ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TITULO: Las Fuerzas Armadas y la ejecución de las operaciones multidominio.

AUTOR: MY (EA) Facundo Martín GÓMEZ

TUTOR: MY (EA) Sebastián Andrés José NOTARO

AÑO: 2024

RESUMEN

Las operaciones multidominio constituyen el nuevo paradigma estratégico-operacional de las fuerzas armadas en respuesta a las amenazas emergentes en el escenario geopolítico actual. Su esencia radica en la capacidad de influir de manera sinérgica y sincronizada en todas las dimensiones del campo de batalla, con el propósito de imponer múltiples dilemas al adversario mediante acciones cinéticas y no cinéticas, incluso por debajo del umbral del conflicto.

En este contexto, las fuerzas armadas a nivel global han desarrollado operaciones multidominio para adaptarse a escenarios y contextos caracterizados por su dinamismo y variabilidad. Estos entornos operacionales complejos demandan respuestas rápidas para facilitar la toma de decisiones, dado que, en un teatro de operaciones, no siempre existen límites tangibles.

Este tipo de operaciones requiere la coordinación de acciones entre diferentes componentes del Estado, incluyendo fuerzas de seguridad, fuerzas armadas, así como organizaciones privadas, gubernamentales y no gubernamentales. Para ello, es fundamental contar con una estructura organizativa que permita planificar y conducir operaciones multidominio, proporcionando asistencia y asesoramiento en el proceso de toma de decisiones.

En este tipo de operaciones, es fundamental que los distintos actores comprendan las acciones que deben ejecutar, así como quién asume el esfuerzo principal y la conducción de las mismas. Cada actor debe entender, coordinar, asesorar y asistir al órgano encargado de dirigir la operación, garantizando que esta se desarrolle de manera rápida y eficaz.

Asimismo, es esencial que cada participante trabaje de forma independiente y con libertad de acción, lo que facilita la toma de decisiones alineadas con la intención del comandante o con la misión del órgano decisor.

PALABRAS CLAVES.

Operaciones multidominio – Operaciones interagenciales – Ambiente operacional – Conflictos híbridos – Teatro de operaciones complejo

INDICE

INTRODUCCIÓN

Las operaciones multidominio representan una evolución estratégica en el ámbito militar, diseñadas para enfrentar las crecientes complejidades de los conflictos modernos. Este concepto integra las capacidades en tierra, mar, aire, ciberespacio y espacio ultraterrestre, permitiendo una sinergia operativa que supera las limitaciones de las estrategias tradicionales. Su origen se encuentra en la necesidad de adaptarse a amenazas que trascienden los enfrentamientos físicos y abarcan dimensiones como la desinformación, la guerra cibernética y la guerra híbrida.

Formalizado por las fuerzas armadas de Estados Unidos a través de la doctrina Multidomain Operations (MDO), este enfoque busca coordinar acciones en todos los dominios para imponer múltiples dilemas al adversario, reduciendo su capacidad de respuesta (U.S. Army Training and Doctrine Command, 2018). Ejercicios como "Project Convergence" y conflictos como la guerra en Ucrania han demostrado la efectividad de las operaciones multidominio al integrar tecnologías avanzadas, inteligencia artificial y drones autónomos en un marco operativo conjunto.

En Argentina, las operaciones multidominio constituyen una oportunidad para potenciar capacidades en áreas estratégicas, como la ciberdefensa y el desarrollo espacial. Iniciativas como el programa SAOCOM han permitido avances significativos en el monitoreo y la observación estratégica, consolidando al país como un referente regional en tecnología satelital. No obstante, la implementación efectiva de estas operaciones requiere superar desafíos como la falta de interoperabilidad entre dominios y la modernización de sistemas de comando y control.

Estos esfuerzos buscan posicionar a las fuerzas armadas en un entorno cada vez más dinámico, donde los conflictos trascienden las fronteras físicas para involucrar a actores estatales y no estatales. Para ello, es esencial desarrollar un sistema de comando eficiente, procesos de toma de decisiones ágiles y una integración efectiva entre los niveles estratégico, operacional y táctico.

Las operaciones multidominio no solo redefinen las tácticas militares, sino que también requieren un cambio en la mentalidad estratégica. En este contexto, Argentina debe continuar fortaleciendo sus capacidades a través de

la cooperación internacional y la inversión en tecnologías disruptivas, como la inteligencia artificial y las comunicaciones seguras.

CONTEXTO HISTÓRICO

El concepto de operaciones multidominio tiene raíces históricas profundas, derivadas de la necesidad de coordinar fuerzas terrestres y marítimas desde el siglo XVIII. Durante la Primera y Segunda Guerra Mundial, la aparición del dominio aéreo revolucionó la estrategia militar, incorporando nuevas dimensiones al campo de batalla. Posteriormente, la Guerra Fría consolidó el ciberespacio y el espectro electromagnético como dominios clave, marcando el inicio de una transformación en los enfoques operacionales.

En las últimas décadas, potencias como Estados Unidos, Rusia y China han liderado el desarrollo de capacidades multidominio, integrando tecnología avanzada y estrategias híbridas. Estados Unidos, por ejemplo, formalizó su doctrina de operaciones multidominio en 2017 a través del Army Training and Doctrine Command (TRADOC) (U.S. Army Training and Doctrine Command, 2018), con un enfoque en la integración de los cinco dominios principales: tierra, mar, aire, ciberespacio y espacio. Este modelo ha sido probado en ejercicios como "Cyber Blitz" y "Project Convergence", demostrando la importancia de la interoperabilidad y la coordinación interagencial.

Por su parte, Rusia ha adoptado un enfoque híbrido, combinando ataques cibernéticos, campañas de desinformación y maniobras militares convencionales. Ejemplo de ello es su actuación en el conflicto en Ucrania, donde tácticas como el ciberespionaje y el uso de drones han sido fundamentales para desestabilizar a su adversario. China, en cambio, ha centrado sus esfuerzos en la militarización del espacio y el desarrollo de capacidades cibernéticas, utilizando su Fuerza de Apoyo Estratégico para garantizar la superioridad tecnológica en estos dominios (Martínez-Valera, 2022).

En América Latina, el desarrollo de operaciones multidominio es más limitado (Angulo Molina, 2019), pero países como Argentina han comenzado a explorar este enfoque. Históricamente, las fuerzas armadas argentinas han enfrentado desafíos relacionados con la modernización de sus estructuras de

comando y control. Sin embargo, iniciativas recientes, como el desarrollo de satélites SAOCOM y la creación del Comando Conjunto de Ciberdefensa, representan pasos significativos hacia la integración de dominios no físicos en sus operaciones.

Estudios realizados por oficiales argentinos destacan la necesidad de adaptar las estructuras de comando para coordinar eficazmente los dominios terrestre, marítimo, aéreo, espacial y cibernético. Además, subrayan la importancia de la colaboración internacional y la incorporación de tecnologías avanzadas para enfrentar las amenazas emergentes. En este sentido, las operaciones multidominio no solo representan un cambio en la forma de conducir la guerra, sino también una oportunidad para fortalecer la soberanía nacional y la defensa regional.

ESTADO SITUACIONAL

El entorno operacional actual está definido por la competencia entre grandes potencias y el auge de amenazas híbridas que combinan ciberespionaje, desinformación y operaciones militares tradicionales. En este contexto, las operaciones multidominio se han convertido en una estrategia central para garantizar la superioridad en conflictos complejos y dinámicos.

Estados Unidos lidera el desarrollo de estas operaciones, especialmente en la región del Indo-Pacífico, donde enfrenta la creciente influencia de China. A través de la Iniciativa de Defensa del Pacífico, ha implementado una disuasión integrada que combina capacidades en tierra, mar, aire, ciberespacio y espacio. Ejercicios como "Project Convergence" han demostrado la eficacia de tecnologías avanzadas, como inteligencia artificial y drones autónomos, en la sincronización de operaciones multidominio (Royal United Services Institute, 2022; Clúster de la Industria de Defensa, 2022).

China, por su parte, ha fortalecido su capacidad militar mediante la Fuerza de Apoyo Estratégico, que integra capacidades cibernéticas, espaciales y de guerra electrónica. Este enfoque le permite competir tanto a nivel regional como global, priorizando la vigilancia espacial y la seguridad cibernética. Mientras tanto, Rusia ha adoptado una estrategia de guerra híbrida, combinando ataques cibernéticos y campañas de desinformación con

maniobras militares convencionales, como se ha observado en el conflicto en Ucrania (Clúster de la Industria de Defensa, 2022).

En América Latina, las capacidades para desarrollar operaciones multidominio son limitadas, pero algunos países, como Argentina, han comenzado a construir capacidades específicas. El programa satelital SAOCOM destaca como un ejemplo de cómo la tecnología espacial puede contribuir al monitoreo estratégico y la vigilancia regional. Además, la creación del Comando Conjunto de Ciberdefensa refleja un esfuerzo por abordar las crecientes amenazas en el ciberespacio.

A nivel internacional, las alianzas desempeñan un papel crucial en el fortalecimiento de las operaciones multidominio (Iturriaga Delgado, 2021). Organismos como la (Organización del Atlantico Norte) OTAN y acuerdos regionales en ciberseguridad facilitan la cooperación en defensa, inteligencia y tecnología. En América Latina, aunque no existe un organismo similar a la OTAN, la colaboración entre países se da a través de iniciativas como la Junta Interamericana de Defensa.

Las tecnologías emergentes, como la inteligencia artificial, los drones autónomos y los sistemas de vigilancia avanzada, están redefiniendo el panorama operacional. Estas herramientas permiten una toma de decisiones más rápida y efectiva, optimizando las capacidades de respuesta en múltiples dominios. Para países como Argentina, la integración de estas tecnologías, combinada con la cooperación internacional, es clave para garantizar una defensa efectiva y la protección de su soberanía en un entorno global cada vez más complejo.

ALCANCES Y LIMITACIONES

Este trabajo analiza las operaciones multidominio en el ámbito de la defensa nacional argentina, abordando los desafíos estratégicos y operativos para integrar capacidades en dominios terrestres, marítimos, aéreos, cibernéticos y espaciales. Su alcance se centra en proponer una estructura ideal para un comando conjunto que permita la dirección eficaz de estas operaciones, tanto en tiempos de paz como en situaciones de conflicto.

El estudio se limita al análisis de los dominios cibernético y espacial, priorizando la ciberdefensa y la vigilancia espacial como pilares estratégicos.

En el ámbito cibernético, se examinan aspectos como la protección de infraestructuras críticas, la recopilación de inteligencia y el manejo de amenazas en tiempo real. En el dominio espacial, el énfasis está en el uso de satélites como los SAOCOM para la observación y el apoyo a operaciones conjuntas, excluyendo aspectos técnicos más amplios de la exploración espacial.

Se tomará como referencia la experiencia de fuerzas armadas extranjeras, específicamente de Estados Unidos y España, para identificar buenas prácticas y lecciones aprendidas en ciberdefensa y operaciones espaciales. Particular atención se dará al funcionamiento de centros de comando y control multidominio, evaluando su capacidad para coordinar recursos y adaptar estrategias en entornos operativos complejos.

Otro aspecto clave es la interacción entre las fuerzas armadas y actores gubernamentales y no gubernamentales, como ministerios, agencias de inteligencia y empresas tecnológicas. Se evaluarán los mecanismos de colaboración interagencial y la participación de actores privados en la protección de infraestructuras críticas. Sin embargo, no se abordarán aspectos económicos ni comerciales relacionados con estas colaboraciones.
El enfoque general busca proporcionar un marco práctico y aplicable para el desarrollo de capacidades multidominio en Argentina, tomando en cuenta las limitaciones actuales y las oportunidades de crecimiento en el ámbito nacional e internacional.

Sin embargo, el trabajo no abordará los aspectos económicos ni comerciales de estas colaboraciones, ni las políticas de contratación vinculadas.

Finalmente, se explorará cómo la integración de los dominios no físicos (cibernético y espacial) impacta en las operaciones tradicionales de tierra, mar y aire, así como en las operaciones de información y desinformación durante situaciones de crisis.

APORTES TEÓRICOS Y/O PRÁCTICOS AL CAMPO DISCIPLINAR

Este trabajo tiene como objetivo desarrollar un modelo de diseño para la estructuración de un comando conjunto multidominio en el nivel estratégico-operacional. El modelo propuesto demostrará cómo deben articularse y

coordinarse las operaciones en los dominios terrestre, marítimo, aéreo, cibernético y espacial. Esta propuesta servirá como base para la creación de un estado mayor multidominio dentro de un comando operacional, adaptado tanto para operaciones en tiempos de paz como en situaciones de crisis y conflicto.

Las estructuras y funciones planteadas en este modelo estarán diseñadas para integrar recursos y conocimientos provenientes de diversas disciplinas, así como de actores interagenciales y no gubernamentales. Esta integración proporcionará un marco de cooperación que fortalecerá la protección de infraestructuras críticas y la defensa en el ciberespacio. Además, se busca establecer parámetros claros para la colaboración y el intercambio de información con el sector privado y agencias gubernamentales, de modo que el comandante operacional pueda tomar decisiones informadas y estratégicas ante amenazas que puedan surgir en cualquiera de los dominios.

El trabajo también contribuirá al desarrollo doctrinal de la defensa nacional, específicamente en la conformación y conducción de estados mayores a nivel estratégico-operacional. Proveerá lineamientos para la integración de los dominios no físicos de forma transversal, garantizando que las fuerzas armadas puedan mantener una capacidad de respuesta ágil y resiliente frente a las operaciones multidominio de un adversario. Este enfoque busca avanzar en la doctrina de defensa nacional, proponiendo una estructura que refleje la complejidad del entorno contemporáneo, permitiendo que el instrumento militar nacional opere de manera coordinada y efectiva en el contexto de operaciones conjuntas y multinacionales.

OBJETIVO

Desarrollar una estructura óptima de comando y control para las Fuerzas Armadas Argentinas que permita ejecutar eficientemente operaciones multidominio, garantizando la integración sinérgica de actores estatales y no estatales en un entorno operacional complejo, y fomentando una respuesta coordinada frente a amenazas emergentes.

Objetivos Partiulares

- Analizar las doctrinas y operaciones multidominio exitosas realizadas por otros países, identificando buenas prácticas y lecciones aprendidas que puedan ser aplicables al contexto argentino.
- Evaluar las herramientas tecnológicas y estructuras de comando necesarias para garantizar una comunicación eficiente y una toma de decisiones ágil en escenarios operativos multidominio.
- Proponer procedimientos y políticas específicas para la creación de órganos interagenciales permanentes, promoviendo la modernización y efectividad de las Fuerzas Armadas Argentinas frente a amenazas híbridas y emergentes.

HIPÓTESIS

Un comando conjunto multidominio organizado bajo una estructura integrada con capacidades en todos los dominios (terrestre, marítimo, aéreo, cibernético y espacial) y coordinado con actores gubernamentales y no gubernamentales, permitirá una respuesta efectiva y oportuna en la toma de decisiones estratégicas y operacionales, optimizando la defensa nacional y la protección de infraestructuras críticas frente a amenazas en entornos complejos y en constante cambio.

METODOLOGÍA DE LA INVESTIGACIÓN

La investigación se servirá del método deductivo, partiendo de conceptos generales sobre las operaciones multidominio y sus interacciones con actores gubernamentales y no gubernamentales, para luego analizar su aplicabilidad en el contexto argentino. Además, se incluirá el uso de inferencias inductivas, mediante la comparación de doctrinas y estructuras de mando multidominio de Estados Unidos y España, que servirán como referencia para proponer un modelo adaptado a las fuerzas armadas argentinas.

En primer lugar, se analizarán las bases legales y doctrinales de Argentina en el ámbito de las operaciones multidominio, para delimitar el marco normativo y doctrinario en el que operan sus fuerzas armadas. La segunda etapa consistirá en un compendio y análisis de información sobre las prácticas y estructuras de comando multidominio en Estados Unidos y

España, con énfasis en la coordinación interagencial y el rol de los actores no gubernamentales en la protección de infraestructuras críticas y la ciberdefensa.

En una tercera etapa, se relacionarán los principios y estructuras de ciberdefensa del sistema de comando estratégico operacional argentino con las prácticas observadas en las fuerzas extranjeras analizadas. A partir de esta relación, se diseñará un modelo preliminar de comando conjunto multidominio que permita la colaboración efectiva con actores externos en tiempos de paz y en situaciones de crisis.

La investigación seguirá un diseño de carácter explicativo, y se estructurará en un objetivo general y tres objetivos particulares.

Como técnica de validación, se empleará el análisis bibliográfico de fuentes académicas, doctrinarias y normativas, complementado con documentos de defensa y estudios de caso de operaciones multidominio en las fuerzas armadas de España y Estados Unidos. Esta metodología permitirá establecer una base teórica y comparativa sólida para el diseño de un comando multidominio adaptado a las necesidades y capacidades de la defensa argentina.

CAPÍTULO I

ANÁLISIS DE LAS BASES LEGALES Y DOCTRINARIAS DE ARGENTINA EN OPERACIONES MULTIDOMINIO

Este capítulo analiza el marco normativo y doctrinario que define los límites, responsabilidades y capacidades de las Fuerzas Armadas argentinas, destacando su relevancia para operaciones multidominio. La integración de leyes, directivas y doctrinas permite a las fuerzas operar de manera coordinada en contextos de alta complejidad.

1.1 Marco Normativo de las Fuerzas Armadas Argentinas

El marco normativo establece las bases legales para la actuación de las Fuerzas Armadas en operaciones multidominio, definiendo su rol en la defensa nacional y en la protección de infraestructuras críticas.

1.1.1 Ley de Defensa Nacional N.º 23.554

Esta ley define las funciones esenciales de las Fuerzas Armadas, centradas en la protección de la soberanía y la integridad territorial.

En el contexto multidominio, delimita la acción de las fuerzas en dominios emergentes, como el ciberespacio y el espacio ultraterrestre.

Durante ejercicios conjuntos nacionales, la Ley 23.554 ha sido la base para garantizar que las operaciones respeten los principios de subordinación al poder civil.

1.1.2 Decreto Reglamentario de la Ley de Defensa Nacional (Decreto N.º 727/2006)

Establece las condiciones específicas para el uso de las Fuerzas Armadas, enfocándose en la planificación conjunta.

Muestra la subordinación de acciones militares a las directivas del poder político y el enfoque en la integración de tecnologías avanzadas para operaciones coordinadas.

La colaboración con el Ministerio de Ciencia y Tecnología en proyectos como SAOCOM muestra la aplicación de este decreto.

1.1.3 Decreto de Creación del Comando Conjunto de Ciberdefensa (Decreto N.º 641/2019)

Este decreto establece al Comando Conjunto de Ciberdefensa como una herramienta estratégica en la defensa nacional.

Tiene como funciones la protección de infraestructuras críticas nacionales y la coordinación con actores civiles y privados en el ámbito de la ciberseguridad.

La participación del Comando en simulacros de ciberdefensa refleja su importancia en el ámbito multidominio.

1.1.4 Directiva de Planeamiento de Defensa N.º 1/2021

Define las prioridades estratégicas de las Fuerzas Armadas, destacando la modernización de capacidades en ciberdefensa y operaciones espaciales.

La inclusión del espacio y el ciberespacio en ejercicios conjuntos muestra la implementación práctica de esta directiva (Ministerio de Defensa de España, 2018).

1.1.5 Ley de Inteligencia Nacional N.º 25.520

Habilita la cooperación entre fuerzas armadas y agencias de inteligencia civiles para operaciones conjuntas.

Durante situaciones de emergencia, esta ley permite un flujo rápido de información entre actores estatales.

1.2 Marco Doctrinario de las Fuerzas Armadas Argentinas

El marco doctrinario establece los lineamientos para la integración de los dominios tradicionales y emergentes, garantizando la interoperabilidad y la capacidad de respuesta frente a amenazas complejas.

1.2.1 Doctrina de Operaciones Conjuntas (DPCO)

La DPCO establece la necesidad de coordinación entre las distintas ramas de las Fuerzas Armadas para maximizar las capacidades en operaciones conjuntas.

La interoperabilidad entre la Fuerza Aérea y la Armada durante ejercicios navales demuestra la aplicación de estos principios.

1.2.2 Doctrina de Ciberdefensa y Ciberseguridad

Reconoce al ciberespacio como un dominio crítico para la defensa nacional.

La colaboración con universidades nacionales para el desarrollo de herramientas de ciberseguridad es un reflejo del enfoque doctrinario.

1.2.3 Doctrina Aérea y Espacial

La Fuerza Aérea ha comenzado a incorporar elementos espaciales en su doctrina, como el uso de satélites para vigilancia y comunicaciones.

Los proyectos satelitales SAOCOM y ARSAT son ejemplos de la implementación práctica de esta doctrina.

1.2.4 Doctrina de Guerra Asimétrica y Híbrida

Responde a amenazas modernas combinando medios convencionales y no convencionales.

La integración de operaciones psicológicas y ciberdefensa en ejercicios nacionales.

1.2.5 Doctrina de Inteligencia Estratégica y Operacional

Garantiza que la inteligencia abarque todos los dominios, incluyendo el cibernético y el espacial.

El uso de sistemas ISR (Inteligencia, Vigilancia y Reconocimiento) para recopilar información en tiempo real.

1.3 Relevancia de las Normas y Doctrinas para el Multidominio

El marco normativo y doctrinario argentino proporciona una base sólida para el desarrollo de operaciones multidominio (Ley de Defensa Nacional N.º 23.554, 1988).

1.4 CONCLUSIÓN PARCIAL

El análisis del marco normativo y doctrinario de Argentina evidencia que las Fuerzas Armadas cuentan con una base jurídica y operativa para implementar operaciones multidominio. No obstante, es esencial seguir adaptando estas normativas y doctrinas a los desafíos emergentes, promoviendo la integración de dominios y la colaboración con actores estatales y no estatales.

Este trabajo comienza explorando el marco normativo y doctrinario que define los principios y las limitaciones legales de las operaciones multidominio, sentando así las bases para el análisis de las capacidades tecnológicas y estructurales necesarias.

CAPÍTULO II

CAPACIDADES TECNOLÓGICAS Y OPERACIONALES PARA EL MULTIDOMINIO

Las operaciones multidominio representan un desafío estratégico-operacional que exige la integración de capacidades tecnológicas avanzadas y estructuras organizativas flexibles. Este capítulo analiza cómo estas capacidades se han desarrollado e implementado en el ámbito internacional, y qué lecciones pueden extraerse para su aplicabilidad en Argentina.

2.1 Doctrina sobre Multidominio de España

España, como miembro de la OTAN, ha adaptado su doctrina militar para incluir los dominios cibernético y cognitivo como componentes esenciales en sus operaciones. Esto ha permitido enfrentar amenazas modernas de manera más integral.

2.1.1 Dominio Cognitivo

La gestión de información es clave para influir en percepciones públicas y decisiones políticas. España ha desarrollado estrategias para contrarrestar campañas de desinformación, basándose en experiencias como las campañas de propaganda durante conflictos en Europa del Este.

Tras los ataques de Estonia en 2007, España integró capacidades cognitivas en sus operaciones conjuntas, alineándose con estándares de la OTAN.

La batalla narrativa y las operaciones de influencia psicológica, combinadas con el uso de tecnologías de análisis de datos, han fortalecido su capacidad para actuar en este dominio.

2.1.2 Dominio Ciberespacial

España ha desarrollado una infraestructura cibernética que incluye el Centro Criptológico Nacional (CCN) (Ministerio de Defensa de España, 2018) y una estrecha colaboración con la OTAN para

fortalecer la ciberdefensa. Estas medidas han permitido una rápida adaptación a las amenazas emergentes.

En ejercicios como "Cyber Coalition", las fuerzas españolas han demostrado su capacidad para proteger infraestructuras críticas y coordinar ciberdefensa con aliados.

2.1.3 Batalla Multidominio

La doctrina española enfatiza la coordinación de dominios físicos (tierra, mar, aire) con dominios no físicos (ciberespacio, espectro electromagnético). Esta integración asegura que las fuerzas puedan operar simultáneamente en múltiples frentes.

Un desafío es lograr interoperabilidad completa entre sistemas nacionales e internacionales sigue siendo una prioridad.

2.2 Desarrollo de Operaciones Multidominio en las Fuerzas Armadas de los Estados Unidos

Estados Unidos es pionero en el desarrollo de las MDO (U.S. Army Training and Doctrine Command, 2018), diseñadas para enfrentar amenazas de grandes potencias como China y Rusia en entornos operativos complejos.

2.2.1 Integración Total de Dominios

Las MDO se basan en la sincronización de capacidades terrestres, marítimas, aéreas, espaciales y cibernéticas. Cada dominio actúa como un multiplicador de fuerza para los demás.

Durante el ejercicio "Project Convergence", EE.UU. integró sensores terrestres y espaciales con sistemas de inteligencia artificial para optimizar decisiones operativas en tiempo real (Royal United Services Institute, 2022).

2.2.2 Uso de Tecnología Avanzada

La inteligencia artificial (IA) se utiliza para analizar grandes volúmenes de datos en tiempo real, mejorando la precisión en la toma de decisiones.

Herramientas como drones autónomos y redes de comunicación satelital (por ejemplo, Starlink) han demostrado su eficacia en entornos hostiles, como en el conflicto en Ucrania.

2.2.3 Colaboración Interagencial

Las agencias civiles, como la NSA y el FBI, colaboran estrechamente con las fuerzas armadas para compartir inteligencia en tiempo real y garantizar una respuesta unificada ante amenazas emergentes.

Empresas privadas, como SpaceX y Microsoft, aportan tecnologías innovadoras que han transformado las capacidades de las fuerzas armadas.

2.2.4 Lecciones Aprendidas

Ejercicios como "Cyber Blitz" han demostrado que la interoperabilidad entre dominios es esencial para maximizar la eficacia operativa. Este enfoque obliga a los adversarios a dispersar recursos y reducir su capacidad de respuesta.

2.3 Interacción con Actores Estatales

La interacción con actores estatales es un componente crítico en las operaciones multidominio. En este contexto, varios países han establecido mecanismos formales para garantizar una coordinación efectiva:

2.3.1 Estados Unidos

El Joint All-Domain Command and Control (JADC2) integra datos de agencias civiles y militares, permitiendo decisiones tácticas y estratégicas basadas en inteligencia en tiempo real.

Durante un ataque cibernético, el JADC2 permite a los comandantes priorizar respuestas en múltiples dominios.

2.3.2 Rusia

El FSB asesora a los comandantes operacionales en materia de ciberseguridad e inteligencia. Este modelo ha sido implementado en conflictos como el de Ucrania, donde la guerra híbrida combina dominios tradicionales y cibernéticos.

2.3.4 China

La Strategic Support Force (SSF) coordina las operaciones en los dominios cibernético y espacial, trabajando con empresas estatales para garantizar una superioridad tecnológica.

2.4 Interacción con Actores No Estatales

Los actores no estatales desempeñan un rol crucial en las operaciones multidominio, ya sea como colaboradores, contratistas privados o amenazas.

2.4.1 Contratistas Privados

Proveen tecnología avanzada, como sistemas de inteligencia artificial, análisis de datos y ciberseguridad.

Ejemplo práctico: Empresas como Lockheed Martin han desarrollado herramientas cibernéticas utilizadas en ejercicios conjuntos con las fuerzas armadas.

2.4.2 ONGs y Organismos Internacionales

Colaboran en misiones humanitarias y de estabilización, asegurando que las operaciones no afecten a la población civil de manera innecesaria.

En Afganistán, las ONGs trabajaron junto con fuerzas militares para establecer corredores humanitarios.

2.4.3 Adversarios y Amenazas

Grupos como "Sandworm" han demostrado cómo los actores no estatales pueden influir en operaciones militares mediante ciberataques y campañas de desinformación.

2.5 CONCLUSIÓN PARCIAL

El análisis de capacidades tecnológicas y operacionales destaca la importancia de integrar doctrinas internacionales, tecnologías avanzadas y colaboración interagencial. Las fuerzas armadas deben adaptarse continuamente a las amenazas emergentes, maximizando la interoperabilidad entre dominios y actores. Este enfoque garantiza una preparación adecuada para operar en entornos cada vez más complejos.

Este trabajo comienza explorando el marco normativo y doctrinario que define los principios y las limitaciones legales de las operaciones multidominio, sentando así las bases para el análisis de las capacidades tecnológicas y estructurales necesarias.

CAPÍTULO III

ESTRUCTURA Y PROCEDIMIENTOS PARA LA COORDINACIÓN INTERAGENCIAL. ESQUEMA PROPUESTO PARA UN CENTRO MULTIDOMINIO Y CIBERNÉTICO

Basado en los conceptos anteriores y analizando la doctrina y leyes vigentes en el país, realizando un estudio sobre cómo podría conformar una estructura para poder llevar adelante las operaciones multidominio por parte de las Fuerzas Armadas logre desarrollar el siguiente.

3.1 ESTRUCTURA ORGANIZATIVA

3.1.1 NIVEL ESTRATÉGICO (Decisiones y Políticas)

El nivel estratégico en las operaciones militares se enfoca en la planificación y conducción general de las acciones necesarias para alcanzar los objetivos políticos y estratégicos de un país. En este nivel, se definen las políticas, estrategias y directrices que orientan el uso de los recursos militares y no militares para enfrentar las amenazas y garantizar la seguridad nacional. Además, este nivel coordina la interacción con otros actores del Estado y con aliados internacionales, asegurando que las operaciones se integren en un marco amplio de decisiones políticas y estratégicas.

En las operaciones multidominio los responsables son Ministerio de Defensa, que mantiene un enlace directo con el Ministerio de Seguridad y la Cancillería Argentina, así como al Comando Conjunto de las Fuerzas Armadas. Estas entidades tienen como funciones principales establecer los objetivos estratégicos para este tipo de operaciones, aprobar y supervisar el empleo de ciberoperaciones y otras capacidades multidominio en coherencia con las políticas nacionales, y gestionar las relaciones con diversos actores, tanto estatales como no estatales, incluyendo contratistas, organizaciones no gubernamentales y socios internacionales.

3.1.2 NIVEL OPERACIONAL (Comando y Control)

El nivel operacional en las operaciones militares actúa como un puente entre el nivel estratégico y el táctico, enfocándose en la planificación y ejecución de campañas y operaciones específicas para cumplir los objetivos estratégicos. En este nivel se desarrollan planes operativos, se asignan recursos y se sincronizan las acciones entre las distintas fuerzas y componentes, asegurando que las operaciones sean coherentes con las directrices estratégicas y se ajusten a las condiciones del entorno operacional.

En este contexto, los responsables principales son los comandantes de los teatros de operaciones y sus estados mayores (Angulo Molina, 2019), quienes tienen la función de coordinar las operaciones de las distintas fuerzas armadas y otros componentes involucrados. Esto incluye la implementación de directrices estratégicas en acciones concretas dentro de su área de responsabilidad, adaptándose a las características del entorno y asegurando la integración entre los diferentes dominios operacionales.

3.1.3 NIVEL TÁCTICO (Ejecutores)

El nivel táctico en las operaciones militares se encarga de la ejecución directa de las misiones y tareas específicas definidas por los niveles superiores, actuando en el terreno para materializar los objetivos operacionales y estratégicos. En este nivel, las unidades desplegadas, ya sean terrestres, aéreas, marítimas o cibernéticas, cumplen un rol esencial al llevar a cabo las acciones concretas necesarias para lograr los resultados planificados.

Los responsables en este nivel son las unidades tácticas desplegadas, que tienen como funciones principales implementar las directrices emitidas por el comandante operacional, contando con el soporte directo de los centros de comando. Además, estas unidades tienen la responsabilidad de proporcionar retroalimentación inmediata sobre el impacto y los resultados de las operaciones

multidominio, lo que permite realizar ajustes en tiempo real si es necesario.

3.2 FLUJOS DE INFORMACIÓN

La recolección de datos en operaciones multidominio se lleva a cabo tanto desde actores estatales como no estatales. Entre los actores estatales se incluyen agencias de inteligencia, que cumplen un rol similar a organismos internacionales, sistemas de satélites nacionales y de aliados internacionales, y datos compartidos por el Ministerio de Seguridad relacionados con ciberseguridad y análisis de amenazas. Por otro lado, los actores no estatales comprenden empresas tecnológicas contratistas, que aportan software, análisis de big data o sistemas de detección de amenazas, así como ONGs y socios internacionales involucrados en misiones humanitarias.

En cuanto al análisis y procesamiento de la información, se emplea IA para correlacionar datos provenientes de diferentes dominios, como el cibernético, terrestre, marítimo, aéreo y espacial, además de identificar patrones de amenazas. Equipos de analistas multidominio, compuestos por especialistas en cada área, consolidan la información obtenida para generar reportes claros y precisos que sirvan de base para la toma de decisiones.

Finalmente, en la toma de decisiones, el Equipo de Asesores Multidominio (EAM) presenta al comandante operacional diversas opciones estratégicas, evaluando las ventajas y desventajas de cada curso de acción e identificando el impacto potencial en cada dominio. Por ejemplo, se analiza cómo un ciberataque podría afectar la logística terrestre. Con esta información, el comandante selecciona una estrategia específica y delega su ejecución al nivel correspondiente.

3.3 INTERACCIÓN CON ACTORES EXTERNOS

Los actores estatales desempeñan un papel fundamental en las operaciones multidominio, con responsabilidades claramente definidas. El Ministerio de Defensa se encarga de establecer las reglas de enfrentamiento y coordinar acciones con otros ministerios para garantizar

una respuesta integral. Por su parte, la Cancillería Argentina asegura que las operaciones se realicen en conformidad con los tratados internacionales vigentes y gestiona las posibles implicaciones diplomáticas derivadas de estas acciones. Asimismo, el Ministerio de Seguridad contribuye protegiendo las infraestructuras críticas nacionales, fundamentales para la seguridad y el funcionamiento del país.

En cuanto a los actores no estatales, su participación también es clave. Los contratistas privados suministran herramientas avanzadas, como software de ciberseguridad, inteligencia artificial y drones, que son esenciales para llevar a cabo operaciones eficientes y tecnológicamente robustas. A su vez, las ONGs y agencias internacionales aportan datos valiosos de carácter humanitario y logístico, especialmente en contextos de misiones conjuntas o de estabilización, facilitando la coordinación y el éxito de las operaciones en entornos complejos.

3.4 COMPONENTES PRINCIPALES DEL CENTRO

La Sala de Operaciones Multidominio (SOM) constituye el núcleo central para la planificación y supervisión de las operaciones multidominio. Está equipada con una infraestructura tecnológica avanzada que incluye sistemas de visualización en tiempo real y acceso a información proveniente de todos los dominios, lo que permite un monitoreo constante de las actividades operativas.

Dentro de la SOM, la Unidad de Inteligencia Cibernética se especializa en recolectar y analizar amenazas en el ciberespacio. Además, coordina ciberoperaciones tanto ofensivas, como la neutralización de redes enemigas, como defensivas, enfocadas en proteger las redes propias frente a posibles ataques.

Por otro lado, la Unidad de Análisis Estratégico evalúa el impacto político y estratégico de las operaciones multidominio. Su labor incluye la coordinación con actores gubernamentales y no gubernamentales, con el objetivo de mitigar riesgos asociados a las acciones emprendidas.

La Unidad de Innovación Tecnológica juega un papel clave en el desarrollo y adaptación de herramientas tecnológicas para operaciones futuras. Esta unidad colabora estrechamente con universidades y

empresas tecnológicas, consolidando datos en tiempo real, identificando amenazas y oportunidades, y definiendo objetivos que potencien la efectividad de las operaciones.

El asesoramiento al comandante operacional se realiza a través del Equipo de Asesores Multidominio, que presenta cursos de acción detallados, destacando ventajas, desventajas e impactos potenciales. Además, el equipo transmite las órdenes a las unidades tácticas en cada dominio y monitorea los resultados, ajustando la estrategia según sea necesario para garantizar el cumplimiento de los objetivos establecidos.

Éste esquema se explica en el Anexo 1

3.5 CONTRATISTAS PRIVADOS

3.5.1 DESARROLLO DE TECNOLOGÍA Y EQUIPOS AVANZADOS

Los contratistas privados juegan un papel fundamental en la investigación, desarrollo y provisión de tecnologías innovadoras que refuerzan las capacidades de las fuerzas armadas en las MDO y ciberoperaciones. Su colaboración complementa y potencia los esfuerzos estatales, brindando soluciones tecnológicas avanzadas y servicios estratégicos esenciales para el éxito de estas operaciones.

Entre las tecnologías desarrolladas por los contratistas privados se encuentran sistemas de ciberseguridad, diseñados para la detección y neutralización de amenazas cibernéticas; drones y sistemas autónomos, como los vehículos aéreos no tripulados (UAVs) que apoyan misiones de inteligencia y operaciones tácticas; IA, utilizada para análisis predictivo y correlación de datos en múltiples dominios; y herramientas de guerra electrónica, capaces de interferir en las comunicaciones y radares enemigos.

Esta colaboración se observa en Estados Unidos, donde empresas como Raytheon, Lockheed Martin y Boeing desarrollan sistemas de defensa multidominio y tecnologías cibernéticas avanzadas, las cuales son empleadas por el Pentágono para mantener su ventaja estratégica en el ámbito global.

3.5.2 APOYO OPERACIONAL Y LOGÍSTICO

También desempeñan un rol crucial en el despliegue y sostenimiento de operaciones militares en el terreno, proporcionando servicios esenciales que complementan las capacidades de las fuerzas armadas en contextos operacionales complejos.

Entre sus roles específicos se destacan las funciones de logística, que incluyen el transporte de personal y material, el mantenimiento de equipos y la gestión de suministros en zonas de conflicto. En el ámbito de la ciberinfraestructura, los contratistas son responsables del mantenimiento de redes seguras y de la recuperación de sistemas críticos en caso de ciberataques. Además, en ciertas operaciones, participan directamente en el terreno a través de operaciones in situ, operando equipos especializados como drones o sistemas cibernéticos avanzados.

Esta colaboración se observa en empresas como KBR o DynCorp, que han gestionado servicios logísticos y de infraestructura para las fuerzas armadas estadounidenses durante las operaciones en Irak y Afganistán, demostrando la importancia de los contratistas en el éxito de las misiones militares.

3.5.3 ANÁLISIS DE INTELIGENCIA

Los mismos constituyen un papel esencial en la recolección, procesamiento y análisis de datos, contribuyendo a la generación de inteligencia estratégica y operativa que guía la toma de decisiones en operaciones militares.

Sus roles específicos incluyen el desarrollo de capacidades en inteligencia geoespacial (GEOINT), utilizando imágenes satelitales para identificar movimientos y actividades del adversario. También se destacan en el análisis cibernético, monitoreando redes y actividades en el ciberespacio con el fin de anticipar posibles ataques. Además, manejan grandes volúmenes de información a través del análisis de big data, correlacionando datos de múltiples dominios para detectar amenazas y oportunidades.

Este apoyo se observa en el trabajo de Palantir Technologies, una empresa que proporciona software avanzado de análisis de datos. Sus herramientas han sido empleadas por las fuerzas armadas de Estados Unidos para identificar amenazas en tiempo real, demostrando el impacto directo de los contratistas privados en la inteligencia militar moderna.

3.5.4 PARTICIPACIÓN EN CIBEROPERACIONES

Algunas empresas privadas son contratadas para participar en ciberataques, ya sea de carácter ofensivo o defensivo, en apoyo a los objetivos militares, fortaleciendo las capacidades cibernéticas de las fuerzas armadas.

Entre los roles específicos que desempeñan se encuentra la ciberdefensa, que implica el monitoreo y la protección de sistemas militares críticos frente a posibles intrusiones. En el ámbito ofensivo, desarrollan ataques cibernéticos, como la creación de malware o la explotación de vulnerabilidades en sistemas enemigos para desestabilizar sus capacidades. Además, realizan pruebas de penetración, simulando ataques para identificar debilidades en las redes propias y fortalecer la seguridad de las infraestructuras militares.

Esto muestra la colaboración de empresas como FireEye y Mandiant, que han asistido a gobiernos en el rastreo de ataques cibernéticos y en el desarrollo de contramedidas eficaces, demostrando su valor como aliados estratégicos en el ámbito de la ciberseguridad militar.

3.5.5 ENTRENAMIENTO Y CAPACITACIÓN

Los contratistas privados también juegan un papel clave en la formación de militares y personal civil, proporcionando programas de entrenamiento en áreas críticas que son esenciales para las operaciones modernas.

Entre las áreas de entrenamiento ofrecidas se incluye el uso de tecnologías avanzadas, como drones, sistemas de inteligencia

artificial y herramientas de ciberseguridad. También desarrollan programas de simulación de escenarios, permitiendo a los participantes practicar respuestas a ciberataques y situaciones multidominio. Además, capacitan en guerra electrónica y operaciones conjuntas, mejorando la coordinación entre diferentes fuerzas y dominios operativos.

Este tipo de colaboración se observa en el Reino Unido, donde contratistas privados diseñan simuladores de combate que integran capacidades cibernéticas y terrestres, proporcionando entrenamiento de alta calidad a las fuerzas armadas y preparándolas para los desafíos del campo de batalla contemporáneo.

3.5.6 SOPORTE HUMANITARIO Y DE ESTABILIZACIÓN

En operaciones militares desarrolladas en contextos de crisis humanitaria, los contratistas privados pueden desempeñar un papel esencial al colaborar en tareas que complementan los esfuerzos de las fuerzas armadas y ayudan a estabilizar las áreas afectadas.

Entre sus contribuciones destacan la reconstrucción de infraestructuras críticas, como sistemas de electricidad, agua y comunicaciones, esenciales para restablecer las condiciones básicas de vida. También participan en la provisión de servicios médicos y logísticos destinados a atender las necesidades de la población civil en zonas de conflicto. Además, apoyan en programas de desminado y en el fortalecimiento de la seguridad local, ayudando a crear un entorno más seguro y sostenible para las comunidades afectadas.

Esta colaboración muestra el trabajo de empresas como Halliburton, que participaron en la reconstrucción de infraestructura en Irak, brindando apoyo tanto logístico como civil, demostrando la capacidad de los contratistas privados para contribuir significativamente en escenarios humanitarios complejos.

3.5.7 INTEGRACIÓN MULTIDOMINIO

Los contratistas privados desempeñan un papel crucial en el desarrollo de soluciones que facilitan la interoperabilidad entre sistemas y fuerzas operando en diferentes dominios (Martínez-Valera, 2022), fortaleciendo la coordinación y efectividad de las operaciones multidominio.

Entre sus roles específicos se incluye el diseño de plataformas de comando y control capaces de integrar datos provenientes de dominios cibernéticos, espaciales y tácticos, proporcionando a los comandantes una visión integral del campo de batalla. También desarrollan herramientas para comunicaciones seguras entre dominios, garantizando que la información sensible pueda ser transmitida sin riesgos. Además, trabajan en la optimización de sistemas de detección y respuesta multidominio, mejorando la capacidad de identificar y reaccionar ante amenazas en tiempo real.

La integración con los contratistas privados o empresas se integrarían según Anexo 2.

Un ejemplo práctico de estas iniciativas es el programa JADC2 de EEUU, que se apoya en contratistas privados para conectar sensores y sistemas de armas en múltiples dominios, logrando una integración sin precedentes en las operaciones militares modernas.

3.5.8 VENTAJAS Y DESAFÍOS DE SU PARTICIPACIÓN

El uso de contratistas privados en operaciones militares presenta una serie de ventajas y desafíos que deben considerarse cuidadosamente para maximizar sus beneficios y mitigar los riesgos.

Entre las principales ventajas se encuentra su especialización técnica, que permite a las fuerzas armadas acceder a tecnologías avanzadas que, en muchos casos, no pueden desarrollar internamente. También ofrecen una gran flexibilidad, ya que pueden desplegarse rápidamente en zonas de conflicto o crisis, adaptándose a las necesidades operativas. Además, la reducción de costos es otro beneficio clave, ya que subcontratar ciertas funciones

específicas puede resultar más económico que invertir en el desarrollo interno de esas capacidades.

Sin embargo, también existen desafíos significativos asociados a su utilización. Uno de ellos es la dependencia, ya que una delegación excesiva en contratistas privados puede comprometer la soberanía militar y la capacidad de las fuerzas armadas de operar de manera autónoma. Otro aspecto crítico es el dilema ético, ya que, en algunos casos, los intereses lucrativos de estas empresas pueden entrar en conflicto con los objetivos militares o humanitarios de las misiones.

3.5.9 EMPRESAS ARGENTINAS POTENCIALES PARA COLABORAR CON LAS FUERZAS ARMADAS

Argentina cuenta con una variedad de empresas especializadas en defensa y ciberseguridad que pueden colaborar con las Fuerzas Armadas en operaciones multidominio y ciberoperaciones, aportando capacidades tecnológicas y servicios estratégicos fundamentales. A continuación, se destacan algunas de las principales:

INVAP S.E.: Empresa líder en tecnología, especializada en sistemas de radar, satélites y proyectos nucleares. Su contribución potencial incluye la provisión de sistemas avanzados de vigilancia y comunicaciones, esenciales para operaciones multidominio.

Fabricaciones Militares Sociedad del Estado (FMSE): Organismo estatal dedicado a la producción de armamento, municiones y equipos para la defensa. Puede aportar equipamiento y soporte logístico clave para las fuerzas armadas.

CITEDEF (Instituto de Investigaciones Científicas y Técnicas para la Defensa): Instituto de investigación y desarrollo en tecnologías de defensa. Su contribución se centra en el desarrollo de soluciones tecnológicas innovadoras que potencien las capacidades militares.

VENG S.A.: Empresa especializada en servicios y desarrollos tecnológicos en el ámbito aeroespacial. Ofrece apoyo en proyectos

de satélites y lanzadores, mejorando las capacidades de observación y comunicación estratégica.

Delta Protect: Especialista en ciberseguridad que asiste en la selección e implementación de herramientas de protección. Su potencial radica en la evaluación de vulnerabilidades y el fortalecimiento de la seguridad informática en operaciones militares.

Vates: Empresa de tecnología que ofrece servicios de desarrollo de software y soluciones de TI. Puede contribuir mediante el diseño de sistemas de información y plataformas de comando y control para operaciones multidominio.

Onapsis: Firma especializada en la seguridad de aplicaciones empresariales críticas. Su contribución potencial incluye la protección de sistemas ERP y aplicaciones esenciales para la logística y administración militar.

Estas empresas representan un recurso estratégico para las fuerzas armadas, aportando capacidades técnicas y soluciones innovadoras que pueden fortalecer las operaciones militares y garantizar su éxito en contextos complejos y multidominio.

3.6 CONCLUSIÓN PARCIAL

En este capítulo demuestra que la creación de un órgano de comando, control, asesoramiento y asistencia para la toma de decisiones en el ámbito operacional de las Fuerzas Armadas Argentinas es esencial para enfrentar los desafíos de las operaciones multidominio. La experiencia de España y Estados Unidos resalta la importancia de estructuras organizativas flexibles e integradas, capaces de coordinar recursos y fuerzas en los dominios terrestre, marítimo, aéreo, cibernético y espacial.

Se destaca que un órgano de estas características debe garantizar la interoperabilidad entre los distintos dominios y niveles de comando, promoviendo la colaboración interagencial y la interacción con actores no estatales. Asimismo, la incorporación de tecnologías avanzadas, como sistemas de inteligencia artificial y plataformas de comando y control en

tiempo real, resulta fundamental para optimizar la planificación y ejecución de operaciones.

Por último, el diseño de este órgano en el contexto argentino debe considerar las capacidades existentes, los recursos disponibles y las particularidades del entorno geoestratégico nacional. La implementación efectiva de esta estructura fortalecerá la defensa nacional.

La propuesta de un centro conjunto multidominio, basada en experiencias internacionales y adaptada al contexto nacional, sintetiza los elementos analizados a lo largo de este trabajo y ofrece una solución integral para enfrentar los desafíos actuales y futuros en el ámbito de la defensa.

CONCLUSIONES

Las operaciones multidominio constituyen una herramienta estratégica indispensable para abordar los desafíos modernos en el ámbito de la defensa nacional. A través de este trabajo, se identificaron las capacidades tecnológicas, doctrinarias y estructurales necesarias para que las Fuerzas Armadas Argentinas integren esta modalidad operativa de manera efectiva.

El análisis de doctrinas internacionales, como las de Estados Unidos y España, resalta la importancia de una planificación conjunta que combine los dominios tradicionales (tierra, mar y aire) con los emergentes (espacial y cibernético). Estas experiencias permiten extraer lecciones valiosas, como la necesidad de contar con estructuras flexibles de comando y control que promuevan la interoperabilidad y la respuesta ágil ante amenazas híbridas y asimétricas.

En el contexto argentino, la implementación de operaciones multidominio requiere superar limitaciones actuales, como la escasez de recursos tecnológicos y la fragmentación entre organismos estatales y privados. No obstante, iniciativas como el programa satelital SAOCOM y la creación del Comando Conjunto de Ciberdefensa demuestran que existen bases sólidas sobre las cuales construir una estrategia efectiva.

Se concluye que la creación de un centro conjunto multidominio, diseñado para integrar las capacidades de todos los dominios y actores involucrados (U.S. Army Training and Doctrine Command, 2018; Royal United Services Institute, 2022), es una prioridad estratégica. Este centro debe incluir sistemas de comando y control avanzados, mecanismos de cooperación interagencial y una visión a largo plazo que garantice su sostenibilidad y evolución frente a las amenazas emergentes.

Finalmente, se proyecta que, al adoptar este modelo, las Fuerzas Armadas Argentinas no solo fortalecerán su capacidad de defensa nacional, sino que también contribuirán significativamente a la seguridad regional, posicionándose como un actor clave en el ámbito geoestratégico de América Latina.

MARCO INSTITUCIONAL Y REGULATORIO

La creación de una Estrategia Nacional de Operaciones Multidominio y Ciberoperaciones es esencial para definir las prioridades, roles y responsabilidades de las Fuerzas Armadas, el sector privado y otros actores estatales, garantizando una coordinación efectiva y alineada con los objetivos de seguridad nacional.

El objetivo principal de esta estrategia es establecer un marco claro que permita a todos los actores involucrados trabajar en conjunto, maximizando recursos y capacidades. Entre los componentes clave se incluyen:

- Lineamientos para la cooperación público-privada, que promuevan la colaboración entre las Fuerzas Armadas y contratistas privados en áreas críticas como ciberseguridad, logística y tecnología avanzada.
- Protocolos para el intercambio de información entre contratistas y el Estado, asegurando que los datos relevantes fluyan de manera segura y eficiente para apoyar la toma de decisiones operativas.
- Regulaciones para la protección de información sensible, con el fin de evitar filtraciones o accesos no autorizados que puedan comprometer la seguridad nacional.

Propuesta: El liderazgo en la creación de esta estrategia debe recaer en el Ministerio de Defensa, en colaboración con el Ministerio de Ciencia, Tecnología e Innovación y el Ministerio de Seguridad. Esta coordinación interministerial garantizará que la estrategia incorpore perspectivas tecnológicas, operativas y de seguridad, logrando un enfoque integral para abordar los desafíos de las operaciones multidominio y ciberoperaciones.

FORTALECER LA COOPERACIÓN PÚBLICO-PRIVADA

El establecimiento de convenios de colaboración entre el Estado y empresas nacionales especializadas en defensa y ciberseguridad es una estrategia clave para fortalecer las capacidades operativas del país. Estos acuerdos permitirían desarrollar soluciones específicas y adaptadas a las necesidades de las Fuerzas Armadas. Por ejemplo, una posible colaboración entre INVAP, especializada en sistemas de radar, y RAN Security, experta en ciberseguridad, podría dar lugar al diseño de sistemas de radar integrados con capacidades avanzadas de protección cibernética. Del mismo modo, Delta

Protect podría contribuir evaluando vulnerabilidades y fortaleciendo la seguridad de estas infraestructuras.

Paralelamente, es fundamental promover la industria de defensa nacional, incentivando la inversión en el desarrollo de tecnologías propias para reducir la dependencia de proveedores extranjeros. Esto incluye la creación de un programa de financiación destinado a startups y empresas tecnológicas capaces de ofrecer soluciones innovadoras en el ámbito de la defensa y la ciberseguridad.

un fondo nacional gestionado por el Banco de Inversión y Comercio Exterior (BICE), dedicado a financiar proyectos de investigación y desarrollo en defensa. Este fondo permitiría movilizar recursos hacia sectores clave, fomentando la innovación tecnológica y fortaleciendo la autonomía estratégica del país.

DESARROLLO DE UN CENTRO MULTIDOMINIO Y CIBERNÉTICO

La creación de un centro estratégico para operaciones multidominio y ciberoperaciones puede estructurarse en dos fases principales, enfocándose en la planificación, diseño e implementación progresiva.

Fase 1: Planificación y Diseño

En esta etapa, se debe conformar un grupo interdisciplinario que diseñe la estructura organizativa y defina las funciones específicas del centro. Este equipo debe incluir expertos de las Fuerzas Armadas, académicos, y representantes de empresas tecnológicas. La participación de contratistas privados es clave; por ejemplo, VENG podría aportar su conocimiento en el diseño de sistemas espaciales y de comunicación, fundamentales para las operaciones multidominio.

Fase 2: Implementación

En esta fase, se establecería el centro en una ubicación estratégica, como Córdoba, donde ya existe un ecosistema tecnológico consolidado que incluye capacidades aeroespaciales y de innovación. El centro debe integrar capacidades cibernéticas, espaciales y logísticas, aprovechando la tecnología y los servicios ofrecidos por contratistas privados para asegurar una operatividad eficiente y avanzada.

Propuesta: Se recomienda lanzar un proyecto piloto utilizando tecnologías ya existentes, lo que permitiría probar y ajustar la funcionalidad del centro en sus primeras etapas. A medida que se identifiquen necesidades y oportunidades, el alcance del centro podría expandirse gradualmente, incorporando nuevas capacidades y tecnologías avanzadas. Esta estrategia progresiva garantizará un desarrollo sostenible y exitoso del proyecto.

INTEGRACIÓN DE CONTRATISTAS EN OPERACIONES MILITARES

La asignación de roles específicos para los principales actores nacionales en operaciones multidominio y ciberoperaciones es esencial para maximizar las capacidades y recursos disponibles. Entre las responsabilidades propuestas:

- INVAP: Lideraría el desarrollo de sistemas de radar, satélites y monitoreo geoespacial, fundamentales para la vigilancia y el control en operaciones multidominio.
- RAN Security y Delta Protect: Se encargarían de fortalecer la ciberseguridad, protegiendo infraestructuras críticas y asegurando la resiliencia de las redes frente a amenazas.
- Vates y Onapsis: Estarían a cargo del desarrollo de software para sistemas de comando y control, así como de herramientas tecnológicas que optimicen la gestión de operaciones. Además, podrían colaborar en la capacitación tecnológica del personal militar.

En el ámbito de la capacitación y entrenamiento, estas empresas podrían trabajar junto al Ejército Argentino, la Armada Argentina y la Fuerza Aérea Argentina, diseñando programas de formación en el uso de tecnologías avanzadas, ciberseguridad y operaciones multidominio.

Propuesta: Se recomienda establecer una oficina de enlace dentro del Comando Conjunto de las Fuerzas Armadas. Esta oficina sería responsable de coordinar y supervisar la colaboración con los contratistas privados, asegurando una integración efectiva de sus capacidades en las operaciones militares y alineando sus contribuciones con los objetivos estratégicos de la defensa nacional.

IMPLEMENTACIÓN DE TECNOLOGÍAS AVANZADAS

La definición de proyectos prioritarios en operaciones multidominio y ciberoperaciones permitirá enfocar los esfuerzos tecnológicos y estratégicos en áreas clave para fortalecer la seguridad nacional. Los proyectos se dividen en las siguientes categorías:

- Ciberoperaciones: Se propone implementar sistemas avanzados de detección y respuesta a ciberamenazas desarrollados por RAN Security y Delta Protect, y utilizar las tecnologías de Onapsis para proteger aplicaciones críticas, asegurando la resiliencia de los sistemas esenciales.
- Sistemas de Radar y Vigilancia: Se recomienda integrar los sistemas de radar desarrollados por INVAP con capacidades de análisis de datos, permitiendo su uso en operaciones multidominio y mejorando la capacidad de vigilancia y control en tiempo real.
- Comando y Control: El desarrollo de plataformas de integración multidominio, en colaboración con Vates, conectará datos de los dominios terrestre, marítimo, aéreo, cibernético y espacial, proporcionando a los comandantes una visión integral del entorno operativo.
- Inteligencia Artificial y Big Data: Se sugiere utilizar herramientas como las ofrecidas por Palantir para analizar grandes volúmenes de datos y predecir movimientos adversarios, fortaleciendo la toma de decisiones estratégicas.

Propuesta: Para asegurar una implementación efectiva, se sugiere desplegar estos sistemas en fases, comenzando con un teatro de operaciones piloto, como la vigilancia de la frontera norte. Este enfoque permitirá probar las capacidades integradas, realizar ajustes según las necesidades específicas y escalar gradualmente el alcance de los proyectos prioritarios en todo el territorio nacional.

CREACIÓN DE PROGRAMAS DE ENTRENAMIENTO Y SIMULACIÓN

El desarrollo de simuladores multidominio y programas de entrenamiento en ciberoperaciones es fundamental para preparar a las fuerzas armadas frente a los desafíos contemporáneos en el ámbito de la defensa.

- Simuladores Multidominio: Se propone que contratistas privados diseñen simuladores que integren escenarios terrestres, marítimos, aéreos y

cibernéticos, ofreciendo un entorno de entrenamiento que refleje la complejidad de las operaciones multidominio.

- Entrenamiento en Ciberoperaciones: Diseñar programas de capacitación para las fuerzas armadas enfocados en temas clave como ciberdefensa, manejo de inteligencia artificial y uso de sistemas autónomos. Estos entrenamientos fortalecerían las capacidades del personal militar para operar en un entorno digital y multidominio, alineando sus habilidades con las demandas tecnológicas actuales.

Propuesta: Crear un centro de simulación en colaboración con CITEDEF y Delta Protect, combinando la experiencia técnica y el conocimiento de estos actores para desarrollar un sistema de simulación avanzado y adaptado a las necesidades operativas nacionales.

La integración que combina simulación y capacitación, mejorará significativamente la preparación y efectividad de las fuerzas armadas, permitiéndoles enfrentar los desafíos en los diferentes dominios operacionales.

MEDICIÓN Y AJUSTE

El monitoreo del progreso y la revisión continua son aspectos clave para garantizar el éxito y la sostenibilidad de la colaboración entre el Estado y los contratistas privados en operaciones multidominio y ciberoperaciones.

- Monitoreo del Progreso: Se debe establecer un conjunto de indicadores de éxito que permitan evaluar de manera objetiva el impacto de estas colaboraciones. Por ejemplo, uno de los indicadores podría ser la reducción de los tiempos de respuesta a ciberamenazas en un 50% en un plazo de dos años, lo que reflejaría una mejora significativa en la capacidad de ciberdefensa.
- Revisión y Expansión: Basándose en los resultados obtenidos, el modelo de cooperación público-privada puede ajustarse para mejorar su efectividad. Esto incluye identificar áreas que requieran optimización o fortalecer ciertos aspectos de la colaboración. Asimismo, si los resultados lo justifican, se podría ampliar la colaboración hacia empresas internacionales que puedan aportar tecnologías o conocimientos

complementarios para satisfacer necesidades específicas no cubiertas por los actores nacionales.

Esto garantizará que las colaboraciones evolucionen de acuerdo con los objetivos estratégicos, maximizando los beneficios para la seguridad nacional y optimizando el uso de recursos en el ámbito de defensa y ciberseguridad.

IMPACTO ESPERADO

El desarrollo de capacidades multidominio y ciberseguridad en Argentina requiere una visión estratégica que contemple metas a corto, mediano y largo plazo, permitiendo avances progresivos en la defensa nacional y su proyección regional.

Corto plazo: En esta etapa inicial, el objetivo principal es fortalecer la protección de infraestructuras críticas, garantizando la seguridad de los sistemas esenciales del país frente a ciberamenazas. Además, se busca mejorar la capacidad de las Fuerzas Armadas para realizar operaciones conjuntas, integrando recursos y tecnologías disponibles para una mayor efectividad operativa.

Mediano plazo: A medida que se consoliden las capacidades básicas, se enfocará en el despliegue de tecnologías avanzadas en misiones multidominio. Esto incluye la integración de sistemas de inteligencia artificial, drones, ciberseguridad y plataformas de comando y control, optimizando las operaciones en diferentes dominios y entornos complejos.

Largo plazo: Finalmente, el objetivo estratégico es posicionar a Argentina como un referente regional en defensa multidominio y ciberseguridad. Esto implica no solo el desarrollo de capacidades tecnológicas y operativas de vanguardia, sino también la consolidación de alianzas internacionales y la exportación de tecnologías nacionales, fortaleciendo el rol del país como líder en el ámbito de la defensa en América Latina.

Este enfoque escalonado asegura avances sostenidos, adaptándose a las necesidades inmediatas mientras se construyen las bases para un liderazgo a largo plazo en el ámbito de la seguridad y la defensa multidominio.

BIBLIOGRAFÍA

1. Ley de Defensa Nacional N.º 23.554. (1988). Publicada en el Boletín Oficial de la República Argentina.

2. Ley de Seguridad Interior N.º 24.059. (1992). Publicada en el Boletín Oficial de la República Argentina.

3. Decreto Reglamentario de la Ley de Defensa Nacional N.º 727/2006. (2006). Publicado en el Boletín Oficial de la República Argentina.

4. Decreto de Creación del Comando Conjunto de Ciberdefensa N.º 641/2019. (2019). Publicado en el Boletín Oficial de la República Argentina.

5. Ministerio de Defensa de España. (2018). Publicación Doctrinal Conjunta para el empleo de las fuerzas armadas. Madrid: Ministerio de Defensa.

6. TRADOC. (2017). Multidomain Operations (MDO). Army Training and Doctrine Command. Estados Unidos.

7. Academia de las Ciencias y las Artes Militares. (2020). Batalla narrativa y dominios cognitivos. Madrid, España.

8. Angulo Molina, R. O. (2019). Análisis comparativo de capacidades multidominio en grandes potencias. Revista de Estrategia y Defensa, 6(2), 34-56.

9. Iturriaga Delgado, S. (2021). Incorporación del espectro electromagnético y espacio en operaciones modernas. Revista Internacional de Seguridad, 10(1), 22-40.

10. U.S. Army Training and Doctrine Command. (2018). The U.S. Army in Multi-Domain Operations 2028. TRADOC Pamphlet 525-3-1. https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

11. Royal United Services Institute. (2022). Project Convergence 22: An Important Step Towards Multi-Domain Integration.

12. Rodriguez, J. P. (2020). Las operaciones de información multidominio y el equipo de combate de brigada: Lecciones aprendidas del ejercicio Cyber Blitz 2018. Military Review, Primer Trimestre, 72-83.

13. Martínez-Valera, G. (2022). El enfrentamiento avanzado: las operaciones multidominio. Global Strategy Report, 20.

14. Clúster de la Industria de Defensa. (2022). La guerra multidominio y mosaico.

15. U.S. Army. (2019). Cyber Blitz, Orient Shield build future capabilities, multi-domain operations partnership. https://www.army.mil/article/228113/cyber_blitz_orient_shield_build_future_capabilities_multi_domain_operations_partnership

Anexo 1: Propuesta de esquema de un Centro Multidominio y Cibernético

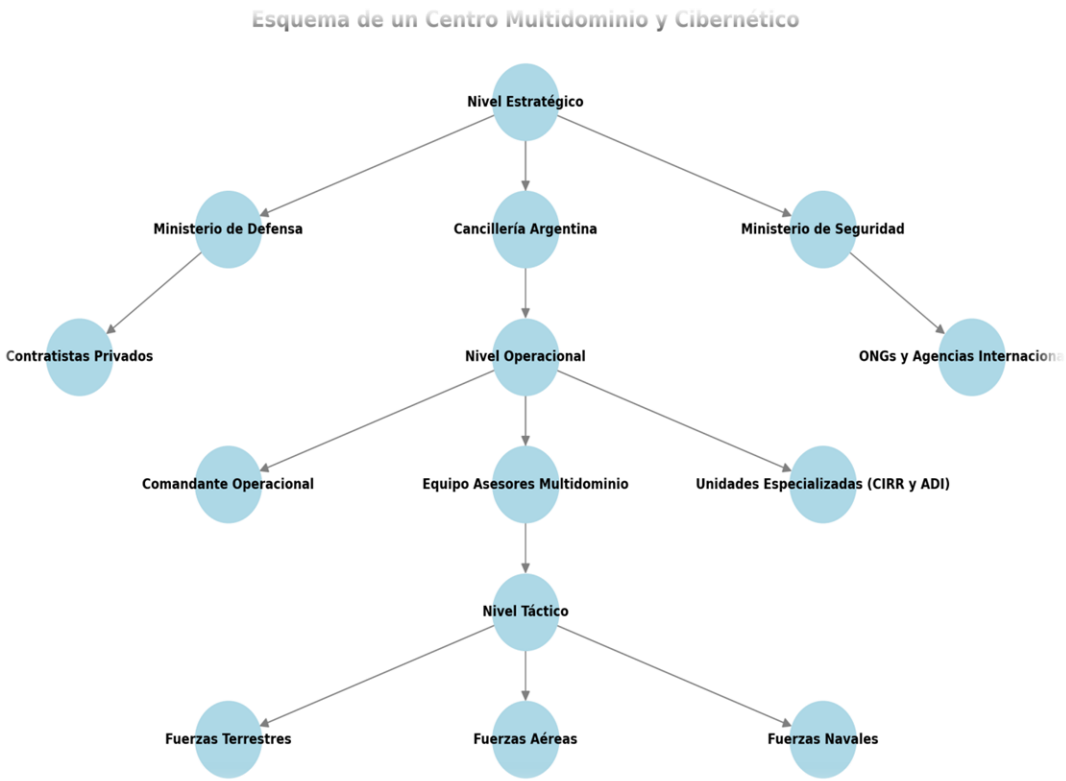

Diagrama del centro multidominio y cibernético (Elaboración propia).

Nivel Estratégico: Representado por las instituciones gubernamentales clave (Defensa, Relaciones Exteriores y Seguridad), que establecen objetivos y directrices generales.

Nivel Operacional: Encabezado por el Comandante Operacional, con apoyo del Equipo de Asesores Multidominio y Unidades Especializadas (como el CIRR y los ADI).

Nivel Táctico: Representado por las fuerzas desplegadas en los diferentes dominios (terrestres, aéreas y navales), ejecutando las directrices operacionales.

Interacción con Actores Externos: Contratistas privados y ONGs/agencias internacionales que aportan capacidades tecnológicas y humanitarias, vinculándose con el nivel estratégico.

Anexo 2: Esquema propuesto para la Integración de Contratistas Privados en las Fuerzas Armadas

```
A [Ministerio de Defensa] -->|Establece políticas y directrices| B [Comando Conjunto de las Fuerzas Armadas]
B -->|Coordina operaciones| C [Contratistas Privados]
C -->|Proveen tecnología y servicios| D [Ejército Argentino]
C -->|Proveen tecnología y servicios| E [Armada Argentina]
C -->|Proveen tecnología y servicios| F [Fuerza Aérea Argentina]
D -->|Implementan en operaciones| G [Unidades Operativas]
E -->|Implementan en operaciones| G
F -->|Implementan en operaciones| G
```

Esquema de Integración de Contratistas Privados en las Fuerzas Armadas Argentinas. (Elaboración propia)

El esquema se explica y describe de la siguiente manera:

Ministerio de Defensa: Define las políticas y directrices generales para la defensa nacional.

Comando Conjunto de las Fuerzas Armadas: Coordina las operaciones y la implementación de las políticas establecidas.

Contratistas Privados: Proporcionan tecnología avanzada, servicios de ciberseguridad, entrenamiento y apoyo logístico.

Ejército Argentino, Armada Argentina y Fuerza Aérea Argentina: Trabajan en conjunto con los contratistas para integrar las soluciones proporcionadas en sus operaciones.

Unidades Operativas: Implementan en el terreno las tecnologías y estrategias desarrolladas en colaboración con los contratistas.