mejorando la seguridad nacional en su conjunto.

## Conclusiones Finales

Esta investigación ha explorado el diseño y aplicación de fuerzas multidominio en el contexto de defensa nacional, centrándose en los parámetros y conceptos esenciales para la efectividad de las capas estratégicas Conjurar y Repeler. A través del análisis y desarrollo de los capítulos, se lograron establecer los fundamentos teóricos y prácticos que confirman la viabilidad y necesidad de estos parámetros, respondiendo favorablemente a la hipótesis planteada.

En el Capítulo 1, se introdujeron los conceptos de operaciones multidominio y guerra mosaico, analizando su evolución y aplicación en la doctrina de defensa nacional. Las operaciones multidominio permiten una integración de fuerzas en los dominios terrestre, aéreo, marítimo, espacial, cibernético y de información, ofreciendo una ventaja operacional al coordinar esfuerzos en múltiples espacios de combate de forma sinérgica. Por su parte, la guerra mosaico, al utilizar unidades modulares y autónomas, proporciona flexibilidad y resistencia ante amenazas diversificadas, permitiendo que las fuerzas se adapten rápidamente a cambios en el entorno y generen dilemas constantes para el enemigo. La combinación de ambos conceptos facilita la defensa en las capas Conjurar y Repeler, donde la modularidad, interoperabilidad y autonomía son clave para enfrentar tanto amenazas convencionales como asimétricas en el teatro de operaciones.

El Capítulo 2 profundizó en los parámetros de diseño de fuerzas multidominio, centrándose en la modularidad, interoperabilidad, escalabilidad, adaptabilidad, convergencia e integración tecnológica. Estos principios crean una fuerza adaptable y resistente, capaz de ajustar su tamaño, estructura y capacidades según el nivel de amenaza y la evolución del conflicto. La modularidad permite que las fuerzas se organicen en unidades autónomas y flexibles, la interoperabilidad asegura que las distintas fuerzas actúen de forma coordinada en los múltiples dominios, y la escalabilidad y adaptabilidad permiten una rápida reorganización en función de las exigencias operativas.

La convergencia refuerza la capacidad de las Fuerzas Armadas para integrar y sincronizar recursos en tiempo real, maximizando la eficacia operativa en escenarios complejos. Este enfoque permite la eliminación de barreras entre dominios, generando efectos combinados que potencian la adaptabilidad y flexibilidad en el campo de batalla. Su implementación proporciona una ventaja significativa frente a amenazas emergentes, al tiempo que subraya la importancia de la interoperabilidad tecnológica y la protección de redes críticas para garantizar su sostenibilidad operativa. La convergencia, por lo tanto, no solo complementa los parámetros tradicionales como la modularidad, la interoperabilidad y la escalabilidad, sino

que también posiciona a las fuerzas multidominio como un modelo avanzado y cohesionado de defensa integral.

La integración de tecnología avanzada, como IA y sistemas autónomos, fortalece la capacidad de vigilancia, análisis y toma de decisiones en tiempo real, asegurando que las fuerzas puedan operar eficazmente en condiciones de alta incertidumbre y riesgo.

Estos principios se alinean con la concepción estratégica de las capas Conjurar y Repeler, que buscan, en primer lugar, disuadir y degradar las capacidades del enemigo, y, en segundo lugar, neutralizarlo mediante una defensa de alta intensidad.

La implementación de estos parámetros permite la disposición de fuerzas con una estructura flexible, escalable y de alta interoperabilidad, lo que facilita la respuesta rápida y proporcional en el teatro de operaciones. Además, esta estructura no solo maximiza la eficiencia de los recursos, sino que también asegura que las fuerzas puedan adaptarse a los cambios en la táctica y tecnología del enemigo. La hipótesis de que el análisis de los parámetros de diseño facilita la creación de fuerzas interoperables, modulares y adaptables en conflictos multidominio se confirma positivamente, ya que estos principios permiten la conformación de una fuerza robusta, preparada para operar en ambientes complejos y para enfrentar amenazas en varios dominios simultáneamente.

La IA y los SANT están revolucionando el panorama de las operaciones multidominio al mejorar significativamente la modularidad, adaptabilidad y la capacidad de toma de decisiones en tiempo real. Estas tecnologías permiten a las Fuerzas Armadas operar con mayor precisión y rapidez, lo que refuerza su eficacia en entornos complejos y dinámicos. Sin embargo, su integración también presenta desafíos relacionados con la seguridad cibernética y consideraciones éticas y legales.

Las ventajas estratégicas de la IA y los SANT son innegables. Estas tecnologías aumentan la letalidad y precisión de las fuerzas multidominio al permitir ataques más coordinados y eficientes, reduciendo los daños colaterales y optimizando el uso de recursos. Asimismo, los SANT destacan en operaciones autónomas en áreas de alto riesgo, como entornos contaminados químicamente o bajo fuego enemigo, eliminando la exposición del personal a peligros directos.

En términos éticos y legales, el uso de tecnologías avanzadas en operaciones multidominio plantea importantes cuestiones que deben ser abordadas. Los sistemas autónomos tienen la capacidad de tomar decisiones sin intervención humana, lo que genera preocupaciones sobre su habilidad para distinguir entre combatientes y civiles. Para garantizar el cumplimiento del Derecho Internacional Humanitario (DIH), es esencial mantener la

intervención humana en decisiones críticas, especialmente aquellas que puedan resultar en la pérdida de vidas humanas. Además, se deben establecer protocolos estrictos que prioricen la protección de civiles y la infraestructura no militar.

Aunque el DIH proporciona principios fundamentales como la necesidad, la proporcionalidad y la humanidad, el ámbito cibernético presenta lagunas normativas, especialmente en lo referente al uso de ciberarmas. La ausencia de un marco regulatorio claro genera incertidumbre y subraya la necesidad de establecer estándares globales que regulen su uso en conflictos armados.

La delegación de decisiones en sistemas autónomos plantea preguntas sobre la responsabilidad en caso de errores operativos o violaciones al DIH. Es crucial definir claramente quién será responsable en estas situaciones, ya sea el operador, el desarrollador del sistema o el comandante militar. Esto garantizará que las decisiones autónomas se alineen con los principios éticos y legales, consolidando un uso responsable y legítimo de estas tecnologías en el ámbito de la defensa.

Este trabajo proporciona una base sólida para el diseño de fuerzas multidominio, estableciendo los parámetros esenciales para enfrentar los desafíos de defensa en un escenario global marcado por la volatilidad, incertidumbre y rápida evolución tecnológica. Este diseño de fuerzas permite no solo una defensa adaptativa y eficiente, sino que también potencia la capacidad de disuasión y respuesta frente a agresores externos, garantizando una defensa soberana y moderna alineada con las exigencias de la guerra contemporánea.

## Anexo 1

La Escuela de Guerra del Ejército de Tierra, teniendo en cuenta nuevo enfoque de mando descentralizado, elaboró un modelo que, mediante la analogía de ascensión al monte K2, explica cómo llegar a la excelencia en el liderazgo en el sentido que ambas actividades se realizan en ambientes volátiles, inciertos, complejos y ambiguos.

### Modelo de Liderazgo K2

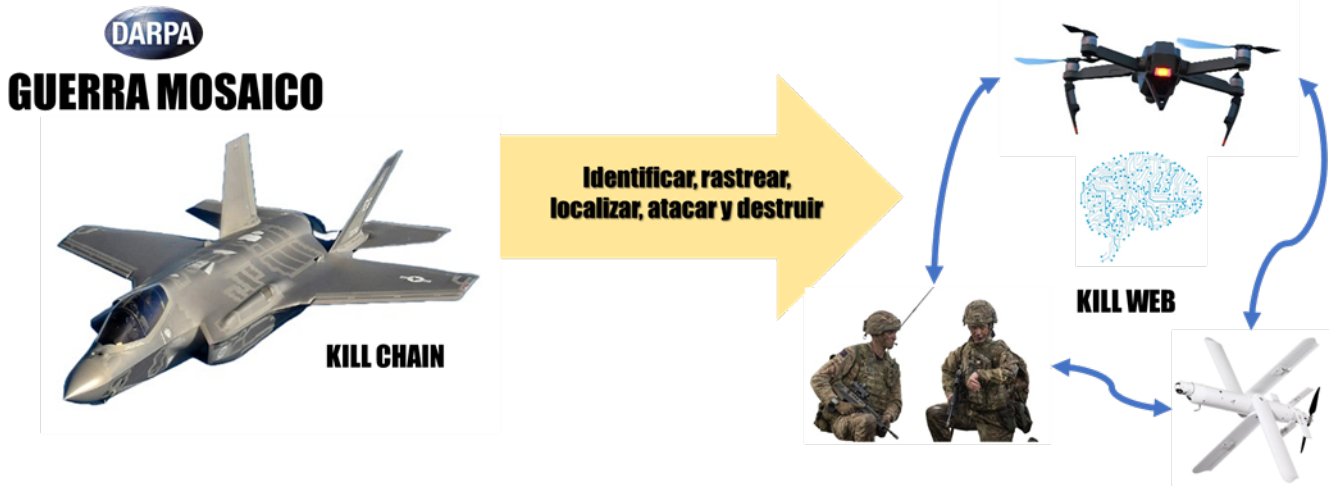


*Nota.* Adaptado de “Horizonte 2035 Hacia el Ejército que España necesita”.

## Anexo 2

### Concepto de la Guerra Mosaico

En la guerra mosaico, la fuerza mosaico está formada esencialmente por decisores, sensores y tiradores reemplazando plataformas monolíticas por plataformas desagregadas.



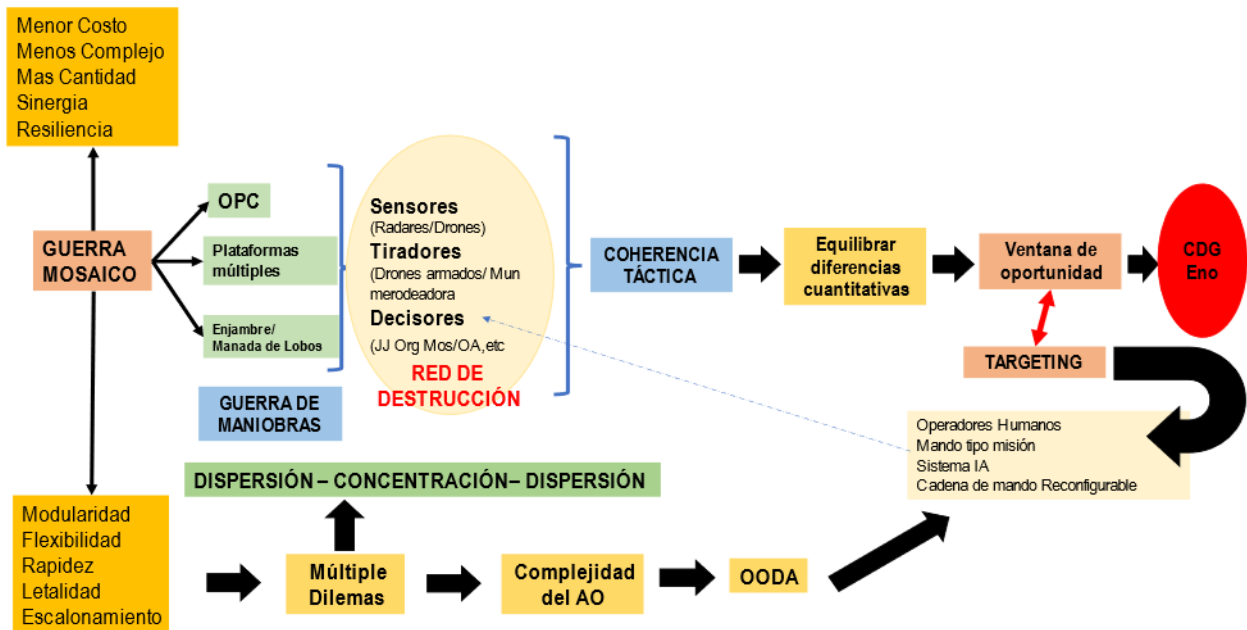
Plataforma monolítica con KILL CHAIN (red integrada en la que la misma plataforma identifica, rastrea, localiza, ataca y destruye)

Plataforma mosaico con KILL WEB (red integrada en la que diferentes plataformas identifican, rastrean, localizan, atacan y destruyen. Normalmente conformada por decisores, sensores y tiradores.)

### Anexo 3

#### El Mosaico de Combate

En el contexto de las operaciones multidominio, los conductores tácticos deberán ser capaces de tomar decisiones rápidas y precisas en un entorno complejo y cambiante. Para hacerlo, requerirán una habilidad mental avanzada y un entrenamiento riguroso preparándolos para actuar con eficacia. Con estas organizaciones lo que se busca es lograr la dispersión – concentración – dispersión, buscando que la concentración sea a través de conformación de enjambres, procedentes de diversas direcciones creando al enemigo la mayor cantidad de dilemas posibles buscando condicionar su ritmo de avance. Esta forma de accionar de las organizaciones tipo mosaico caracterizadas por la resiliencia, deberán buscar su supervivencia en el permanente movimiento llevando el concepto de guerra de maniobras a su máxima expresión con una gran dependencia de la autosuficiencia táctica. (EMCO, 2023).



## Bibliografía

- Arquilla, J. & Ronfeldt D. (2000). *Swarming and the Future of Conflict*, National Defense Research Institute. [https://www.rand.org/content/dam/rand/pubs/documentedbriefings/2005/RAND\\_DB311.pdf](https://www.rand.org/content/dam/rand/pubs/documentedbriefings/2005/RAND_DB311.pdf)
- Clark, B. & Patt, D. & Schramm, H. (2020). *Mosaic Warfare. Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations*, Center for Strategic and Budgetary Assessment. <https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations>
- Clark, B. & Patt, D. & Walton, T. (2021). *Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage*, Hudson Institute, Center for Defense Concepts and Technology. <https://www.hudson.org/policycenters/center-defense-concepts-technology>.
- Department of Defense (2022). *Joint All-Domain Command & Control*.
- DARPA (2017, Abril 8). Strategic Technology Office Outlines Vision for “Mosaic Warfare”. <https://www.darpa.mil/news-events/2017-08-04#>
- Donnelly, William (2007). *Transforming an Army at War*. Center of Military History United States Army. CMH Pub 70–108–1
- ESFAS. (2022). *Libro A13 Planeamiento de Operaciones y Ejercicios Conjuntos*. Escuela Superior de las Fuerzas Armadas.
- Ejército Argentino (2015). *Conducción para las Fuerzas Terrestres*, Ejército Argentino
- Ejército de Tierra. (2023). *Fuerza 35: Una visión para el futuro*. Ministerio de Defensa.
- Ejército de Tierra. (2023). *Hacia el Ejército que España Necesita: Horizonte 2035*. Edición Especial, Ejército 35.
- Estado Mayor Conjunto de las Fuerzas Armadas (2023a, Mayo 8). Conceptos generales sobre la concepción estratégica de capas, restricción de áreas y de operaciones multidominio. *Boletín Informativo Conjunto – EMCO*, pp. 1-44.
- Estado Mayor Conjunto de las Fuerzas Armadas (2023b). *Glosario de términos de empleo militar para la acción militar conjunta*, Estado Mayor Conjunto de las Fuerzas Armadas.
- Fojón, E. (2020). *La era digital y la evolución del carácter de la guerra en Occidente*. Documento de Opinión IEEE.
- García, A. J. (2021, Marzo 12). *¿Una tercera estrategia de compensación? Mejor una gran estrategia*. [https://www.ieee.es/Galerias/fichero/docs\\_opinion/2021/DIEEEO32\\_2021](https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO32_2021)

- Grana, J., Lamb, J., & O'Donoghue, N. A. (2021). *Findings on Mosaic Warfare from a Colonel Blotto Game*. RAND Corporation.
- Grayson, T. P., & Lilliu, S. (2021). *Mosaic Warfare and Human–Machine Symbiosis*. Strategic Technology Office, DARPA.
- Lind, W. (1999). *Manual de la Guerra de Maniobras*, Circulo Militar.
- López Díaz, J. Á. (2021). Guerra Mosaico vs Confrontación de Sistemas. *Revista de Defensa Nacional*.
- Mercado, D. S. (2024). *Combate antitanque a través de la conformación de Organizaciones Mosaico con capacidades modulares*. Escuela Superior de Guerra.
- Milley, M. A. (2028). *El Ejército de los Estados Unidos en Operaciones de Múltiples Dominios*. TRADOC Pamphlet 525-3-1.
- Monge Gaitan, E. (2020). Las Operaciones Multidominio: El nuevo reto. *Revista del Ejército de Tierra Español No 947*
- Perkins, David. (2017). Multi-Domain Battle the Advent of Twenty-First Century War. [armyupress.army.mil/Portals/7/military-review/Archives/English/Multi-Domain-Battle-The-Advent-of-Twenty-First-Century-War.pdf?ver=2017-10-26-160929-763](http://armyupress.army.mil/Portals/7/military-review/Archives/English/Multi-Domain-Battle-The-Advent-of-Twenty-First-Century-War.pdf?ver=2017-10-26-160929-763)
- Pulido, G. (2021). Guerra multidominio y mosaico. El nuevo pensamiento militar estadounidense, Editorial Catarata.
- Reino de España (2020). Nota conceptual Operaciones Multidominio. *Estado Mayor de la Defensa*.
- República Argentina (2021). *Directiva Política de la Defensa Nacional*, <http://servicios.infoleg.gob.ar/infolegInternet/anexos/350000-354999/352107/dec457.pdf>
- Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company.