



Las operaciones multidominio en la guerra Rusia - Ucrania y su incidencia en la doctrina de operaciones de información.

Jimbo Galarza, José Homero y Oña Toapanta, Franklin Alfredo

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Defensa y Seguridad

Trabajo de titulación, previo a la obtención del título de Magíster en “Defensa y Seguridad mención Conducción Militar”

PhD. Galarza Torres, Sandra Patricia

20 Septiembre de 2023



Oña-Jimbo Análisis operaciones mult...

Scan details

Scan time:
September 6th, 2023 at 12:19 UTC

Total Pages:
91

Total Words:
22749

Plagiarism Detection



Types of plagiarism		Words
● Identical	1.3%	291
● Minor Changes	0.8%	184
● Paraphrased	1.3%	290
○ Omitted Words	0%	0

AI Content Detection



Text coverage
● AI text
○ Human text

PhD. Galarza Torres, Sandra

C.C.: 1717671422

Directora



Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación: **“Las operaciones multidominio en la guerra Rusia - Ucrania y su incidencia en la doctrina de operaciones de información”** fue realizado por los señores **Jimbo Galarza, José Homero y Oña Toapanta, Franklin Alfredo**; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 20 de septiembre de 2023.

PhD. Galarza Torres, Sandra

C.C.: 1717671422



Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de Autoría

Nosotros **Jimbo Galarza, José Homero** con cédula de ciudadanía nº 1103058374 y **Oña Toapanta, Franklin Alfredo** con cédula de ciudadanía nº 1002659520, declaramos que el contenido, ideas y criterios del trabajo de titulación: “**Las operaciones multidominio en la guerra Rusia - Ucrania y su incidencia en la doctrina de operaciones de información**” es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 20 de septiembre de 2023.

Jimbo Galarza, José Homero

C.C.: 1103058374

Oña Toapanta, Franklin Alfredo

C.C.:1002659520



Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Autorización de Publicación

Nosotros **Jimbo Galarza, José Homero** con cédula de ciudadanía n°1103058374 y **Oña Toapanta, Franklin Alfredo** con cédula de ciudadanía n°1002659520, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: “**Las operaciones multidominio en la guerra Rusia - Ucrania y su incidencia en la doctrina de operaciones de información**” en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 20 de septiembre de 2023.

Jimbo Galarza, José Homero

C.C.:1103058374

Oña Toapanta, Franklin Alfredo

C.C.:1002659520

Dedicatoria

El presente trabajo, esta dedicado al todo poderoso que nos brinda la vida y salud, es quien ilumina nuestras acciones diarias, a mi amada esposa Sandra Ivonne, quien es el pilar y seguridad de mi hogar, a mis hijos Daniel e Isabella, que día a día alegran mi existir brindandome amor y ternura, a mis padres que me inculcaron valores y a luchar en los peores momentos, mi padre que desde el cielo mi guía y cuida, a mi familia y amigos que nos ayudan a seguir cosechando triunfos.

Gracias a los docentes y tutores que supieron guiar esta investigación, sin duda ha enriquecido nuestro aserbo cultural con conocimiento nuevo.

Franklin Alfredo Oña Toapanta.

El presente trabajo de investigación está dedicado a mi familia quienes son el pilar fundamental y la motivación que me impulsan a seguir día a día superando todos los obstáculos para alcanzar las metas y lograr el desarrollo personal y profesional.

A mi querida esposa que siempre me apoya en las decisiones a lo largo de toda nuestra vida juntos y es quien vela por el nuestro hogar ante mi ausencia, a mi querida hija Sofia que con su esfuerzo y dedicación es un ejemplo desde muy pequeña de como se alcanzan los objetivos, a mi pequeña hija Verito Anahi que con sus ideas me alegra cada instante de la vida.

Mención especial a mi querida Madre que es ejemplo de fortaleza que siempre me ha guiado por el camino del bien y que sus consejos siempre son los más adecuados.

A mi recordado Padre que desde el cielo se siente alagado por los objetivos cumplidos por sus hijos y que mientras me acompaño con su presencia fue una demostración de como con esfuerzo dedicación se alcanzan las metas, y que estoy seguro que desde el cielo está muy orgulloso de ver la consolidación de su hijo y que siempre está presente con sus bendiciones.

A mi querida institución que me ha permitido el desarrollo académico acorde a las nuevas exigencias del mundo actual.

José Homero Jimbo Galarza.

Agradecimiento

Nuestro agradecimiento eterno al Señor que nos puso en el camino correcto para hacer de nuestra profesión militar, nuestra razón de vivir, nuestro ejemplo para nuestros hijos y las futuras generaciones militares. A nuestros profesores de la Academia de Guerra del Ejército y de nuestra eterna Universidad de las Fuerzas Armadas un agradecimiento extenso, quienes supieron brindarnos la oportunidad de crecer académicamente y ampliar nuestros conocimientos para complementar en nuestras actividades profesional al mando de unidades militares y personal profesional.

A nuestra amada familia, queremos agradecerles de todo corazón. Su apoyo inquebrantable, amor y paciencia han sido fundamentales en cada paso que he dado. Finalmente, agradecemos a nuestros compañeros, amigos y a todas las personas que participaron en este trabajo, así como a quienes de alguna manera contribuyeron a la realización de esta tesis. Sus aportaciones fueron esenciales para la consecución de este trabajo.

Jose Homero

Franklin Alfredo

Índice de contenidos

Resultados de la herramienta para prevención y/o verificación de similitud de contenidos	2
Certificación	3
Responsabilidad de Autoría	4
Autorización de Publicación	5
Dedicatoria	6
Agradecimiento	8
Resumen	16
Capítulo I	18
El Problema de Investigación	18
Planteamiento del problema	18
Formulación del problema de investigación.....	20
Subproblemas o preguntas de investigación	21
Antecedentes	21
Justificación	24
Objetivos.....	26
Objetivo General.....	26
Objetivos Específicos	26
Capítulo II	27
Marco de Referencia.....	27

	10
Estado del arte	27
Marco teórico.....	29
Operaciones multidominio en la guerra Rusia-Ucrania	31
El ciberespacio y la ciberguerra	34
El multidominio desde la perspectiva de la prevención y resolución de conflictos ..	37
Evolución de la doctrina militar ecuatoriana	37
Proceso de desarrollo y transformación de las capacidades militares	40
Escenarios prospectivos de las amenazas a la defensa y seguridad el Estado ecuatoriano	41
La guerra híbrida y el multidominio	44
Operaciones de la Información en el Contexto de la Guerra Multidominio.....	46
Concepción de operaciones de multidominio en la doctrina militar actual	49
Implicaciones de las operaciones multidominio en el sistema de defensa y seguridad del Estado.....	50
Marco conceptual.....	51
Amenazas a la seguridad del Estado	51
Guerra Híbrida.....	52
Multidominio.....	53
Operaciones de la información	53
Complejidad.....	54
Marco Legal.....	55
Sistemas de variables	57

	11
Definición nominal	57
Definición conceptual	58
Definición operacional	58
Hipótesis.....	59
Hipótesis general:	59
Hipótesis específicas:.....	59
Operacionalización de las variables	61
Capítulo III.....	62
Marco Metodológico.....	62
Metodología.....	62
Tipo de investigación	62
Diseño de la investigación	63
Población.....	64
Muestra.....	64
Técnicas e instrumentos de recolección de datos	65
Revisión bibliográfica documental.....	65
Entrevista.....	65
Encuesta	66
Instrumentos de recolección de datos	66
Capítulo IV	67
Resultados de la investigación	67

	12
Análisis e interpretación de resultados.....	67
Resumen de resultados de la entrevista	76
Análisis de los Resultados de las Entrevistas sobre Operaciones Multidominio y Operaciones de Información en el Conflicto Rusia-Ucrania.....	76
Capítulo V	78
Propuesta de la investigación.....	78
Propuesta doctrinaria de operaciones multidominio en las FFAA del Ecuador	78
Introducción.....	78
Antecedentes	79
Justificación.....	81
Metodología.....	82
Evolución de las operaciones multidominio.....	83
Aplicación doctrinaria	84
Operaciones multidominio en la seguridad y defensa	85
Operaciones militares en entornos urbanos	85
Operaciones militares en el espacio aéreo.....	85
Operaciones militares en entornos ciberespaciales	86
Doctrina Integral de Operaciones Multidominio en la Seguridad y Defensa Nacional: Cimientos y Fundamentos	87
La Fundamentación Estratégica de las Operaciones Militares Multidominio en Entornos Urbanos para las Fuerzas Armadas del Ecuador.....	89

Doctrina para las Operaciones Militares Multidominio en entornos aéreos de las Fuerzas Armadas del Ecuador.....	91
Doctrina para las Operaciones Militares Multidominio en entornos marítimos de las Fuerzas Armadas del Ecuador.....	95
Doctrina para las Operaciones Militares Multidominio para el ciberespacio de las Fuerzas Armadas del Ecuador.....	97
Conceptos clave	98
Mecanismos para la implementación de la propuesta doctrinaria	100
Validación de la propuesta.....	102
Capítulo V	106
Conclusiones y Recomendaciones	106
Conclusiones.....	106
Recomendaciones.....	107
Bibliografía	108

Índice de tablas

<i>Tabla 1</i> Conceptualización de las variables.....	58
<i>Tabla 2</i> Definición operacional de las variables.....	58
<i>Tabla 3</i> Operacionalización de las variables.....	61
<i>Tabla 4</i> Ámbitos de las operaciones multidominio.....	67
<i>Tabla 5</i> Eficiencia del desarrollo cualitativo de la fuerza de combate.....	68
<i>Tabla 6</i> Dependencia de la tecnología.....	69
<i>Tabla 7</i> Efectividad del empleo de las operaciones multidominio.....	70
<i>Tabla 8</i> Aplicación de operaciones multidominio en las Fuerzas Armadas del Ecuador.....	71
<i>Tabla 9</i> Integración de doctrina.....	73
<i>Tabla 10</i> Aplicación de las operaciones multidominio para evitar posición de desventaja.....	74
<i>Tabla 11</i> Factibilidad de desarrollo de una propuesta doctrinaria de operaciones multidominio.....	75
<i>Tabla 12</i> Mecanismos de implementación.....	101
<i>Tabla 13</i> Cuadro resumen análisis FODA de la propuesta.....	102

Índice de figuras

<i>Figura 1 Competencia militar.....</i>	<i>33</i>
<i>Figura 2 Ámbitos de las operaciones multidominio</i>	<i>67</i>
<i>Figura 3 Eficiencia del desarrollo cualitativo de la fuerza de combate.....</i>	<i>68</i>
<i>Figura 4 Dependencia de la tecnología.....</i>	<i>70</i>
<i>Figura 5 Efectividad del empleo de las operaciones multidominio.....</i>	<i>70</i>
<i>Figura 6 Aplicación de operaciones multidominio en las Fuerzas Armadas del Ecuador</i>	<i>72</i>
<i>Figura 7 Integración de doctrina.....</i>	<i>73</i>
<i>Figura 8 Aplicación de las operaciones multidominio para evitar posición de desventaja</i>	<i>74</i>
<i>Figura 9 Factibilidad de desarrollo de una propuesta doctrinaria de operaciones multidominio</i>	<i>75</i>

Resumen

El presente trabajo investigativo “Las operaciones multidominio en la guerra Rusia - Ucrania y su incidencia en la doctrina de operaciones de información”, recaba información de los problemas de defensa y seguridad mundial, regional y local, considernado el ejemplo del conflicto Rusia-Ucrania, que empezo coomo una guerra convencional y que con el tiempo su desarrollo se ha visto envuelto en conflictos cambiantes, dando lugar a las guerras asimétricas o híbridas, sin duda tema de debates académicos en las diferentes academias de guerra, así como debates políticos-estratégicos, económicos, de religión y tambien la parte social, es ahí que la investigación se fundamento en las operaciones multidominio que se vienen realizando en dicho conflicto, desde los niveles político-estratégico, estratégico y táctico, y como cada uno de estos componentes afectan al desarrollo del conflicto, lo que ha tenido injerencia en nuestro país, sobre las operaciones de información que fuerzas armadas ha venido implementando, convirtiendose en el nuevo paradigma táctico-operacional de los ejércitos a nivel mundial y el nuestro propio, por el mismo hecho de la evolución de las amezas y desarrollo tecnológico, al final se propone realizar una actualización doctrinaria de las operaciones multidominio con especial atención al desarrollo de las capacidades del ejército y la transformación que se viene desarrollando.

Palabras claves: multidominio, conjuntez, interoperabilidad, híbrido, amenazas

Abstract

The present investigative work "Multi-domain operations in the Russia - Ukraine war and its impact on the doctrine of information operations", collects information on global, regional and local defense and security problems, considering the example of the Russia-Ukraine conflict, that began as a conventional war and that over time its development has been involved in changing conflicts, giving rise to asymmetric or hybrid wars, undoubtedly the subject of academic debates in the different war academies, as well as political-strategic debates, economic, religious and also the social part, it is there that the research is based on the multi-domain operations that have been carried out in said conflict, from the political-strategic, strategic and tactical levels, and how each of these components affect the development of the conflict, which has had an interference in our country, on the information operations that the armed forces have been implementing, becoming the new tactical-operational paradigm of the armies worldwide and our own, due to the same fact of evolution of the threats and technological development, in the end it is proposed to carry out a doctrinal update of multi-domain operations with special attention to the development of the army's capabilities and the transformation that is being developed.

Keywords: multidomain, conjunction, interoperability, hybrid, threats

Capítulo I

El Problema de Investigación

Planteamiento del problema

El conflicto en curso entre Rusia y Ucrania es un reflejo de las operaciones multidominio complejas que se están llevando a cabo en la guerra moderna y que han sido teorizadas en los últimos años. El uso de drones, armas hipersónicas, aeronaves de todos los tamaños y tipos además del empleo de fuerzas terrestres, todas trabajando al unísono en un contexto de sanciones económicas y presión diplomática determinan las características de las operaciones multidominio.

Tradicionalmente, las guerras se han librado en tierra, mar, aire y, en cierta medida, en el espacio. En las últimas dos décadas, este espectro ha aumentado para abarcar dominios cibernéticos y de información. Los primeros cuatro dominios son clásicamente físicos y los otros dos son virtuales. El efecto global de la cibernética y la información en la conducción de las guerras convencionales ha creado un espectro de conflicto nuevo, híbrido y de múltiples dominios, lo que ha dado lugar a que las tácticas y estrategias más antiguas pasen de moda.

En este contexto y considerando el desarrollo de las amenazas a la seguridad y la defensa del Estado ecuatoriano, las medidas que se tomen para garantizar la integridad y soberanía del Ecuador deben estar acordes con la concepción moderna de la guerra (Comando Conjunto de Fuerzas Armadas, 2019). Ante esto se puede afirmar que, para asegurar que se cumpla con el mandato constitucional, existe un imperativo definitivo para, reformar, rediseñar y reconstruir la maquinaria de guerra tradicional y de esta manera lograr la adaptación a este nuevo paradigma emergente. En este sentido son muchos los esfuerzos que se hacen, sobre todo en la concepción del desarrollo y transformación de las capacidades militares, sin embargo, la evolución de los conflictos muchas veces trasciende a estos procesos sobre todo

en la concepción y adaptación de este tipo de paradigmas que transforman la visión de la doctrina convencional.

Considerando que a medida que la interconexión de la información produce conocimiento y modelos de gestión de la defensa, un ataque cibernético en las redes utilizadas puede paralizar las estructuras de comando y control. Lo que infiere que, en una próxima guerra, el enemigo podría no ser un país o una organización definida sino un ente híbrido transnacional no estatal implicando que muchas veces nunca se sabría quiénes son los perpetradores de un ataque, e incluso dados los avances tecnológicos que utilizan las amenazas relacionadas con el crimen cibernético no se podría cuándo ni desde dónde tendría lugar un ataque. En el futuro inmediato, al no concebir adecuadamente a las operaciones multidominio y tomar las medidas adecuadas los riesgos de ser atacados en todos los frentes, que incluyen, el estrangulamiento económico, el aislamiento diplomático, los cortes de información o la negación distribuida de servicios, puede suceder incluso antes de disparar una sola bala en un hipotético conflicto armado convencionalmente esperado.

Es muy probable que la guerra futura sea de naturaleza híbrida y el espectro del conflicto se extienda a través de todos los dominios, desde convencional a subconvencional, cinético a no cinético y letal a no letal, todo bajo una proyección nuclear. Las armas que se analizan en la actualidad en las operaciones multidominio en la guerra de Ucrania Rusia van desde pequeños virus informáticos hasta misiles hipersónicos. Es así que el análisis de esta realidad de la guerra moderna debe considerarse en la gestión de la defensa y en el desarrollo de capacidades necesarias para asumirla con la responsabilidad constitucional pertinente en el contexto doctrinario respectivo.

En un entorno de conflictos internacionales y en constante evolución, la naturaleza de la guerra ha experimentado transformaciones significativas, caracterizadas por la integración de tecnologías avanzadas y la interconexión de múltiples dominios. El conflicto entre Rusia y Ucrania ha servido como un ejemplo ilustrativo de cómo las operaciones multidominio y de

información han sido empleadas de manera simultánea y coordinada para lograr objetivos estratégicos. Estas estrategias han redefinido la forma en que se libran los conflictos modernos, trascendiendo las fronteras tradicionales y enfocándose en la combinación de operaciones en el terrestre, marítimo, aéreo, ciberespacial y espacio exterior.

En este enfoque, el problema central de esta investigación radica en comprender cómo las operaciones multidominio implementadas en el conflicto entre Rusia y Ucrania han incidido en la doctrina de operaciones de información en las FFAA de Ecuador. La cuestión fundamental es si las experiencias y estrategias observadas en el conflicto ruso-ucraniano podrían influir en la forma en que Ecuador concibe y aplica las operaciones de información dentro de su contexto militar y de seguridad.

Las FFAA de Ecuador enfrentan la creciente necesidad de adaptarse a las transformaciones en la naturaleza del conflicto y la seguridad internacional. La interconexión de los dominios y la creciente importancia de las operaciones de información plantean desafíos y oportunidades para la formulación de estrategias militares y políticas efectivas. En este sentido, el conflicto entre Rusia y Ucrania proporciona un caso de estudio relevante para evaluar cómo la aplicación coordinada de operaciones multidominio enfocadas en los sistemas de información puede impactar la forma en que las FFAA de Ecuador abordan su doctrina y prácticas de operaciones de información en todos sus niveles.

Formulación del problema de investigación

¿Cómo han influido las estrategias y ejecución de las operaciones multidominio implementadas en el conflicto entre Rusia y Ucrania en la evolución y adaptación de la doctrina de operaciones de información en las Fuerzas Armadas de Ecuador?

Subproblemas o preguntas de investigación

¿Cuál es la naturaleza y el alcance de la aplicación de las operaciones multidominio en el conflicto entre Rusia y Ucrania, específicamente en el ámbito de las operaciones de información, y cómo han sido empleadas de manera coordinada para lograr objetivos estratégicos, operacionales y tácticos?

¿Cómo ha influido la implementación de las operaciones multidominio en el conflicto entre Rusia y Ucrania en la doctrina de operaciones de información en otros países, incluyendo Ecuador, y cuáles son los principales cambios y adaptaciones que se han observado en estas doctrinas en respuesta a las nuevas dinámicas multidominio?

¿Qué propuestas de solución pueden derivarse de las lecciones aprendidas de la guerra de Rusia Ucrania y la implementación de las operaciones multidominio en la doctrina militar ecuatoriana, para mejorar las capacidades de las Fuerzas Armadas ecuatorianas en operaciones de información y fortalecer su capacidad de respuesta ante desafíos multidominio en el entorno actual de seguridad internacional?

Antecedentes

El término operaciones multidominio se utilizó por primera vez en el Ejército de los Estados Unidos en 2018 como un concepto doctrinal nacional. El término se utilizó principalmente para optimizar la potencia de combate terrestre en los niveles operativo y táctico. El concepto de operaciones multidominio se basa en la doctrina de la "Batalla aire-tierra" del Ejército de los EE. UU. de la década de 1980, que se definió como una respuesta a la amenaza planteada por el ejército soviético en el teatro europeo. En cualquier caso, el desafío para el Ejército de los EE. UU. seguía siendo el de mando y control de las fuerzas para derrotar a un enemigo de la escala del ejército soviético al integrarse en la lucha conjunta en los dominios tradicionales de maniobras físicas de aire y tierra.

El concepto de batalla multidominio se estableció como un sucesor de "Batalla aire-tierra". Para 2018, "batalla" se reemplazó por "dominio", ya que esto estaba más en línea con la forma en que el Ejército imaginó la guerra conjunta. Al utilizar toda la potencia de fuego, el ejército de los EE. UU. podría recuperar la superioridad en un mundo cada vez más complejo. En otras palabras, aunque el Ejército de los EE. UU. eligió un término diferente para la batalla en múltiples dominios, la idea siguió siendo la misma que la de las operaciones en múltiples dominios.

En la actualidad las operaciones multidominio se enfrenta a la amenaza de la última tecnología comercial y aprovecha la misma, así como la tecnología más avanzada, para mejorar el mando y control de las fuerzas. Esta nueva amenaza está en el corazón del nuevo Memorando de Entendimiento entre el Ejército de los EE. UU. y la Fuerza Aérea, desarrollado bajo el nombre *Combined Joint All-Domain* mando y control. Para la Fuerza Aérea de los EE. UU., abordar los desafíos de los dominios múltiples significa concebir que las operaciones militares se llevarán a cabo a través de los mejores sistemas de mando, control, comunicaciones, inteligencia, vigilancia y reconocimiento, es decir, bajo la etiqueta de mando y control multidominio.

Fuera del ejército de los EE. UU., específicamente en la OTAN, el término operaciones multidominio es más genérico y significa diferentes cosas para diferentes naciones. También hay conceptos relacionados, como la nube de combate multidominio, que intenta crear una conexión entre las plataformas tripuladas y no tripuladas y el soporte de inteligencia artificial. Independientemente de cómo se use el término operaciones multidominio en la OTAN o en los EE. UU. este concepto corresponde a una concepción estrictamente militar.

La investigación sobre "Las operaciones multidominio en la guerra Rusia-Ucrania y su incidencia en la doctrina de operaciones de información" surge en el contexto del conflicto que comenzó en 2014 cuando Rusia anexó la península de Crimea y apoyó a los separatistas en el este de Ucrania. El conflicto ha sido descrito como una guerra híbrida, ya que ha involucrado

una combinación de operaciones militares, políticas, económicas y de información (Dmitriev, 2016).

En este contexto, la investigación se centra en el papel de las operaciones multidominio en la guerra y cómo han afectado a la doctrina de operaciones de información en el campo militar. La guerra Rusia-Ucrania ha sido un ejemplo destacado de cómo las operaciones multidominio pueden ser utilizadas en un conflicto moderno para lograr objetivos estratégicos (Hunt, 2019).

Por ejemplo, Rusia ha utilizado una combinación de operaciones cibernéticas, operaciones de información y operaciones militares para lograr sus objetivos en Ucrania. La propaganda y la desinformación han sido una herramienta clave en el arsenal de Rusia, con el objetivo de influir en la opinión pública y crear desunión en Ucrania (Voronkov, 2017). Además, Rusia ha utilizado la superioridad aérea y naval para apoyar a sus fuerzas terrestres en Ucrania, mientras que también ha utilizado la ciberdefensa para proteger sus sistemas y redes (Bloomberg, 2015).

La investigación busca analizar cómo la experiencia de la guerra Rusia-Ucrania ha afectado a la doctrina de operaciones de información en otros países, incluyendo Ecuador. La integración de las operaciones multidominio y las operaciones de información en la estrategia militar puede ser crucial para lograr objetivos estratégicos y tácticos en un conflicto moderno (Oliver, 2018).

Las diferentes interpretaciones y aplicaciones del término operaciones multidominio son una continuación de una idea tan antigua como Sun Tzu que dice ganar la pelea antes de que comience (Tzu, 2015). Esta es la razón por la que es imprescindible monitorear y contrarrestar la tecnología utilizada por el enemigo.

Dicho esto, el dominio y la mejora de la ciencia en la guerra moderna, en particular la tecnología de la información, no debe ocurrir a expensas del arte de mando y control. Independientemente de lo que la tecnología haga por las fuerzas militares, este nuevo tipo de

operaciones o dicho de mejor forma de plantear las operaciones militares aprovechando los recursos tecnológicos, es manifiesta recurrentemente en los conflictos modernos como el de Rusia y Ucrania, en el cual se ha podido observar la utilización efectiva de estas operaciones en las dos partes.

Es así que muchos ejércitos del mundo han empezado ya a desarrollar una doctrina específica para aplicar este tipo de operaciones, así inicialmente el ejército de Estados Unidos ya cuenta con el desarrollo doctrinario respectivo (Perkins, 2018). De igual manera los ejércitos de los países miembros de la OTAN como Alemania y España entre otros, tienen avances significativos en la concepción y la doctrina correspondiente de estas operaciones (Ministerio de Defensa de España, 2020). Lo que traduce el interés global por la concepción de la idea y la aplicación efectiva de estas operaciones en la guerra moderna.

En el Ecuador aún no existen estudios específicos al respecto, en el marco de la investigación militar existe una aproximación a las operaciones multidominio por parte de la Fuerza Aérea denominado: En camino al multidominio. Un análisis transdisciplinario en complejidad (Bolaños, Jiménez, & Noboa, 2022) ; cabe destacar que dentro del proceso de transformación de capacidades (Comando Conjunto de Fuerzas Armadas, 2021) y las acciones encaminadas a la investigación para mejorar las mismas, como el planteado por este trabajo, se hace énfasis en la necesidad de una actualización de la doctrina existente.

Justificación

La investigación sobre "Las operaciones multidominio en la guerra Rusia-Ucrania y su incidencia en la doctrina de operaciones de información" es de vital importancia en el contexto actual de la seguridad y la defensa. La guerra en Ucrania ha sido considerada como un ejemplo de guerra híbrida, que involucra una combinación de operaciones militares, políticas, económicas y de información. Esta combinación de elementos puede ser utilizada para lograr objetivos estratégicos y tácticos en un conflicto moderno.

El objetivo de esta investigación es analizar cómo las operaciones multidominio, en particular las operaciones de información, han sido utilizadas en la guerra Rusia-Ucrania y cómo han influido la doctrina de operaciones de información en otros países, incluyendo Ecuador. La integración de las operaciones multidominio en especial las operaciones de información en la estrategia militar puede ser crucial para lograr objetivos en un conflicto moderno y para el desarrollo de capacidades de operaciones de información en las Fuerzas Armadas ecuatorianas.

La importancia de este estudio radica en la necesidad de adaptarse a las nuevas formas de conflicto y amenazas a la seguridad, donde las operaciones de información juegan un papel fundamental en la construcción de la opinión pública, la comunicación social, los sistemas de guerra electrónica, inteligencia y ciberdefensa enfocados en la influencia en los resultados de una guerra. La guerra en Ucrania ha demostrado que la propaganda y la desinformación pueden ser herramientas poderosas en el arsenal de un país en conflicto, y que la protección de la información y la capacidad de contrarrestar la desinformación son habilidades críticas en el campo militar.

Por lo tanto, el concepto de las operaciones multidominio aborda tanto la competencia antes, durante y después de la guerra, como el conflicto armado entre Rusia y Ucrania, en donde las operaciones multidominio representa un cambio dramático en el enfoque del Ejército de las operaciones de contrainsurgencia (Barro, 2022) o las operaciones basadas en la tecnología como las naves no tripuladas (DW, 2022). Debido al amplio alcance de las operaciones multidominio, la variedad de actividades de debate, diálogo y desarrollo de fuerzas toca todos los aspectos del Ejército.

Es por ello que la investigación de las operaciones multidominio y su impacto en la doctrina de operaciones de información es esencial para el desarrollo de capacidades de operaciones de información en las Fuerzas Armadas ecuatorianas. Esto permitirá que el Ecuador esté mejor preparado para enfrentar los desafíos y amenazas actuales en el campo

militar y que pueda desarrollar estrategias más efectivas para lograr objetivos estratégicos, operacionales y tácticos, que facilite al mando y control en todos los niveles a mejores tomas de decisión.

Objetivos

Objetivo General

Analizar la incidencia de las operaciones multidominio en el ámbito de las operaciones de información durante el conflicto entre Rusia y Ucrania y su impacto en la doctrina de operaciones de información en Ecuador.

Objetivos Específicos

- Estudiar la aplicación de las operaciones multidominio en el conflicto entre Rusia y Ucrania, en particular en el ámbito de las operaciones de información.
- Analizar la incidencia de las operaciones multidominio en la doctrina de operaciones de información en otros países, incluyendo Ecuador.
- Desarrollar una propuesta de solución para mejorar las capacidades de las Fuerzas Armadas ecuatorianas en operaciones de información a través de la aplicación de los aprendizajes obtenidos de la guerra Rusia-Ucrania y la implementación de las operaciones multidominio en la doctrina militar ecuatoriana.

Capítulo II

Marco de Referencia

Estado del arte

En el ámbito de la seguridad y la defensa, las operaciones multidominio han surgido como una respuesta a los desafíos cambiantes en el campo de batalla moderno. La evolución de la tecnología y la interconexión de los dominios terrestre, marítimo, aéreo, ciberespacial y espacial han impulsado la necesidad de una coordinación efectiva entre estos ámbitos. Las operaciones multidominio buscan maximizar la sinergia entre los distintos dominios para lograr efectos integrados y obtener ventajas estratégicas.

La perspectiva de la guerra futura y los caminos a seguir determinados ya en el estudio del ejército de Estados Unidos denominado “Preparándonos para combatir hoy. Las Operaciones Multidominio y el Manual de Campaña 3-0” enfatiza la importancia de las operaciones multidominio (Perkins, 2018), como una respuesta a los desafíos contemporáneos de seguridad. Se destacan los esfuerzos de diversas naciones para integrar y coordinar sus capacidades en múltiples dominios, reconociendo la necesidad de una sinergia efectiva entre terrestre, marítimo, aéreo, ciberespacio y espacio exterior.

En este campo estudios como “The U.S. Army in Multi-Domain Operations 2028”, también determinan la importancia del desarrollo tecnológico y de su aprovechamiento en la guerra futura, (U.S. Army, 2021). En este aspecto, se ha explorado cómo las operaciones multidominio permiten la generación de efectos integrados en el campo de batalla moderno. La conectividad y la interoperabilidad entre diferentes dominios se consideran fundamentales para lograr la superioridad en situaciones conflictivas.

En este contexto, el ciberespacio ha emergido como un dominio crítico en las operaciones multidominio. Los ciberataques y la guerra de la información habían sido utilizados

para desestabilizar a los adversarios y socavar sus capacidades (González, 2017). La importancia del ciberespacio y la información en el ámbito de la seguridad también ha experimentado un aumento significativo. La creciente dependencia de las redes digitales y la comunicación electrónica ha llevado a la consideración del ciberespacio como un dominio crítico en sí mismo. La guerra de la información, que implica la manipulación de la percepción pública y la difusión de desinformación, se ha convertido en una herramienta poderosa utilizada por actores estatales y no estatales.

La doctrina de operaciones de información se ha vuelto fundamental en este entorno. Las fuerzas armadas y las organizaciones de seguridad reconocen la necesidad de controlar y gestionar la información para influir en la percepción pública y alcanzar sus objetivos estratégicos (Comando Conjunto de Fuerzas Armadas, 2021). Esto va más allá de las operaciones de combate tradicionales y abarca la gestión de la narrativa, la contrarrestación de la desinformación y la protección de la infraestructura de información crítica.

Diferentes estudios a nivel local desarrollados para la planificación del desarrollo de capacidades futuras de Fuerzas Armadas (Comando Conjunto de Fuerzas Armadas, 2021) se han enfocado ya en la importancia de la doctrina de operaciones de información en el entorno de seguridad contemporáneo (Gniesco, 2019). Es así que entran ya en el análisis, las estrategias de comunicación, gestión de la información y contrarrestación de la desinformación como componentes esenciales de las operaciones militares y de seguridad.

Un evento de importancia global como la guerra en Ucrania han subrayado cómo las operaciones multidominio y las estrategias de información podían influir en el curso y el resultado de los conflictos (Martínez, 2022). Se destacan las tácticas utilizadas por actores estatales y no estatales para lograr sus objetivos a través de la manipulación de la información y la narrativa.

En este ámbito del desarrollo de capacidades necesarias en la guerra moderna, las Fuerzas Armadas de Ecuador y otras organizaciones similares enfrentan el desafío de adaptar

su doctrina y estrategias a esta nueva realidad multidominio. El estudio de las experiencias en conflictos como el de Rusia y Ucrania proporciona datos valiosos sobre cómo integrar operaciones multidominio y operaciones de información en sus prácticas y políticas.

El estado del arte de esta investigación refleja un enfoque creciente en las operaciones multidominio y la guerra de la información en el ámbito de la seguridad y la defensa. La interconexión de los dominios, junto con la necesidad de controlar la información, ha impulsado la evolución de las estrategias y doctrinas en este campo. La investigación futura puede aprovechar las lecciones aprendidas de conflictos como el de Rusia y Ucrania para informar y mejorar las prácticas en organizaciones militares y de seguridad en todo el mundo.

Marco teórico

La fundamentación teórica de la investigación "Las operaciones multidominio en la guerra Rusia-Ucrania y su incidencia en la doctrina de operaciones de información" se basa en varias teorías y enfoques que explican los conceptos claves que se abordan en la investigación. A continuación, presentamos algunas de las teorías que sustentan el desarrollo de las capacidades militares y la importancia de las operaciones multidominio y de información.

En primer lugar, se encuentra la teoría del Realismo, que es una corriente de pensamiento que sostiene que los estados buscan maximizar su poder y seguridad en un sistema internacional anárquico, en el que la competencia y el conflicto son inevitables. El Realismo defiende que la guerra es una herramienta legítima de la política internacional y que la fuerza militar es una forma eficaz de conseguir los objetivos de seguridad nacional (Blinder, 2021). En este sentido, las capacidades militares son esenciales para el poder y la influencia de un Estado, y su desarrollo y mantenimiento son una prioridad para la defensa de sus intereses.

Por otro lado, el enfoque liberal sostiene que el Estado debe actuar en base a valores democráticos y de derechos humanos, y que la cooperación y la interdependencia son fundamentales para la estabilidad y la seguridad internacional. En este sentido, las

capacidades militares deben estar enfocadas no solo en la defensa del territorio y la soberanía, sino también en la promoción de la paz y la seguridad a nivel global. Las operaciones multidominio y de información son herramientas importantes para el logro de estos objetivos, ya que permiten la coordinación y el trabajo conjunto de las diferentes ramas de las fuerzas armadas y de otros actores civiles.

La teoría de la guerra de redes destaca la importancia de la interconexión y la interoperabilidad de las fuerzas militares para el éxito en el campo de batalla. Según esta teoría, la integración de las diferentes unidades militares y la capacidad de compartir información en tiempo real son esenciales para la coordinación y la toma de decisiones efectivas. Como señala Arquilla y Ronfeldt (2001), "Las redes de unidades militares interconectadas a través de los sistemas de información y comunicaciones forman la base para la guerra de redes. La clave para la victoria es lograr una mayor integración de las diferentes unidades de la red y una mayor capacidad para compartir información en tiempo real" (p. 5).

La teoría de la información como poder sostiene que la capacidad de obtener, procesar y difundir información es clave para el éxito en cualquier tipo de operación militar o estratégica. Según esta teoría, el control de la información puede ser tan importante como el control del territorio o los recursos naturales. Como señala Valeriano y Maness (2015), "La información puede ser utilizada para influir en el comportamiento de los adversarios, socavar su capacidad de decisión y controlar el campo de batalla. Las guerras modernas son cada vez más una cuestión de información" (p. 2).

Como señala Gerasimov (2013), "La guerra híbrida es un método de lucha que combina acciones militares y no militares. El objetivo es debilitar la voluntad del adversario para resistir y lograr los objetivos políticos deseados" (p. 3).

Estas teorías proporcionan un marco teórico para entender la importancia de las operaciones multidominio y de información en el contexto de la guerra Rusia-Ucrania y su impacto en la doctrina militar ecuatoriana. La interconexión y la interoperabilidad de las fuerzas

militares, la capacidad de obtener y procesar información en tiempo real y la combinación de diferentes formas de guerra y tácticas son elementos clave para el éxito en el campo de batalla en la era moderna.

Operaciones multidominio en la guerra Rusia-Ucrania

Las Operaciones de Dominio Múltiple son el empleo de armas combinadas de las capacidades conjuntas y del Ejército para crear y explotar ventajas relativas que logran objetivos, derrotan a las fuerzas enemigas y consolidan ganancias en nombre de comandantes de fuerzas conjuntas (Perkins, 2018). El empleo de las capacidades conjuntas y del Ejército hace uso de todo el poder de combate disponible de cada dominio para cumplir las misiones al menor costo. Las operaciones multidominio son la contribución del Ejército a las campañas conjuntas, que abarcan la continuidad de la competencia.

Por debajo del umbral del conflicto armado, las operaciones multidominios son la forma en que las fuerzas del Ejército acumulan ventajas y demuestran preparación para el conflicto, disuadiendo a los adversarios mientras aseguran a sus fuerzas.

Durante el conflicto, son la forma en que las fuerzas del Ejército se acercan al enemigo y lo destruyen, derrotan las formaciones enemigas, toman terreno crítico y controlan las poblaciones y los recursos para lograr resultados sostenibles.

El Ejército de Estados Unidos desarrolló operaciones multidominio en respuesta a la Estrategia de Defensa Nacional de 2018 (Perkins, 2018), que cambió el enfoque anterior de la seguridad nacional de EE. UU. de contrarrestar a los extremistas violentos en todo el mundo a confrontar a los poderes revisionistas. —principalmente Rusia y China— que se dice que “quieren dar forma a un mundo consistente con su modelo autoritario, ganando autoridad de veto sobre las decisiones económicas, diplomáticas y de seguridad de otras naciones”.

Según *The U.S. Army in MultiDomain Operations 2028* (U.S. Army, 2021): China y Rusia explotan las condiciones del entorno operativo para lograr sus objetivos sin recurrir a un

conflicto armado al fracturar las alianzas, asociaciones y resolución de EE. UU. Intentan crear un enfrentamiento a través de la integración de acciones diplomáticas y económicas, guerra no convencional y de información (redes sociales, narrativas falsas, ataques cibernéticos) y el empleo real o amenazado de fuerzas convencionales.

Al crear inestabilidad dentro de los países y alianzas, China y Rusia crean una separación política que resulta en una ambigüedad estratégica que reduce la velocidad del reconocimiento amistoso, la decisión y la reacción. A través de estas acciones competitivas, China y Rusia creen que pueden lograr objetivos por debajo del umbral del conflicto armado. Cómo pretende competir el ejército, podría decirse que la competencia es un aspecto crítico de las operaciones multidominio porque, si se lleva a cabo con éxito, se podría evitar el conflicto. Según el documento del Jefe de Estado Mayor del Ejército de EE. UU. (U.S. Army, 2021), El ejército en competencia militar, compite de tres maneras:

Figura 1

Competencia militar



Nota. Adaptado de (U.S. Army, 2021)

La *competencia narrativa* se refleja en el auge y la caída de la reputación de un país en función de las percepciones generales de su fortaleza, fiabilidad y determinación. El Ejército contribuye siendo una fuerza letal, competente y creíble y siendo reconocido como tal por aliados, socios y adversarios.

La *competencia directa* abarca toda la gama de actividades competitivas, desde la competencia de menor intensidad por debajo del conflicto armado hasta el conflicto estatal general. En competencia directa, el objetivo es crear influencia para los Estados Unidos y negar influencia a los adversarios.

La competencia indirecta en la cual el objetivo es obtener una ventaja (o negársela al adversario). Este objetivo contrasta con el concepto más contundente de apalancamiento en la competencia directa. El Ejército contribuye al ofrecer una variedad de opciones creíbles para los formuladores de políticas.

Algunas de estas opciones incluyen ejercicios en el extranjero, cooperación en materia de seguridad, asistencia de las fuerzas de seguridad, intercambios entre militares, bases en el extranjero, intercambio de inteligencia y socorro en casos de desastre. En este sentido, la competencia indirecta no es un concepto operativo “nuevo”, sino una “redesignación” de actividades tradicionales que no son conflictos armados. El liderazgo del Ejército cree que, si el Ejército y los demás Servicios prevalecen en estas “competencias”, se deben lograr los objetivos de seguridad nacional (Perkins, 2018).

La idea central del Ejército es prevalecer compitiendo con éxito en todos los dominios excepto en el conflicto, disuadiendo así a un enemigo potencial. Si la disuasión falla, el Ejército y las Fuerzas Conjuntas deben:

Penetrar los sistemas enemigos de negación de área y anti acceso (A2/AD) (sistemas de ataque de precisión de largo alcance en capas e integrados, capacidades litorales antibuque, defensas aéreas y sistemas de ataque de largo alcance). sistemas de artillería y cohetes) para permitir la maniobra estratégica y operativa de las fuerzas estadounidenses. Manual básico de defensa: operaciones multidominio del ejército.

Desintegrar, interrumpir, degradar o destruir los sistemas A2/AD para permitir la maniobra operativa y táctica de las fuerzas estadounidenses.

Explotar la libertad de maniobra resultante para lograr objetivos operativos y estratégicos al derrotar a las fuerzas enemigas en todos los dominios.

Re competir: consolidar las ganancias en todos los dominios y forzar un regreso a la competencia en términos favorables para las propias fuerzas y sus aliados.

El ciberespacio y la ciberguerra

Para comprender a la ciber guerra es necesario concebir inicialmente al ciberespacio, el cual es el espacio dinámico y virtual creado por la informática y las computadoras. En otras

palabras, el ciberespacio es la red electrónica de consumo, de dispositivos de acceso digital y redes de comunicaciones que interconectan el mundo.

La guerra cibernética generalmente se define como un ataque cibernético o una serie de ataques dirigidos a un país utilizando al ciberespacio como medio. Tiene el potencial de causar estragos en la infraestructura gubernamental y civil e interrumpir los sistemas críticos, lo que resulta en daños al estado e incluso la pérdida de vidas.

Sin embargo, existe un debate entre los expertos en seguridad cibernética sobre qué tipo de actividad constituye una guerra cibernética. El Departamento de Defensa de EE. UU. (DoD) reconoce la amenaza a la seguridad nacional que representa el uso malintencionado de Internet, pero no proporciona una definición más clara de guerra cibernética (González, 2017). Algunos consideran que la guerra cibernética es un ataque cibernético que puede provocar la muerte.

La guerra cibernética generalmente involucra a un estado-nación que perpetra ataques cibernéticos contra otro, pero en algunos casos, los ataques son llevados a cabo por organizaciones terroristas o actores no estatales que buscan promover el objetivo de una nación hostil. Hay varios ejemplos de supuesta guerra cibernética en la historia reciente, pero no existe una definición universal y formal de cómo un ataque cibernético puede constituir un acto de guerra.

Espionaje. Se refiere a monitorear otros países para robar secretos. En la guerra cibernética, esto puede implicar el uso de botnets o ataques de phishing selectivo para comprometer sistemas informáticos confidenciales antes de filtrar información confidencial .

Sabotaje. Las organizaciones gubernamentales deben determinar la información confidencial y los riesgos si se ve comprometida. Los gobiernos hostiles o los terroristas pueden robar información, destruirla o aprovechar amenazas internas , como empleados insatisfechos o descuidados, o empleados gubernamentales afiliados al país atacante.

Ataques de denegación de servicio (DoS). Este tipo de ataques evitan que los usuarios legítimos accedan a un sitio web al inundarlo con solicitudes falsas y obligar al sitio web a manejar estas solicitudes. Este tipo de ataque se puede utilizar para interrumpir operaciones y sistemas críticos y bloquear el acceso a sitios web confidenciales por parte de civiles, personal militar y de seguridad u organismos de investigación.

Ataques a redes de energía eléctrica. Atacar la red eléctrica permite a los atacantes deshabilitar sistemas críticos, interrumpir la infraestructura y potencialmente provocar daños corporales. Los ataques a la red eléctrica también pueden interrumpir las comunicaciones y dejar inutilizables servicios tales como mensajes de texto y comunicaciones.

Ataques de propaganda. Intentos de controlar las mentes y los pensamientos de las personas que viven o luchan por un país objetivo. La propaganda se puede utilizar para exponer verdades vergonzosas, difundir mentiras para hacer que la gente pierda la confianza en su país o ponerse del lado de sus enemigos.

Interrupción Económica. La mayoría de los sistemas económicos modernos funcionan con computadoras. Los atacantes pueden apuntar a las redes informáticas de los establecimientos económicos, como los mercados de valores, los sistemas de pago y los bancos, para robar dinero o impedir que las personas accedan a los fondos que necesitan.

Ataques sorpresa. Estos son el equivalente cibernético de ataques como Pearl Harbor y el 11 de septiembre. El punto es llevar a cabo un ataque masivo que el enemigo no espera, permitiendo al atacante debilitar sus defensas. Esto se puede hacer para preparar el terreno para un ataque físico en el contexto de la guerra híbrida.

El multidominio desde la perspectiva de la prevención y resolución de conflictos

Entender al multidominio desde esta perspectiva no difiere con el propósito de las operaciones multidominio utilizadas en la guerra, ya que las mismas en definitiva pretenden terminar con un conflicto de una forma eficiente y eficaz, utilizando y coordinando todos los medios disponibles. En este sentido si se puede utilizar la concepción del multidominio para evitar el conflicto con acciones que establezcan el control de diferentes dominios antes del empleo de la Fuerza, ejemplificaría un escenario óptimo del aprovechamiento de recursos en los diferentes dominios y escenarios.

En este sentido se puede interpretar la utilidad del enfoque del multidominio, y no a la aplicación de la fuerza para explotarlos, es decir en la optimización de los mismos para alcanzar la resolución de conflictos, ya sea mediante la prevención o en la creación de condiciones y escenarios que reduzcan al mínimo o de forma total el empleo de la guerra como resolución final.

Evolución de la doctrina militar ecuatoriana

Las Fuerzas armadas ecuatorianas definen a la doctrina como “el conjunto de ideas, conocimientos, teorías y dogmas que, convertidos en norma, inspiran la conducta y normas de acción, como sistema de adaptación y aplicación común” (Comando en Jefe de Educación y Doctrina de las Fuerzas Armadas 2018, 48). En este aspecto la concepción de la doctrina de Fuerzas Armadas inicia con la conformación de sus fuerzas en la época colonial, al plantear la independencia de España, no de la forma formal, pero si en la base de la consolidación de la nacionalidad ecuatoriana en las rebeliones que se dieron en ya en la Real Audiencia de Quito.

Así, ante la necesidad de la conformación de unas Fuerzas Armadas propias el aporte de los ejércitos libertarios y la llegada de misiones extranjeras determinaron la vía de desarrollo doctrinario de las Fuerzas Armadas.

En 1899 llegó una misión del ejército chileno que aportó en gran medida a la profesionalización del ejército mediante el aporte de doctrina. Para el año de 1922, una misión italiana de expertos en defensa promovieron y supervisaron la Academia de Guerra del Ejército (Ejército Ecuatoriano, 2018), entidad que hasta la actualidad se encarga del desarrollo de la doctrina militar, este hito ha sido el más significativo para la conformación de la doctrina de las Fuerzas militares ecuatorianas, ya que se dedicó a llenar los vacíos de las necesidades doctrinarias e investigar por doctrina compatible para ajustar a las necesidades del ejército ecuatoriano que poco a poco fue consolidando la experiencia y generando doctrina propia. Cabe destacar que la doctrina compartida tenía una raíz común en América Latina, poseía aun bases europeas y norteamericanas fundamentalmente.

En el año 1956 otro aporte a la doctrina ecuatoriana, brindaron docentes del ejército de Chile quienes compartieron conocimientos en la Academia de Guerra del Ejército ecuatoriano (Ejército Ecuatoriano, 2018). En este período y en consideración a los objetivos comunes, en función de compartir un enemigo común para ambos ejércitos, (el ejército peruano), los conocimientos fluyeron y se adaptaron a la realidad ecuatoriana luego del conflicto con el vecino del sur.

En 1944, tras el conflicto armado con el Perú, se independizaron las ramas de las Fuerzas Armadas del Ecuador: Ejército, Marina y Aviación (Vásquez, 2021). Sin embargo, por el ámbito generalmente terrestre de las incursiones y ataques peruanos se produjo la especialización y desarrollo de la doctrina terrestre que, posteriormente era modificada y adaptada a las otras ramas de Fuerzas Armadas.

Durante la segunda mitad del siglo pasado y con los continuos enfrentamientos ante la amenaza expansionista del Perú el desarrollo doctrinario se especializó fundamentalmente considerando las condiciones fronterizas que tenía la frontera sur, y se fortaleció en base a la mala experiencia del conflicto del 41 en donde el ejército peruano le arrebató al Ecuador cerca de la mitad de su territorio en la Amazonía.

En este escenario de conflictos y amenazas a la soberanía el ámbito doctrinario amplió su alcance a la política exterior ecuatoriana y a la especialización de la doctrina que sustenta la misma desde el campo de la defensa, por otro lado los convenios de cooperación, capacitación y asistencia por parte de Estados Unidos (Vásquez, 2021), aportó con doctrina fresca, en el ámbito geopolítico global, y con especialización en el campo de la inteligencia y contrainteligencia que era empleada adaptativamente en la defensa contra el Perú y el apareamiento temprano de grupos armados vinculados a movimientos revolucionarios como tendencia en América Latina, concibiendo de forma temprana a otro tipo de amenazas no estatales.

A partir de la especialización de las Academias de Guerra, el desarrollo en el ámbito educativo y el desarrollo de centros de formación especializados así como de la Universidad de Fuerzas Armadas (ESPE), han constituido y lo siguen haciendo los mayores generadores de innovación doctrinaria en función de las necesidades de actualización y modernización de diferentes procesos que desde el fin de la guerra con el Perú han procurado desarrollar una doctrina basada en las capacidades militares y a su vez ésta en los desafíos que suponen las amenazas que han ido evolucionando a no convencionales, para lo cual la necesidad de optimización de las fuerzas, de la especialización y el desarrollo de capacidades (Comando Conjunto de Fuerzas Armadas, 2019) fundamentalmente en el ámbito interno han ido adaptándose a los cambios constitucionales que determina en la actualidad la constitución del Estado y la concepción de la seguridad integral (Ecuador, 2008). En atención a estas demandas, los procesos de desarrollo y transformación de capacidades militares, se encuentran en la actualidad dotando de doctrina actual, en base a la concepción de la guerra actual y de sus necesidades, así como de los distintos escenarios y tipos de operaciones que se generan por influencia tecnológica y de desarrollo de la industria de la defensa.

Proceso de desarrollo y transformación de las capacidades militares

Los procesos de desarrollo y transformación de las capacidades militares proporcionan un fundamento más racional para la toma de decisiones sobre la modernización y optimización de los recursos y estado de las capacidades reales, a la vez ofrece soluciones integrales, para afrontar con éxito los actuales y potenciales escenarios de la seguridad y la defensa, así como la manera más adecuada para enfrentar las amenazas.

A más de las amenazas tradicionales como los conflictos interestatales, se han identificado nuevas amenazas y factores de riesgo. Asimismo, la constante amenaza ciberespacial, y el contexto de amenazas transnacionales no estatales, identificadas en la planificación prospectiva, han determinado una necesidad de modernización de Fuerzas Armadas sobre la base de la planificación por capacidades en un proceso lógico secuencial, inicialmente en la valoración de las capacidades existentes, para luego permitir el desarrollo de capacidades y posteriormente pasar a la transformación de las mismas en función del acortamiento o eliminación de las brechas de capacidad, proceso que se encuentra en ejecución actualmente en las Fuerzas Armadas ecuatorianas.

En ese contexto es necesario redefinir las capacidades militares necesarias para enfrentar las exigencias que plantean los nuevos escenarios, la Constitución del Estado, el Plan Nacional de Desarrollo, la ley de Seguridad Pública y del Estado y las reformas del Estado; la Agenda Política de la Defensa, lo cual significa revisar y actualizar la estructura, la doctrina, las concepciones de seguridad y defensa, el entrenamiento, el equipamiento, los modelos de gestión operacional, institucional y administrativo.

Al interior de la institución se analiza permanentemente la modernización de la Fuerza acorde a los nuevos escenarios, con una organización dinámica, multipropósito y flexible, que facilite cumplir las misiones mediante la integración sinérgica y coordinación de los organismos de planificación, preparación, empleo y apoyo de manera efectiva.

Se evidencia una organización con modelos de concentración regional, unidades orgánicamente completas, de cuadros profesionales, interoperables, flexibles con capacidad de despliegue rápido y empleo conjunto en cualquier parte del territorio nacional, debidamente dotadas y tecnológicamente bien equipadas, en todos sus sistemas operativos, y en condiciones de enfrentar los nuevos desafíos tales como: los problemas derivados de la inseguridad, la afectación psicosocial, el deterioro al ambiente y la constante amenaza ciberespacial.

A diferencia del planeamiento basado en hipótesis de conflicto, que se centraba en la amenaza militar, el nuevo enfoque se centra prioritariamente en adaptarse a la incertidumbre de las amenazas y varios factores de riesgo, disponiendo de capacidades que nos permitan reaccionar ante los supuestos no previstos e intervenir en el contexto estratégico para ajustarlo, sin descuidar la concepción de planes y estrategias de contingencia para atender riesgos menos previsibles.

Escenarios prospectivos de las amenazas a la defensa y seguridad el Estado ecuatoriano

La planificación de escenarios se ha convertido en una herramienta importante para que las Fuerzas Armadas consideren futuros posibles, cómo podrían actuar en esos futuros, cuáles son las tendencias e incertidumbres clave y qué cambios podrían implementarse para hacer que su accionar sea efectivo en función de sus objetivos institucionales, el mandato constitucional y la responsabilidad frente a la defensa y seguridad del Estado ecuatoriano. La intención de la planificación de escenarios es ampliar y desafiar las perspectivas de quienes toman decisiones en la planificación de la defensa y en el desarrollo del Estado.

Los escenarios son parte de los procesos de planificación de la capacidad militar de las Fuerzas armadas ecuatorianas, frente a futuros posibles. Los escenarios de la Defensa para el año 2033 han destacado impulsores nuevos y acelerados que indican un entorno estratégico

cambiante y con retos propios de la globalización y el desarrollo de amenazas no convencionales. En este sentido, el uso de procesos efectivos para prepararse para nuevos desafíos es un factor crítico, que es asumido en la planificación. Los espacios de escenarios factibles son una herramienta base, que puede ser fundamental en la planificación de escenarios militares. Sin embargo, para ser eficaz, debe evolucionar aún más para abarcar el potencial de amenazas no convencionales, incluida la primacía emergente de la guerra de información o las amenazas híbridas en conflictos futuros.

Si bien la probabilidad de los conflictos interestatales es baja, no se descarta la posibilidad de ocurrencia, de ahí que la razón de ser de las Fuerzas Armadas es la defensa de la integridad territorial, de la soberanía, del patrimonio, de la infraestructura crítica y de los intereses del Ecuador, y constituyen el sustento de su existencia, como una institución permanente del Estado.

No obstante persisten, aunque en menor grado, factores de riesgo que afectan el liderazgo gubernamental y el poder del Estado, a través de crisis internas, generadas por aspectos: políticos, ideológicos, económicos y sociales, que pueden desembocar en situaciones de disturbios interiores o tensiones internas que se producen cuando se han rebasado los procedimientos democráticos y la capacidad de gestión de las crisis de las instituciones, traduciéndose en alteraciones del orden, de la paz y del respeto de los derechos y libertades fundamentales de los ciudadanos, que pueden rápidamente tornarse en una manifestación violenta, en un disturbio o en una rebelión, que puede terminar en una lucha armada interna.

A lo que se suma la inseguridad ciudadana, provocada por el incremento de las acciones delincuenciales, en todos los estratos sociales; la delincuencia se ha sofisticado adoptando nuevas y complejas formas a nivel transnacional, cometiendo delitos cada vez más violentos, que transgreden derechos inherentes al ser humano, como son: la vida, la integridad personal y patrimonio. De igual manera persisten factores de riesgo que presentan nuevos

escenarios en el mar y que demandan nuevas respuestas. Entre ellos destacamos: el tráfico de drogas, armas, precursores químicos, contrabando, tráfico ilícito de personas, transporte de material tóxico y el resurgimiento de la piratería. Cada uno de estos factores de riesgo tiene sus propias características, pero tienen como aspecto común el peligro que representa para la población asentada en las islas y a lo largo del litoral ecuatoriano, realizado por actores que, violando el derecho marítimo y los convenios internacionales, puedan perturbar o impedir la actividad legal en el mar territorial o puedan aprovechar este inmenso espacio, como área libre y sin fronteras, para llevar a cabo actividades delictivas.

El ingreso de actores estatales colombianos y de grupos ilegales armados en territorio ecuatoriano, continúa, debido en gran parte a las derivaciones del conflicto interno colombiano y otros actores ilegales generadores de violencia los cuales son difíciles de identificar y emplean tácticas, técnicas y procedimientos asimétricos, no respetan las normas del derecho internacional de los derechos humanos, ni del derecho internacional humanitario, y se sienten con mayor incidencia en el sector fronterizo ecuatoriano–colombiano.

Otro aspecto fundamental en los escenarios prospectivos lo constituye el desarrollo del crimen transnacional, el fortalecimiento de bandas criminales y el narcotráfico, como factores de incidencia en el ámbito interno, el mismo que repercute en la violencia de internos en las cárceles, la inseguridad ciudadana y el aumento de la delincuencia común.

Estas amenazas y factores de riesgo determinan el empleo permanente del Ejército ecuatoriano en misiones de vigilancia, protección, exploración, control y defensa de las fronteras y del espacio aéreo, asegurando la presencia del Estado, el imperio de la ley y de la autoridad y protegiendo a la comunidad, con prioridad en la zona fronteriza norte y la infraestructura crítica; para lo cual es necesario contar con doctrina y entrenamiento especial para este tipo de misiones (operaciones en selva, de contrainsurgencia y urbanas), mantener la capacidad operativa, con un incremento en inteligencia, vigilancia y reconocimiento; y, la movilidad, incluyendo la acción inmediata e interoperabilidad entre las Unidades.

La guerra híbrida y el multidominio

El término “híbrido” proviene del latín, ya que se usaba en el Imperio Romano para describir a un niño nacido de padres de diferente estatus social (por ejemplo, un ciudadano romano y un esclavo). Más tarde, evolucionó para denotar fenómenos, entidades o acciones de naturaleza combinada que no se “mezclan” mecánicamente, sino que están orgánicamente integrados, cohesivos y coordinados (IEEE, 2018). Tal como lo entiende la OTAN, “las amenazas híbridas combinan medios militares y no militares, así como encubiertos y abiertos, incluida la desinformación, los ataques cibernéticos, la presión económica, el despliegue de grupos armados irregulares y el uso de fuerzas regulares. Se utilizan métodos híbridos para desdibujar las líneas entre la guerra y la paz, y se intenta sembrar dudas en la mente de las poblaciones objetivo” (Organización del Tratado del Atlántico Norte, 2019).

El primer uso académico reconocible de "híbrido" aplicado a la guerra se remonta a 2007, cuando el LTC Frank Hoffman escribió sobre el surgimiento de las guerras híbridas en el contexto de Medio Oriente, es decir, la combinación de herramientas cinéticas y no militares utilizadas por actores como Hezbolá durante la campaña militar de Israel de 2006 (Bartolomé, 2019). Cuando Rusia lanzó su agresión contra Ucrania en 2014 utilizando una variedad de medios no militares o clandestinos encubiertos por extensos esfuerzos de desinformación y acompañados de desmentidos oficiales, la OTAN comenzó a usar "híbrido" como el término para describir lo que parecía un nuevo tipo de guerra en ese momento.

Aunque muchos actores han utilizado herramientas no militares a lo largo de la historia para dividir y derrotar a sus enemigos, la guerra híbrida en el siglo XXI ha adquirido una nueva relevancia (IEEE, 2018). Ha sido elevado para convertirse en el estilo de lucha preferido de las potencias más débiles, revisionistas y revanchistas que están ansiosas por elevar su estatus en la escena mundial pero que no se atreven a desencadenar una confrontación convencional a

gran escala que saben que resultaría en una guerra militar. derrota o una conflagración nuclear mundial.

En su lugar, optan por una combinación de medios militares y no militares para dividir y derrotar a sus adversarios más fuertes sin recurrir a una guerra a gran escala (IEEE, 2018). La guerra híbrida incluye elementos, o "líneas", tales como guerra política, diplomática, económica y financiera, legal (lawfare), así como esfuerzos socioculturales, con infraestructura, inteligencia, y los grupos criminales también están siendo ampliamente utilizados.

Estos pasos iniciales de penetración encubierta son seguidos por el despliegue de operativos militares encubiertos y, si es necesario, por contingentes militares limitados para obligar al adversario a someterse y hacer cumplir la paz bajo los términos del agresor híbrido mediante el despliegue de una "misión de mantenimiento de la paz" (Paz, 2012). La operación híbrida en este formato está respaldada por la amenaza implícita del despliegue nuclear táctico o incluso estratégico, para intimidar a los gobiernos e influir en la opinión pública, con la guerra de información, la desinformación, el engaño y la propaganda sirviendo como la columna vertebral de los esfuerzos híbridos.

Sin embargo, es importante señalar que no todas las combinaciones de medios militares y no militares deben calificarse como esfuerzos híbridos (IEEE, 2018). Las operaciones que tienen un gran sesgo no militar y en las que el agresor híbrido trata de negar su participación y sus objetivos reales merecen el título. De manera similar, los esfuerzos occidentales contemporáneos para responder, como la Doctrina de la "Batalla Multidominio" de EE. UU.

La invasión híbrida de Rusia a Ucrania inicialmente tomó por sorpresa a la comunidad transatlántica, especialmente por su combinación de velocidad, cohesión y coordinación entre los actores militares y no militares involucrados en la operación. Aun así, desde 2014, la OTAN ha podido responder y adaptarse rápidamente a la aplicación moderna de estas viejas formas de guerra a una en la cual el multidominio empieza a ser común en este tipo de conflictos.

En este sentido la concepción de guerra multidominio, también conocida como guerra multidimensional o guerra en varios dominios, se refiere a una estrategia militar en la que se emplean operaciones y acciones en múltiples ámbitos o "dominios" simultáneamente para lograr objetivos estratégicos. Estos dominios pueden incluir el terrestre, el marítimo, el aéreo, el ciberespacio y el espacio exterior. La idea detrás de la guerra multidominio es que los conflictos modernos ya no se limitan a un solo campo de batalla, sino que se extienden a través de múltiples ámbitos físicos y virtuales.

En una guerra multidominio, las fuerzas militares y los actores involucrados no solo se centran en la superioridad en un dominio específico, como tradicionalmente se hacía en guerras convencionales, sino que también se esfuerzan por coordinar y sincronizar operaciones en diferentes dominios para obtener efectos integrados y alcanzar ventajas estratégicas. Por ejemplo, un ataque en el ciberespacio podría ser combinado con operaciones terrestres para desestabilizar la infraestructura enemiga y afectar su capacidad de respuesta.

Esta evolución en la forma en que se conciben y se llevan a cabo las operaciones militares ha surgido como respuesta a la creciente interconexión de tecnologías y la necesidad de abordar desafíos de seguridad modernos que trascienden las fronteras físicas. La guerra multidominio requiere una comprensión profunda de las interacciones entre los distintos dominios y la habilidad de adaptarse rápidamente a situaciones cambiantes y complejas en el campo de batalla.

Operaciones de la Información en el Contexto de la Guerra Multidominio

Las operaciones de la información son un conjunto de actividades planificadas y coordinadas que buscan influir en la percepción, la comprensión y el comportamiento de las audiencias específicas, con el objetivo de lograr objetivos estratégicos y tácticos. Estas operaciones se basan en la gestión de la información y la comunicación, y pueden incluir la difusión de información veraz, la contrarrestación de la desinformación, la manipulación de la

narrativa y la creación de condiciones favorables para el logro de los objetivos militares y políticos.

Las operaciones de la información desempeñan un papel crucial al permitir a los actores militares y políticos influir en la percepción pública, erosionar la moral del enemigo y establecer condiciones que faciliten la consecución de objetivos estratégicos. A continuación, se describe cómo las operaciones de la información interactúan en este contexto:

- **Interconexión entre Dominios.**- En una guerra multidominio, las operaciones de la información no ocurren en un vacío. Están intrínsecamente conectadas con otros dominios como el ciberespacio, el terrestre y el marítimo. Por ejemplo, los ciberataques y la desinformación pueden ser utilizados en combinación para socavar la infraestructura enemiga y minar la confianza en sus capacidades.
- **Complementariedad Estratégica.**- Las operaciones de la información pueden complementar y reforzar las operaciones en otros dominios. Por ejemplo, una campaña de información que resalte el apoyo popular a ciertas acciones militares puede reforzar la credibilidad de esas acciones y aumentar la presión sobre el enemigo.
- **Gestión de la Percepción.**- En un entorno multidominio, la percepción pública es un activo valioso. Las operaciones de información buscan influir en cómo se perciben las acciones y los eventos. Pueden desviar la atención de ciertas actividades, exagerar los logros propios y minimizar los éxitos del enemigo.
- **Manipulación del Espacio de Batalla Informativo.**- La guerra multidominio abarca tanto los campos físicos como virtuales. Las operaciones de la información buscan influir en el espacio de batalla informativo, que incluye la diseminación de noticias, la participación en redes sociales y la creación de narrativas en línea. Esta manipulación puede afectar la moral de las tropas enemigas y socavar la percepción internacional del conflicto.

- Adaptabilidad y Agilidad.- En un entorno multidominio, la situación puede cambiar rápidamente. Las operaciones de la información deben ser ágiles y capaces de adaptarse a las novedades en el campo de batalla. Esto puede incluir la rápida corrección de información falsa, la adaptación de la narrativa a medida que evoluciona el conflicto y la explotación de eventos inesperados.

En el contexto de la guerra multidominio, las operaciones de la información desempeñan un papel fundamental al influir en la percepción, la comprensión y el comportamiento de diversos públicos incluido fuerzas enemigas y amigas. Su interconexión con otros dominios y su capacidad para moldear la narrativa hacen que sean un componente estratégico y táctico esencial para los actores en conflicto.

En el conflicto entre Rusia y Ucrania, se ha observado un claro ejemplo de cómo las operaciones multidominio y de la información se han utilizado en conjunto para lograr objetivos estratégicos, operacionales y tácticos (Battaglino, 2022). Rusia ha empleado operaciones en múltiples dominios para lograr efectos integrados. Por ejemplo, en la anexión de Crimea en 2014 y en la invasión de 2022 (Oropesa, 2022), las operaciones terrestres fueron acompañadas por el uso del ciberespacio para desactivar sistemas de comunicación ucranianos y las operaciones de información para influir en la percepción pública tanto en Ucrania como internacionalmente.

La guerra cibernética y la desinformación han sido elementos centrales en el conflicto. Rusia ha utilizado ciberataques para interrumpir las comunicaciones ucranianas y para socavar la infraestructura tecnológica (Tidy, 2023). Además, ha empleado campañas de desinformación para distorsionar la realidad y crear confusión tanto en el frente interno como en la comunidad internacional.

Las operaciones de la información han sido utilizadas para moldear la narrativa y la percepción del conflicto. Rusia ha difundido información falsa y ha creado versiones

alternativas de los eventos para justificar sus acciones y debilitar la posición de Ucrania en la comunidad internacional (Battaglino, 2022).

La combinación de operaciones multidominio y de la información también ha tenido un impacto psicológico en Ucrania (Tidy, 2023). La interrupción de las comunicaciones y la difusión de información falsa pueden generar incertidumbre y desmoralización en las fuerzas ucranianas y en la población en general.

Las operaciones multidominio y de la información también han sido utilizadas en línea con objetivos políticos más amplios. La manipulación de la información y la narrativa pueden contribuir a la desestabilización del gobierno ucraniano y a la creación de condiciones que favorezcan los intereses rusos.

El conflicto entre Rusia y Ucrania es un caso ilustrativo de cómo las operaciones multidominio y de la información pueden ser empleadas en conjunto para lograr una ventaja estratégica (Tidy, 2023). Las operaciones en múltiples dominios, como el ciberespacio y la información, han sido utilizadas para complementar las acciones en el terreno y para influir en la percepción pública y política tanto en Ucrania como a nivel internacional.

Concepción de operaciones de multidominio en la doctrina militar actual

La Fuerza Aérea Ecuatoriana, en el Plan de Gestión Institucional 2021-2025 y 2021-2033 muestra conceptos clave, donde se identifica la existencia de una conciencia referente a la complejidad del entorno (Bolaños, Jiménez, & Noboa, 2022), y asimismo se puede concebir la necesidad que tiene la institución por la edificación de alianzas estatales estratégicas para enfrentar las amenazas emergentes.

Para el Ejército ecuatoriano existen varias aproximaciones conceptuales en donde se explora el concepto y origen del multidominio y se recomienda la actualización de concepto y en definitiva de la doctrina que pueda sustentar este conocimiento (Revista de la Academia de Guerra del Ejército Ecuatoriano, 2019). Es decir, la doctrina militar ecuatoriana es susceptible

de adoptar el enfoque y la concepción, pero se requiere de medios y estudios que puedan interpretar la aplicabilidad de este enfoque de la guerra moderna.

Implicaciones de las operaciones multidominio en el sistema de defensa y seguridad del Estado

Las operaciones multidominio requerirán un cambio en el entrenamiento y en el desarrollo de las capacidades militares, ya que el Ejército necesitará contar con soldados altamente especializados para todos los entornos que prevé la concepción del multidominio. Para aplicar adecuadamente este enfoque y construir el ejército futuro, es posible que se requiera de una transformación de estructura y elementos que inciden en el ámbito operacional para evolucionar a una nueva forma de lucha, que incluso puede llegar a ser virtual o teledirigida (Comando Conjunto de Fuerzas Armadas, 2021). Esto se debe planificar en la preparación para el desafío de posibles operaciones de combate a gran escala, en tareas conjuntas, o incluso en coordinación regional ante amenazas transnacionales físicas o específicas al ciberespacio.

Junto con esas nuevas estructuras de fuerza y entrenamiento, varias tecnologías nuevas serán necesarias para respaldar a las operaciones multidominio del Ejército. Nuevas capacidades como las capacidades anti acceso y de denegación aérea son cruciales para las operaciones de combate a gran escala, razón por la cual el Ejército deberá innovar o respaldarse en el desarrollo científico de la industria de la defensa o directamente de la Academia como fuente innovadora.

Combinado con capacidades de fuego, el Ejército ha de especializarse en efectos de precisión de largo alcance para operaciones de todos los dominios con recursos tecnológicos dedicados y específicos a las necesidades operacionales (Comando de Educación y Doctrina Militar Terrestre, 2020). Se vislumbra la creación de equipos especializados de trabajo multidominio para proporcionar capacidades contra amenazas híbridas, como información de

inteligencia, guerra electrónica, operaciones cibernéticas y espaciales, y planificación prospectiva.

Las armas combinadas seguirán desempeñando un papel clave en las operaciones multidominio del Ejército, sin embargo, el Ejército necesita modificar la forma en que establece y mantiene los puestos de mando, en función de personal capacitado desde el enfoque del multidominio, lo que requiere además una especialización del mando y control y la diferenciación específica del ámbito operativo presencial y dirigido virtual o físico. Con el empleo especializado de elemento tele tripulados, automatizados o que obedezcan a la programación de la inteligencia artificial.

Marco conceptual

Amenazas a la seguridad del Estado

Las amenazas a la seguridad del estado son eventos, condiciones o situaciones que ponen en riesgo la integridad, la estabilidad y los intereses fundamentales de un país o nación (Comando Conjunto de Fuerzas Armadas, 2021). Estas amenazas pueden provenir tanto de fuentes internas como externas y abarcan una variedad de dimensiones, que incluyen la seguridad militar, política, económica, social y medioambiental. Las amenazas a la seguridad del estado pueden variar en naturaleza y gravedad, y su percepción puede diferir según el contexto y los valores nacionales. Algunos ejemplos de amenazas a la seguridad del estado incluyen (Fuerza Terrestre, 2022):

- Amenazas Militares.- Incluyen la posibilidad de agresión militar, la proliferación de armas de destrucción masiva, el terrorismo, los conflictos fronterizos y las tensiones entre estados que pueden escalar a conflictos armados.

- **Ciberataques y Ciberseguridad.**- Las amenazas cibernéticas abarcan desde ataques informáticos que buscan interrumpir sistemas y redes críticas hasta la ciberespionaje y el robo de información sensible.
- **Inestabilidad Política y Social.**- La inestabilidad interna, como disturbios civiles, insurgencia, conflicto étnico o político, y el debilitamiento de las instituciones, puede socavar la seguridad y el funcionamiento del estado.
- **Crisis Económica.**- Una economía débil, la falta de recursos, el desempleo elevado y la dependencia económica pueden amenazar la estabilidad y el bienestar del estado.
- **Cambio Climático y Desastres Naturales.**- Los impactos del cambio climático, como fenómenos meteorológicos extremos y desastres naturales, pueden causar daños significativos a la infraestructura, la población y la economía.
- **Tensiones Internacionales y Diplomáticas.**-Las relaciones tensas con otros estados, disputas territoriales y rivalidades geopolíticas pueden dar lugar a amenazas en el ámbito internacional.
- **Crimen Organizado y Tráfico Ilícito.**- La proliferación del crimen organizado, el tráfico de drogas, armas y personas, y la corrupción pueden erosionar la seguridad interna y socavar la autoridad del estado.
- **Extremismo Ideológico.**- La propagación de ideologías extremistas, ya sean de carácter religioso, político o social, puede generar tensiones y conflictos internos.

Guerra Híbrida

La guerra no convencional, también conocida como guerra asimétrica, es un tipo de conflicto en el cual una de las partes involucradas, generalmente la más débil o menos convencional, utiliza estrategias y tácticas no tradicionales para enfrentar a una fuerza militar convencional o a un adversario superior en términos de recursos y tecnología (CESEDEN, 2012). A diferencia de la

guerra convencional, que se basa en el enfrentamiento directo de fuerzas militares en un campo de batalla tradicional, la guerra no convencional se caracteriza por su enfoque en tácticas no convencionales y en el uso de estrategias que buscan explotar las debilidades y vulnerabilidades del adversario.

Multidominio

Multidominio o dominio múltiple es una concepción del dominio en diferentes, campos, áreas o facetas de un conocimiento específico. Si bien hay muchas discusiones filosóficas sobre el futuro de la guerra, el importante diálogo sobre la definición de dominios se ha mantenido prácticamente intacto. En el campo de la defensa, en la actualidad hay mucha gente tratando de entender lo que esto significa para el empleo de las fuerzas, pero gran parte de esta concepción se basa en la definición de dominio (Leiva & Versalovic, 2020). La doctrina ayuda con la definición de un dominio dentro del entorno operativo.

Lo más cerca que se pone es en la descripción del entorno operativo que lo relaciona con dominios, pero la noción de un entorno operativo no es lo mismo que un dominio, ya que éste puede abarcar algunos o todos los dominios según el lugar donde el comandante necesite operar.

Así el entorno operativo está mucho más cerca del concepto de múltiples dominios como un todo, donde el comandante utilizará una variedad de dominios para lograr sus objetivos operativos y estratégicos.

Operaciones de la información

Las operaciones de la información son un conjunto planificado y coordinado de acciones que buscan influir en la percepción, comprensión y comportamiento de audiencias específicas, con el propósito de lograr objetivos estratégicos y tácticos (IEEE, 2018). Estas operaciones se

basan en la gestión de la información y la comunicación para moldear la narrativa, manipular la opinión pública y generar efectos psicológicos que favorezcan los intereses de quienes las implementan.

Las operaciones de la información se extienden más allá de la difusión de datos y noticias. Incluyen la diseminación de mensajes persuasivos, la creación de narrativas coherentes y la contrarrestación de información falsa o desinformativa (Comando de Educación y Doctrina Militar Terrestre, 2020). Pueden utilizarse tanto en contextos militares como en ámbitos políticos, sociales y empresariales para influir en la toma de decisiones, la moral de las fuerzas, la opinión pública y la percepción internacional.

Estas operaciones pueden involucrar medios tradicionales como la prensa, la radio y la televisión, pero también abarcan el ámbito digital y el ciberespacio, donde la difusión de información falsa y la manipulación de redes sociales han ganado relevancia (Comando de Educación y Doctrina Militar Terrestre, 2020). Las operaciones de la información son una herramienta poderosa en el arsenal de actores estatales y no estatales, y su éxito radica en su capacidad para influir en la percepción y la actitud de las audiencias clave.

Complejidad

La complejidad caracteriza el comportamiento de un sistema o modelo cuyos componentes interactúan de múltiples formas y siguen reglas locales, lo que conduce a la no linealidad, la aleatoriedad, la dinámica colectiva, la jerarquía y la emergencia. El término generalmente se usa para caracterizar algo con muchas partes donde esas partes interactúan entre sí de múltiples maneras, culminando en un orden superior de emergencia mayor que la suma de sus partes (de la Herrán, 2011). El estudio de estos enlaces complejos en varias escalas es el objetivo principal de la teoría de sistemas complejos.

El criterio intuitivo de complejidad se puede formular de la siguiente manera: un sistema sería más complejo si se pudieran distinguir más partes y si existieran más conexiones entre

ellas. La ciencia a partir de 2010 adopta una serie de enfoques para caracterizar la complejidad; reflejan muchos de estos. Neil Johnson afirma que "incluso entre los científicos, no existe una definición única de complejidad, y la noción científica tradicionalmente se ha transmitido usando ejemplos particulares." En última instancia, Johnson adopta la definición de "ciencia de la complejidad" como "el estudio de los fenómenos que emergen de una colección de objetos que interactúan".

Marco Legal

La Constitución de la república del Ecuador en su artículo 158 expresa:

“Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos. Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía e integridad territorial y, complementariamente, apoyar en la seguridad integral del Estado de conformidad con la ley “ (Ecuador, 2018, pág. 91).

Art. 159.- Las Fuerzas Armadas y la Policía Nacional serán obedientes y no deliberantes, y cumplirán su misión con estricta sujeción al poder civil y a la Constitución. Las autoridades de las Fuerzas Armadas y de la Policía Nacional serán responsables por las órdenes que impartan. La obediencia a las órdenes superiores no eximirá de responsabilidad a quienes las ejecuten (Ecuador, 2018).

Art. 160 inciso cuarto. - Los miembros de las Fuerzas Armadas y de la Policía Nacional serán juzgados por los órganos de la Función Judicial; en el caso de delitos cometidos dentro de su misión específica, serán juzgados por salas especializadas en materia militar y policial, pertenecientes a la misma Función Judicial. Las infracciones disciplinarias serán juzgadas por los órganos competentes establecidos en la ley (Ecuador, 2018).

Art. 164.- La Presidenta o Presidente de la República podrá decretar el estado de excepción en todo el territorio nacional o en parte de él en caso de agresión, conflicto armado internacional o interno, grave conmoción interna, calamidad pública o desastre natural. La declaración del estado de excepción no interrumpirá las actividades de las funciones del Estado.

El estado de excepción observará los principios de necesidad, proporcionalidad, legalidad, temporalidad, territorialidad y razonabilidad. El decreto que establezca el estado de excepción contendrá la determinación de la causal y su motivación, ámbito territorial de aplicación, el periodo de duración, las medidas que deberán aplicarse, los derechos que podrán suspenderse o limitarse y las notificaciones que correspondan de acuerdo a la Constitución y a los tratados internacionales (Ecuador, 2018).

Art. 165.- Durante el estado de excepción la Presidenta o Presidente de la República únicamente podrá suspender o limitar el ejercicio del derecho a la inviolabilidad de domicilio, inviolabilidad de correspondencia, libertad de tránsito, libertad de asociación y reunión, y libertad de información, en los términos que señala la Constitución (Ecuador, 2018).

Ley de reforma a la Ley orgánica de Ciencia y tecnología e Innovación:

Artículo 5. De acuerdo con esta Ley, las acciones estatales en materia de ciencia, tecnología, innovación y sus aplicaciones estarán dirigidas a los sujetos mencionados en el artículo 3, dentro de las metas planteadas en el Plan Nacional de Desarrollo Económico y Social de la Nación, para cumplir con los siguientes objetivos:

- 1. Formular la política nacional de ciencia, tecnología, innovación y sus aplicaciones, así como impulsar y controlar la ejecución de las políticas públicas para la solución de problemas concretos de la sociedad y el ejercicio pleno de la soberanía nacional, a través de planes nacionales para la construcción de una sociedad justa e igualitaria (Ecuador, 2019).*

Sistemas de variables***Definición nominal*****Variable Independiente**

Operaciones multidominio en la guerra Rusia-Ucrania.

Variable Dependiente

Incidencia en la doctrina de operaciones de información de las FF.AA. ecuatorianas.

Definición conceptual

Tabla 1

Conceptualización de las variables

Variable	Concepto
Independiente Operaciones multidominio en la guerra Rusia-Ucrania.	Esta variable se refiere a la presencia, uso y efectividad de las operaciones multidominio en la guerra Rusia Ucrania
Dependiente Incidencia en la doctrina de operaciones de información de las FF.AA. ecuatorianas.	Esta variable se refiere a cómo la guerra en Ucrania y el uso de las operaciones multidominio, específicamente en el ámbito de las operaciones de información, han influido en la doctrina de operaciones de información de otros países y en particular en las Fuerzas Armadas ecuatorianas.

Nota. Conceptualización basada en el Manual Fundamental del Ejército. Sistemas Operativos del Campo de Batalla (Comando de Educación y Doctrina Militar Terrestre, 2020)

Definición operacional

Tabla 2

Definición operacional de las variables

Variable	Procedimiento
Independiente Operaciones multidominio en la guerra Rusia-Ucrania.	Se medirá la variable independiente a través del análisis de la documentación oficial disponible, así como de fuentes secundarias tales como artículos académicos y noticias de prensa. Se examinarán las estrategias, tácticas y técnicas utilizadas por las fuerzas militares rusas y ucranianas en los diferentes dominios de la guerra (terrestre, marítimo, aéreo, cibernético, etc.) para determinar su impacto en el

Variable	Procedimiento
Dependiente Incidencia en la doctrina de operaciones de información de las FF.AA. ecuatorianas.	desarrollo de la doctrina de operaciones de información. Se medirá la variable dependiente a través de la revisión y el análisis de la doctrina de operaciones de información actualmente vigente en las Fuerzas Armadas ecuatorianas. Se identificarán los cambios y ajustes realizados a la doctrina en relación con la incorporación de las operaciones multidominio y se evaluará su grado de influencia en la planificación y ejecución de las operaciones de información de las FF.AA. ecuatorianas.

Nota. Conceptualización operacional determinada por la metodología descriptiva mixta

Hipótesis

Hipótesis general:

Las operaciones multidominio en la guerra Rusia-Ucrania han tenido un impacto significativo en la doctrina de operaciones de información de las Fuerzas Armadas ecuatorianas.

Hipótesis específicas:

- La implementación de las operaciones multidominio en la guerra Rusia-Ucrania ha llevado a una mayor importancia y priorización de las operaciones de información como parte integral de la estrategia militar.
- La experiencia en las operaciones multidominio de la guerra Rusia-Ucrania ha llevado a una adaptación y actualización de la doctrina de operaciones de

información de las Fuerzas Armadas ecuatorianas para incluir enfoques multidisciplinarios y tecnológicos.

Operacionalización de las variables

Tabla 3

Operacionalización de las variables

Variables	Conceptualización	Subdimensiones	Indicadores	Pregunta de investigación	Dimensión	Instrumentos y técnicas
Independiente Operaciones multidominio en la guerra Rusia-Ucrania.	Esta variable se refiere a la presencia, uso y efectividad de las operaciones multidominio en la guerra Rusia-Ucrania.	Integración de capacidades en diferentes dominios Coordinación de acciones, sinergia en los efectos.	Grado de integración de capacidades de las fuerzas armadas en diferentes dominios (terrestre, aéreo, marítimo, cibernético, espacial). Nivel de coordinación y cooperación entre las distintas unidades en operaciones multidominio. Sinergia en los efectos: medida en que las operaciones multidominio producen un efecto mayor que la suma de sus partes.	¿Cómo han evolucionado las operaciones multidominio en la guerra Rusia-Ucrania?	Operaciones multidominio	análisis bibliográfico, entrevistas a expertos militares, observación de ejercicios militares, encuestas a personal militar.
Dependiente Incidencia en la doctrina de operaciones de información de las FF.AA. ecuatorianas	Esta variable se refiere a cómo la guerra en Ucrania y el uso de las operaciones multidominio, específicamente en el ámbito de las operaciones de información, han influido en la doctrina de operaciones de información de las Fuerzas Armadas ecuatorianas.	Planificación Ejecución Evaluación Obtención de ventaja sobre el enemigo, Apoyo a los objetivos militares.	Grado de integración de la planificación de operaciones multidominio con la planificación de operaciones de información. Nivel de efectividad de las operaciones de información en operaciones multidominio. Grado de análisis y evaluación de los resultados de las operaciones de información en operaciones multidominio. Medida en que las operaciones de información contribuyen a obtener una ventaja sobre el enemigo. Grado en que las operaciones de información contribuyen a la consecución de los objetivos militares.	¿Cuál es el papel de las operaciones de información en la guerra Rusia-Ucrania y cómo pueden influir en la doctrina de las operaciones de información de las FF.AA ecuatorianas.?	Doctrina de operaciones de información	análisis bibliográfico, entrevistas a expertos militares, observación de ejercicios militares, encuestas a personal militar.

Nota. Operacionalización basada en el Manual Fundamental del Ejército. Sistemas Operativos del Campo de Batalla (Comando de Educación y Doctrina Militar Terrestre, 2020) y en el diseño metodológico de la investigación.

Capítulo III

Marco Metodológico

Metodología

Tipo de investigación

Para la presente investigación se adoptará una investigación mixta, (cuantitativa cualitativa) y exploratoria que permita aprovechar los beneficios de cada una, inicialmente cuantificando los datos que arrojen las encuestas, y posteriormente mediante la cualificación de los criterios de los expertos.

La estructura general de un diseño cuantitativo se basa en el método científico. Utiliza el razonamiento deductivo, donde el investigador forma una hipótesis, recopila datos en una investigación del problema y luego usa los datos de la investigación (Hernández, Metodología de la Investigación, 2016), después de que se realiza el análisis y se comparten las conclusiones, para probar la validez de las hipótesis

La metodología cualitativa es inductiva en su razonamiento. El investigador selecciona un tema general y luego comienza a recopilar información para ayudar en la formación de una hipótesis (Hernández Sampieri, 2014). Los datos recopilados durante la investigación crean la hipótesis para el investigador en este modelo de diseño de investigación.

En el marco de la investigación actual, se plantea la recopilación de datos cuantitativos que aborden la frecuencia y efectividad de las operaciones multidominio y de información en el contexto del conflicto entre Rusia y Ucrania. Simultáneamente, se contempla la posibilidad de obtener información cualitativa mediante entrevistas con expertos, análisis de discursos y examen de documentos pertinentes. Estas aproximaciones permitirán una comprensión más profunda de la implementación y percepción de dichas estrategias.

La investigación exploratoria permitiría explorar posibles relaciones causales entre las operaciones multidominio y de la información en el conflicto ruso-ucraniano y su influencia en la doctrina de operaciones de información en las FFAA de Ecuador. Es así que, se generan hipótesis preliminares sobre cómo estas experiencias podrían haber afectado las políticas y prácticas militares de Ecuador.

Diseño de la investigación

Para la presente investigación se ha optado por un diseño de investigación mixto y exploratorio. A continuación, se describe:

En el componente cuantitativo, se recopila y analiza datos numéricos relacionados con la frecuencia y la efectividad de las operaciones multidominio y de información en el conflicto Rusia - Ucrania. Esto podría incluir estadísticas sobre ataques cibernéticos, campañas de desinformación, acciones militares en diferentes dominios y sus resultados. Estos datos numéricos podrían proporcionar una visión general de cómo se han empleado estas estrategias en el conflicto y cuáles han sido sus impactos.

Para el componente cualitativo, se realiza un análisis en profundidad de las estrategias y tácticas utilizadas en las operaciones multidominio y de información en el conflicto Rusia - Ucrania. Esto implica la aplicación de entrevistas con expertos en seguridad y defensa, análisis de discursos gubernamentales y militares, y revisión de documentos estratégicos y de políticas. A través de estas fuentes cualitativas, se podría obtener una comprensión más profunda de los objetivos subyacentes, las motivaciones y las implicaciones de estas estrategias.

Dado que el tema de investigación implica explorar cómo las experiencias en el conflicto Rusia - Ucrania podrían influir en la doctrina de operaciones de información en las FFAA de Ecuador, el enfoque exploratorio sería esencial. Esto significa que el estudio se centrará en generar nuevas ideas, hipótesis preliminares y comprensión a partir de la información

recopilada. No se partiría de teorías preexistentes, sino que se buscaría comprender la relación entre los dos conceptos de manera más completa y holística.

Una vez que se hayan recopilado y analizado los datos cuantitativos y cualitativos, se integrarían los resultados para obtener una visión completa de cómo las operaciones multidominio y de información se han utilizado en el conflicto Rusia - Ucrania y cómo podrían tener influencia en las FFAA de Ecuador. Los datos cuantitativos podrían respaldar las tendencias generales, mientras que los datos cualitativos podrían proporcionar un contexto y una comprensión más rica de los procesos y las motivaciones involucradas.

El diseño de investigación mixto y exploratorio permitiría una aproximación comprensiva y profunda al tema, al combinar datos numéricos con información cualitativa para entender la relación entre operaciones multidominio y de información en un conflicto específico y su posible repercusión en la doctrina militar de otro país.

Población

Para esto se plantea como población a los oficiales del Curso de Estado Mayor de Arma N° 74 (CEMA 74) y del Curso de Estado Mayor de Servicios N° 41 (CEMS 41) considerando la representatividad de todas las ramas del ejército, así como la experiencia y conocimiento del tema de investigación, se incluye también a directivos y autoridades de la Academia de Guerra del Ejército y del Comando de Educación y Doctrina de la Fuerza Terrestre, oficiales del Ejército Ecuatoriano, como referentes en el conocimiento de la doctrina militar relacionada con el tema de investigación y las características y desarrollo del conflicto entre Ucrania y Rusia. .

Muestra

Dentro de la población de 134 oficiales se estima el cálculo de la muestra con la siguiente fórmula:

Cálculo de la Muestra:

$$n = \frac{K^2 NPq}{e^2(N - 1) + K^2 Pq}$$

En donde:

N= Conjunto universo o población

n = Tamaño de la muestra

Pq = 0,25/N constante que representa la cuarta parte del universo

N-1 = Corrección paramétrica

e = (0.1 a 0.5%: entre 1 y 5 %) Error admisible para las inferencias

K = 1.96 Constante de corrección del error

$$n = \frac{1.96^2 * 0.25 * 143}{0.05^2(143 - 1) + 1.96^2 * 0.25}$$

$$n = 102$$

Técnicas e instrumentos de recolección de datos

Revisión bibliográfica documental

Una revisión bibliográfica comprende un resumen de la teoría y conceptos necesarios para el respaldo metodológico del diseño de la investigación necesarios para alcanzar los objetivos de la misma, esta revisión comprende fuentes primarias oficiales, artículos académicos y bibliografía especializada respecto al tema de investigación.

Entrevista

Una entrevista es generalmente una técnica de investigación cualitativa que implica hacer preguntas abiertas para conversar con los encuestados y recopilar datos sobre un tema. En la mayoría de los casos, el entrevistador es el experto en la materia que intenta comprender

las opiniones de los encuestados en una serie de preguntas y respuestas planificadas y ejecutadas adecuadamente.

Para la presente investigación se realizará una entrevista semiestructurada los directivos y expertos en el tema de investigación de la Academia de Guerra del Ejército y del Comando de Educación y Doctrina de la Fuerza Terrestre.

Encuesta

La investigación define a las encuestas como "la recopilación de información de una muestra de individuos a través de sus respuestas a las preguntas planteadas respecto la resolución de las preguntas de investigación" (Gallardo, 2020). Este tipo de investigación permite una variedad de métodos para reclutar participantes, recopilar datos y utilizar varios métodos de instrumentación. La investigación por encuestas puede usar estrategias de investigación cuantitativa (por ejemplo, usando cuestionarios con ítems calificados numéricamente), estrategias de investigación cualitativa.

Las encuestas encuentran dirigidas al personal militar de la AGE, que por su formación poseen sólidos conocimientos relativos a seguridad y defensa, militares, académicos y profesionales en áreas relacionadas, con experiencia en operaciones multidominio y de información. Estos datos podrían ofrecer perspectivas valiosas sobre la relación entre el conflicto Rusia - Ucrania y la doctrina de operaciones de información en las FFAA de Ecuador.

Instrumentos de recolección de datos

Los instrumentos de la recolección de datos son herramientas definidas como físicas o digitales utilizadas para la aplicación de las técnicas de recolección de datos (Hernández, Metodología de la Investigación, 2016). La presente investigación utiliza medios digitales y reuniones virtuales (Google Forms, Zoom).

Capítulo IV

Resultados de la investigación

Análisis e interpretación de resultados

1. ¿Qué ámbitos de las operaciones multidominio empleadas en la guerra Rusia- Ucrania considera que han sido más decisivas en el desarrollo del conflicto?

Tabla 4

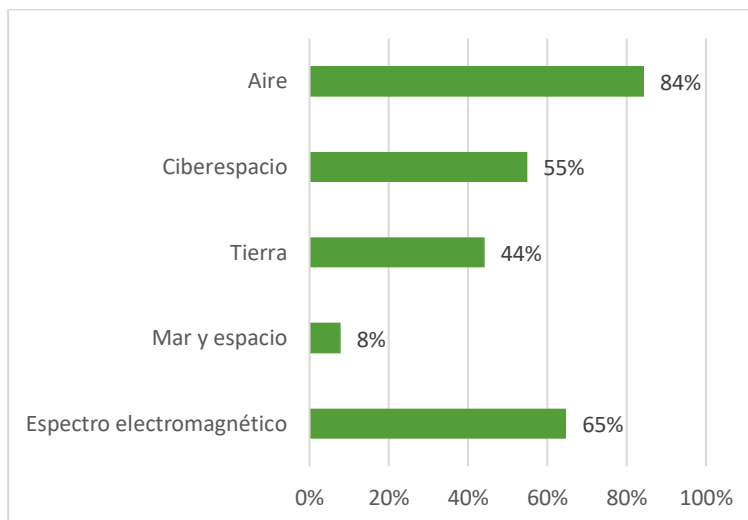
Ámbitos de las operaciones multidominio

Respuesta	Frecuencia	Porcentaje
Aire	86	84%
Ciberespacio	56	55%
Tierra	45	44%
Mar y espacio	8	8%
Espectro electromagnético	66	65%

Nota. Datos de la encuesta realizada

Figura 2

Ámbitos de las operaciones multidominio



Como se puede apreciar en los resultados, el aire 84% y el espectro electromagnético 65% fueron las opciones que más eligieron los entrevistados, seguidas de ciberespacio 55% y tierra 44%; por último, eligieron la mar y espacio con 8%.

Esta apreciación está basada en el empleo de los sistemas de guerra electrónica por parte de las dos naciones, que aunque mediáticamente no son evidenciados, los expertos en seguridad y defensa y en análisis de conflictos, han hecho notar que pese a poderío ruso en este campo las operaciones ucranianas han sabido controlar a las operaciones rusas, en el mismo tema opiniones de expertos ecuatoriano, ejemplifican la efectividad en esta campo de Ucrania pese a contar con menos equipos que los rusos.

2. ¿Cree usted que, desde la perspectiva de ser un conflicto asimétrico, la guerra entre Rusia y Ucrania, ha evidenciado la eficiencia del desarrollo cualitativo de la fuerza de combate en lugar de un incremento cuantitativo de la misma?

Tabla 5

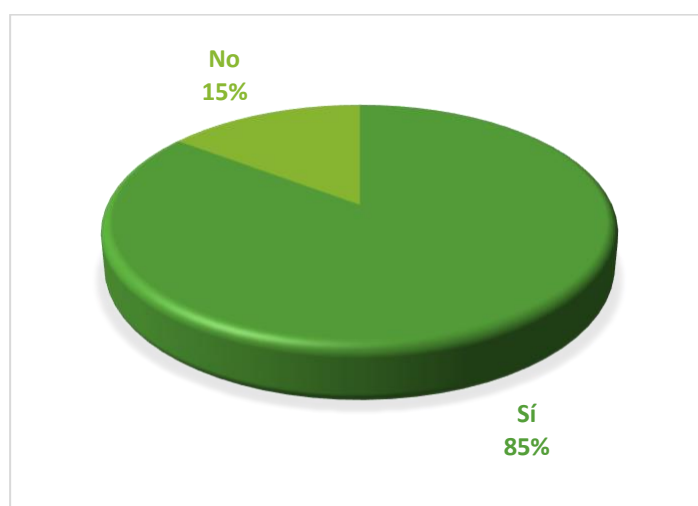
Eficiencia del desarrollo cualitativo de la fuerza de combate

Respuesta	Frecuencia	Porcentaje
Sí	87	85%
No	15	15%
Total	102	15%

Nota. Datos de la encuesta realizada

Figura 3

Eficiencia del desarrollo cualitativo de la fuerza de combate



Los resultados de esta pregunta indican que 85% de la población representada en la muestra encuestada, consideraron el sí como respuesta, mientras que el 15% como opción elegida.

Se puede apreciar que una mayoría muy elevada considera que la guerra asimétrica entre Rusia y Ucrania, ha evidenciado la eficiencia del desarrollo cualitativo de la fuerza de combate en lugar de un incremento cuantitativo de la misma. Esta aseveración parte del uso efectivo del poder de combate, fundamentalmente del lado ucraniano, sin embargo, según expertos entrevistados, las fuerzas rusas, luego de ataques frontales y masivos, también han asumido el dotar a sus operaciones de un poder de combate de mejor calidad antes que de volumen o fuerza, particularmente por el contexto geográfico del ataque y el estiramiento obligado de sus líneas de bastecimiento logístico.

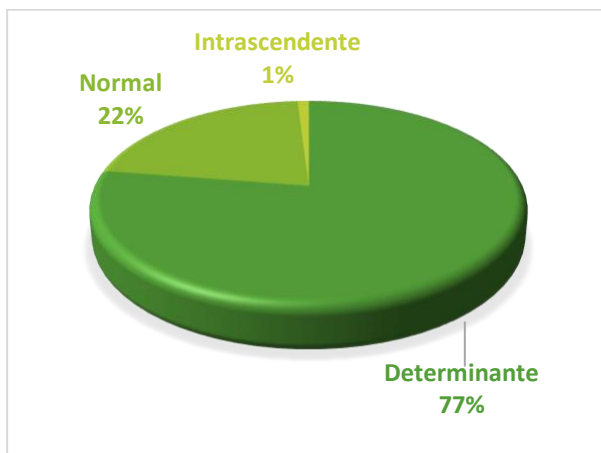
3. ¿De qué manera cree usted que las operaciones multidominio de la guerra entre Rusia y Ucrania han dependido del contexto tecnológico?

Tabla 6

Dependencia de la tecnología

Respuesta	Frecuencia	Porcentaje
Determinante	79	77%
Normal	22	22%
Intrascendente	1	1%
Total	102	1%

Nota. Datos de la encuesta realizada

Figura 4*Dependencia de la tecnología*

El 77% de la muestra respondió que ha sido determinante, el 22%, respondió que ha sido normal y el 1 % respondió que ha sido intrascendente.

Con respecto a esta pregunta, existe mucha información respecto a la dependencia tecnológica en la guerra de Rusia Ucrania. Caracterizado por el empleo de sistemas electrónicos y de armamento controlado por inteligencia artificial, así como el uso de aeronaves no tripuladas (drones), las cuales han tenido una efectividad relativa y una alta efectividad del lado ucraniano con las que ha podido equilibrar el poder de combate.

4. ¿Considera usted que el empleo de las operaciones multidominio por parte de Ucrania en la guerra contra Rusia ha determinado una prolongación inesperada del conflicto?

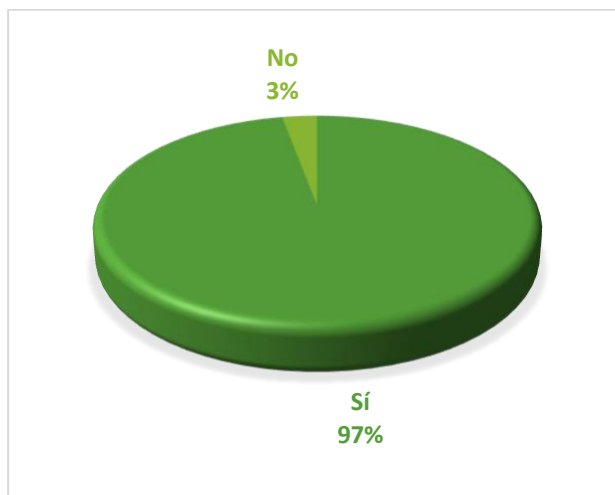
Tabla 7 *Efectividad del empleo de las operaciones multidominio**Efectividad del empleo de las operaciones multidominio*

Respuesta	Frecuencia	Porcentaje
Sí	99	97%
No	3	3%
Total	102	3%

Nota. Datos de la encuesta realizada

Figura 5

Efectividad del empleo de las operaciones multidominio



El 97% de personas encuestadas respondió afirmativamente a la pregunta planteada, mientras que el 3% lo hizo de forma negativa.

Una mayoría casi absoluta, considera que el empleo de las operaciones multidominio por parte de Ucrania en la guerra contra Rusia si ha determinado una prolongación inesperada del conflicto. En este sentido, es importante desatracar que el concepto de multidominio no es nuevo, y hasta hace unos años implicaba conceptualmente el empleo de operaciones de aire mar y tierra, de forma conjunta considerando al espectro electromagnético como un área fundamental para establecer posiciones de dominio, sobre todo aéreo. Este concepto no ha variado mucho, lo que ha cambiado es la inclusión de elementos tecnológicos e informáticos que son decisivos en contrarrestar el poder del enemigo.

5. ¿Cree usted que la concepción de adecuada de las operaciones multidominio pueden ser aplicadas por las Fuerzas Armadas del Ecuador considerando escenarios prospectivos determinadas por el desarrollo de nuevas amenazas?

Tabla 8

Aplicación de operaciones multidominio en las Fuerzas Armadas del Ecuador

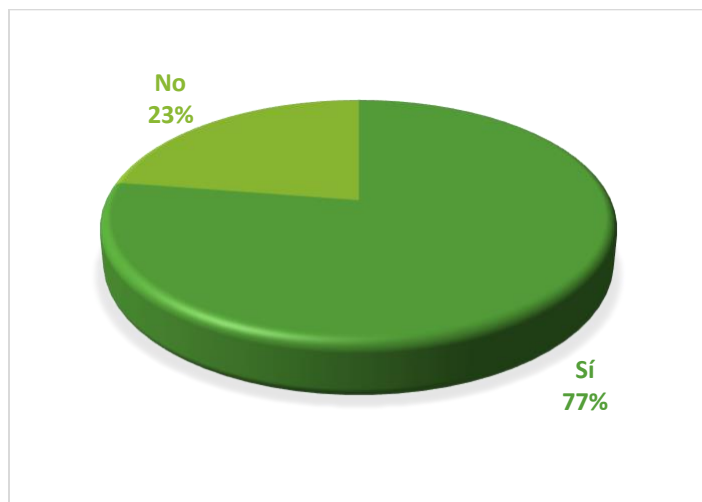
<u>Respuesta</u>	<u>Frecuencia</u>	<u>Porcentaje</u>
------------------	-------------------	-------------------

Sí	79	77%
No	23	23%
Total	102	23%

Nota. Datos de la encuesta realizada

Figura 6

Aplicación de operaciones multidominio en las Fuerzas Armadas del Ecuador



El 77% de los encuestados respondió que sí, a la pregunta planteada mientras que el 23% respondió que no.

La mayoría de los encuestados considera que la concepción de adecuada de las operaciones multidominio pueden ser aplicadas por las Fuerzas Armadas del Ecuador considerando escenarios prospectivos determinadas por el desarrollo de nuevas amenazas, lo que infiere en que los miembros de Fuerzas Armadas están conscientes de las capacidades que tienen Fuerzas Armadas para incorporar conceptos y enfoque nuevos de la guerra para mejorar sus capacidades y la defensa del territorio nacional. Esto se respalda, en el desarrollo de proceso como el de transformación de capacidades y el que en la actualidad plantea el desarrollo de las capacidades futuras. Sin embargo, habría que considerar, como opinan algunos expertos, que estos proyectos deben tener una base sólida para su desarrollo, ya que aún existen ciertas deficiencias para el desarrollo de capacidades y brechas que no han sido

cerradas lo que no ha impedido el emprendimiento de nuevos procesos, esto determina que los procesos cargan deficiencias que impiden una consecución real de objetivos.

6. ¿Considera que doctrina referente a las operaciones multidominio puede ser integrada de manera que las fuerzas operacionales del Ejército puedan aplicar su doctrina sin hacer cambios significativos a la fuerza actual?

Tabla 9

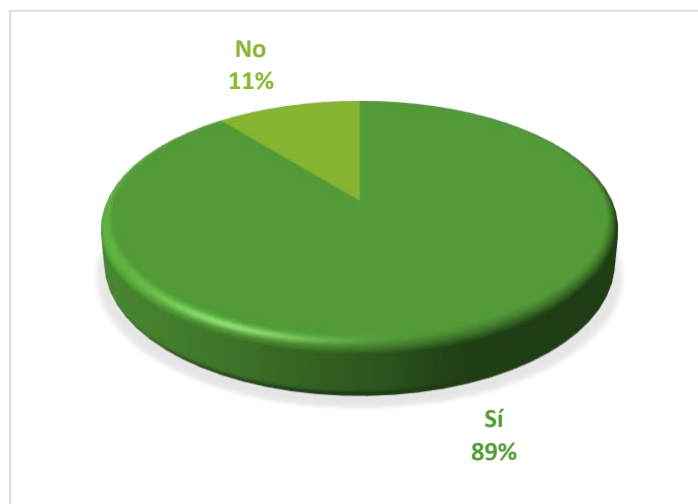
Integración de doctrina

Respuesta	Frecuencia	Porcentaje
Sí	91	89%
No	11	11%
Total	102	11%

Nota. Datos de la encuesta realizada

Figura 7

Integración de doctrina



El 89% opino que si mientras que el 11% negó el contenido de la pregunta respecto a la doctrina de las operaciones multidominio.

Los resultados infieren en que, si es posible alcanzar una integración de la doctrina de las operaciones multidominio sin hacer cambios significativos a la fuerza actual, esto puede ser relevante para la viabilidad de estrategias de cambios doctrinarios, para optimizar los recursos fundamentalmente. Sin embargo y de acuerdo a las opiniones de algunos expertos, la

integración de la doctrina multidominio, generalmente requiere de una gran inversión tecnológica en todas las capacidades.

7. ¿Desde la perspectiva de las Fuerzas Armadas ecuatorianas, la concepción de las operaciones multidominio empleadas en la Guerra de Rusia Ucrania podría ayudar a sus unidades operativas, a evitar una posición de desventaja relativa contra un adversario igual o casi igual en zonas geográficas críticas del territorio ecuatoriano en un futuro cercano?

Tabla 10

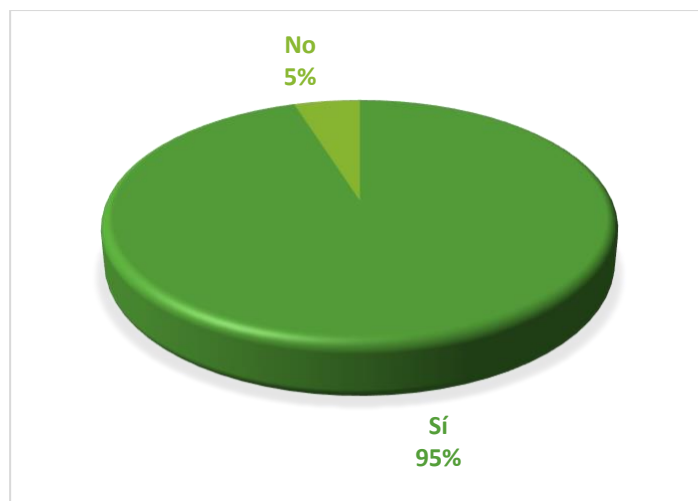
Aplicación de las operaciones multidominio para evitar posición de desventaja

Respuesta	Frecuencia	Porcentaje
Sí	97	95%
No	5	5%
Total	102	5%

Nota. Datos de la encuesta realizada

Figura 8

Aplicación de las operaciones multidominio para evitar posición de desventaja



El 95% de las personas entrevistadas respondieron afirmativamente, mientras que el 5% lo hicieron de forma negativa a la pregunta planteada.

Los resultados determinan una convicción de la utilidad y la aplicabilidad de las operaciones multidominio en la guerra moderna, y las posibles implicaciones para enfrentar

conflictos asimétricos al optimizar el poder de combate mediante la utilización de elementos tecnológicos y conceptos desarrollados por este tipo de operaciones.

8. ¿Cree usted que es factible el desarrollo de una propuesta doctrinaria de operaciones multidominio en las FFAA del Ecuador?

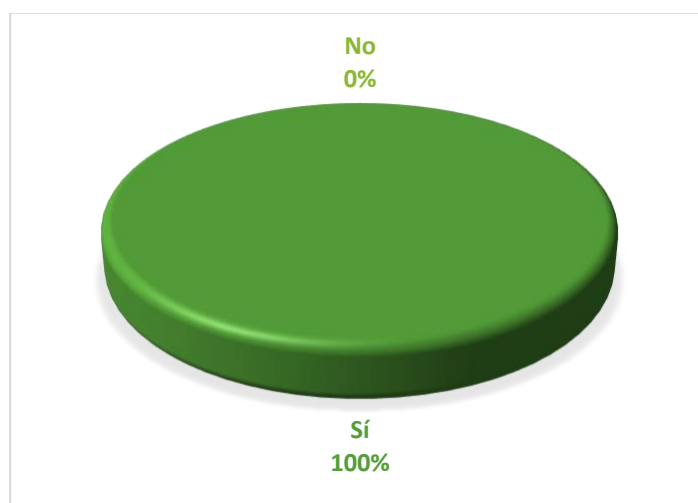
Tabla 11

Factibilidad de desarrollo de una propuesta doctrinaria de operaciones multidominio

Respuesta	Frecuencia	Porcentaje
Sí	102	100%
No	0	0%
Total	102	0%

Nota. Datos de la encuesta realizada

Figura 9 *Factibilidad de desarrollo de una propuesta doctrinaria de operaciones multidominio*



La totalidad e personas encuestadas está de acuerdo con que sí es factible el desarrollo de una propuesta doctrinaria de operaciones multidominio en las FFAA del Ecuador, en este sentido el tema de investigación despierta mucho interés en los miembros de las Fuerzas Armadas, comprometidos con el fortalecimiento institucional, ya que la actualización enfoques respecto a las operaciones militares son compatibles con los procesos modernizadores, como la consecución de capacidades futuras, el reto es entonces crear los mecanismos para plasmar estos avances e integrar los conocimientos adecuadamente de acuerdo a las características de las fuerzas propias.

Resumen de resultados de la entrevista

Análisis de los Resultados de las Entrevistas sobre Operaciones Multidominio y Operaciones de Información en el Conflicto Rusia-Ucrania

Las entrevistas realizadas a diversos expertos en seguridad y defensa, , proporcionaron una visión integral sobre los factores de incidencia y las áreas a considerar en el desarrollo de capacidades militares, las operaciones multidominio y las operaciones de información en el contexto del conflicto entre Rusia y Ucrania. A continuación, se destacan los principales hallazgos y conclusiones:

Todos los expertos destacaron la importancia crucial de la tecnología en el desarrollo de capacidades militares. El contexto tecnológico influyó significativamente en la eficacia de las operaciones multidominio y de información. Esto incluyó sistemas de comunicación avanzados, vigilancia, ciberseguridad y guerra electrónica.

En un conflicto asimétrico como el de Rusia y Ucrania, se enfatizó la eficiencia del desarrollo cualitativo de la fuerza de combate en lugar de un incremento cuantitativo. La adaptabilidad, la modernización y la formación de las fuerzas fueron aspectos clave para resistir y contrarrestar a un adversario más grande.

Además de las capacidades militares, se resaltó la importancia de las operaciones multidominio en los ámbitos económico y diplomático. Las sanciones económicas y la diplomacia efectiva pueden influir en el curso del conflicto.

Desde la perspectiva de un coronel de las FFAA del Ecuador, se subrayó la importancia de mantener a las fuerzas abastecidas, operativas y con apoyo logístico adecuado en el terreno. Esto es esencial para garantizar la capacidad de resistencia y la presión sostenida.

Los expertos resaltaron el papel crucial de la ciberseguridad y las capacidades de guerra electrónica en las operaciones de información. Estos aspectos fueron esenciales para proteger las comunicaciones, desestabilizar al enemigo y moldear la percepción pública.

Se reconoció que las operaciones de información tienen un impacto significativo en la narrativa y la percepción pública. Moldear la opinión tanto nacional como internacional puede influir en el apoyo y la legitimidad de las partes en conflicto.

Conclusiones

El conflicto entre Rusia y Ucrania ha demostrado la importancia de la adaptación y modernización de las capacidades militares en un entorno multidominio y asimétrico.

La tecnología desempeñó un papel destacado en las operaciones multidominio y de información, destacando la necesidad de inversiones y desarrollos en este ámbito.

La influencia económica, diplomática y la logística fueron aspectos complementarios a las capacidades militares en el conflicto.

Las operaciones de información se han convertido en un componente crítico en la estrategia de conflicto, influyendo en la percepción pública y la opinión internacional.

La adaptación de estas lecciones al contexto de las Fuerzas Armadas del Ecuador y su preparación para amenazas emergentes es esencial para garantizar la seguridad nacional en el futuro.

El conflicto Rusia-Ucrania ha resaltado la necesidad de un enfoque multidominio y una mayor atención a las operaciones de información en los conflictos modernos. El desarrollo cualitativo de capacidades, la adaptación tecnológica y la consideración de factores no militares son cruciales para el éxito en entornos de seguridad cambiantes. Considerando estos puntos y factores detectados en la entrevista se cuenta con mejores elementos para el desarrollo de la propuesta de la investigación.

Capítulo V

Propuesta de la investigación

Título

Propuesta doctrinaria de operaciones multidominio en las FFAA del Ecuador

Introducción

En el contexto actual, marcado por una rápida evolución tecnológica y una creciente interconexión global, el panorama estratégico se caracteriza por una complejidad y volatilidad sin precedentes. Las Fuerzas Armadas de la República del Ecuador se encuentran inmersas en un entorno desafiante que exige una adaptación constante y una capacidad de respuesta versátil.

Los desafíos que enfrentan nuestras Fuerzas Armadas han adquirido una dimensión cada vez más diversa y multidimensional. Para hacer frente a estos desafíos de manera efectiva, es esencial adoptar un enfoque integral y coordinado que abarque todas las esferas estratégicas.

En este contexto, las Fuerzas Armadas de la República del Ecuador han iniciado un proceso integral de transformación de sus capacidades militares para adaptarse a las nuevas amenazas y desafíos que surgen constantemente. Para concretar esta visión estratégica, se han promulgado dos documentos cruciales: el "Plan Estratégico de Fuerzas Armadas 2021-2025" por el Comando Conjunto de Fuerzas Armadas en 2021 y el "Plan de Gestión de la Fuerza Terrestre al año 2033" por la Fuerza Terrestre en 2022. Ambos documentos establecen un marco de acción que traza la hoja de ruta para la modernización de las Fuerzas Armadas.

Sin embargo, en un entorno estratégico en constante cambio, es evidente la necesidad de mantener una actualización continua y una adaptación constante de la doctrina y las

capacidades militares. En este contexto, emerge como una iniciativa estratégica y visionaria la propuesta doctrinaria de operaciones multidominio en las Fuerzas Armadas de la República del Ecuador.

Esta propuesta se enfoca en el enfoque multidominio, que busca la integración sinérgica de capacidades en diversos dominios de combate, como el terrestre, marítimo, aéreo, ciberespacial y electromagnético. Este enfoque se considera esencial para abordar los desafíos actuales, que a menudo presentan una dimensión multidimensional que requiere una respuesta integral y coordinada.

Es importante destacar que esta propuesta se basa en los resultados de una exhaustiva investigación titulada "Análisis de las operaciones multidominio en la guerra Rusia-Ucrania y su impacto en la doctrina militar ecuatoriana". También se inspira en las mejores prácticas internacionales y se adapta a las particularidades del entorno operacional de la República del Ecuador. Para llevar a cabo eficazmente esta propuesta, se han formulado medidas específicas destinadas al desarrollo de capacidades y la capacitación del personal militar.

En su conjunto, la propuesta doctrinaria de operaciones multidominio en las Fuerzas Armadas de la República del Ecuador representa una iniciativa de carácter innovador y estratégico. Su objetivo principal es fortalecer la capacidad de defensa del país y garantizar la seguridad en un entorno estratégico caracterizado por su complejidad y constante cambio. Esta visión prospectiva refleja un compromiso inquebrantable con la excelencia y la adaptación, elementos esenciales para la preservación de la integridad y la seguridad de la nación.

Antecedentes

La emergente propuesta doctrinaria de operaciones multidominio en las Fuerzas Armadas de la República del Ecuador se presenta como una respuesta estratégica fundamentada en la comprensión y el abordaje de las amenazas contemporáneas de naturaleza no convencional. Estas amenazas, que van desde grupos terroristas hasta

ciberdelincuentes y organizaciones criminales altamente complejas, trascienden las confrontaciones tradicionales entre Estados-nación, configurando un escenario multidimensional que requiere una respuesta integral y coordinada que abarque diversos ámbitos de combate.

El origen de esta propuesta se encuentra en la necesidad imperante de integrar y coordinar las capacidades inherentes a los diferentes dominios de combate, creando así una sinfonía militar multidisciplinaria con el propósito de hacer frente de manera eficaz a estas amenazas emergentes y garantizar la soberanía y seguridad del país.

Paralelamente, esta iniciativa promueve la adopción de una modalidad de planificación por capacidades en contraposición a una planificación basada únicamente en la evaluación de amenazas específicas. El enfoque por capacidades se presenta como una estrategia de planificación que se centra en la definición de las capacidades esenciales necesarias para cumplir con las misiones y objetivos estratégicos, lo que confiere una mayor versatilidad y adaptabilidad ante las cambiantes condiciones del entorno estratégico.

La propuesta doctrinaria de operaciones multidominio en las Fuerzas Armadas de la República del Ecuador abraza con determinación este enfoque de planificación basada en capacidades, identificando las capacidades fundamentales requeridas para enfrentar las nuevas amenazas (Comando Conjunto de Fuerzas Armadas, 2021). Además, establece un conjunto de medidas específicas destinadas a fortalecer y desarrollar estas capacidades, en un esfuerzo evidente por modernizar y fortalecer nuestras Fuerzas Armadas para los desafíos del siglo XXI.

Esta propuesta no solo representa una respuesta pertinente y visionaria a las complejidades del contexto actual, sino que también refleja un compromiso sólido con la seguridad y el bienestar de la nación. A través de una estrategia que sabiamente amalgama la convergencia multidominio y la planificación por capacidades, se busca actualizar y mejorar la

eficacia de nuestras Fuerzas Armadas en beneficio de la seguridad nacional y el desarrollo de nuestro país.

Justificación

La propuesta doctrinaria de operaciones multidominio en las FFAA del Ecuador encuentra su fundamentación en la imperante necesidad de ofrecer una respuesta efectiva y eficiente a las amenazas no convencionales que acechan al país. Estas amenazas, de diversa procedencia, abarcan desde grupos armados ilegales hasta ciberataques, sabotajes y acciones terroristas, entre otras manifestaciones.

El narcotráfico y el crimen organizado representan un desafío significativo, pues utilizan tácticas de violencia e intimidación para salvaguardar sus intereses, incluso desafiando la autoridad estatal en zonas específicas del territorio. Además, su presencia transnacional y su uso de redes de narcotráfico para expandirse y consolidarse hacen que sean amenazas extremadamente difíciles de erradicar (Comando Conjunto de Fuerzas Armadas, 2019). En respuesta a esta compleja realidad, es crucial contar con una estrategia integral que involucre a todas las ramas de las Fuerzas Armadas, permitiendo un control efectivo del territorio y la disuasión de estas amenazas.

Por otro lado, la protección de los recursos naturales y los sectores estratégicos de la nación se vuelve de vital importancia, ya que son objetivos de interés para otros países o grupos no estatales que buscan obtener beneficios económicos o estratégicos (Comando Conjunto de Fuerzas Armadas, 2021). Estos sectores son vulnerables a amenazas como ataques cibernéticos, sabotajes o actos terroristas, lo que podría tener graves consecuencias para la economía y la estabilidad del país. Por lo tanto, resulta esencial contar con una estrategia integral y una planificación por capacidades que permitan integrar y coordinar las capacidades de los diferentes dominios de combate para proteger estos recursos y sectores estratégicos.

La propuesta de operaciones multidominio en las FFAA del Ecuador busca desarrollar capacidades en múltiples dominios de combate, que abarcan el terrestre, marítimo, aéreo, ciberespacial y el espacio. Este enfoque integral y la planificación por capacidades buscan asegurar que se puedan integrar y coordinar de manera efectiva las capacidades en diferentes dominios para hacer frente a estas amenazas, garantizando así la seguridad y la estabilidad de Ecuador.

Esta propuesta se sustenta en la necesidad apremiante de abordar de manera eficaz y eficiente las amenazas no convencionales que enfrenta el país. Su enfoque integral y su planificación por capacidades se presentan como pilares esenciales para la seguridad y estabilidad de Ecuador, permitiendo una respuesta coordinada y efectiva ante las complejidades y desafíos del entorno estratégico actual.

Metodología

La metodología para el desarrollo de la propuesta de doctrina de operaciones multidominio en las FFAA del Ecuador incluyó una investigación bibliográfica y documental exhaustiva para recopilar información relevante sobre las operaciones multidominio utilizadas en la guerra Rusia-Ucrania, su impacto en la doctrina militar y las mejores prácticas en este tipo de operaciones. Esta investigación también incluyó un análisis de la literatura sobre la doctrina militar ecuatoriana actual y las capacidades militares existentes.

Además de la investigación bibliográfica, se realizaron encuestas a expertos militares en operaciones multidominio, seguridad y defensa, inteligencia y gestión de información, para obtener información valiosa sobre las necesidades, desafíos y oportunidades de las FFAA del Ecuador en este ámbito. Los hallazgos de las características de las operaciones multidominio utilizadas en la guerra Rusia-Ucrania fueron esenciales para la propuesta doctrinaria, ya que sirvieron como un modelo para la definición de los principios y estrategias de las operaciones multidominio en el contexto ecuatoriano.

La importancia de los hallazgos de la investigación es que proporcionaron información relevante y actualizada sobre las operaciones multidominio, que es una necesidad crítica para las FFAA del Ecuador en el contexto de la evolución de la tecnología y las amenazas emergentes. Los hallazgos también sirvieron como base para desarrollar una propuesta doctrinaria efectiva y adaptada a las necesidades específicas del Ecuador, que pueda mejorar la capacidad operativa de las FFAA en entornos multidominio complejos y garantizar la seguridad y defensa del país.

Evolución de las operaciones multidominio

Las operaciones multidominio surgieron como respuesta a los nuevos desafíos que enfrentan las fuerzas militares en el siglo XXI, en un entorno caracterizado por una creciente complejidad y por el uso de tecnologías cada vez más avanzadas por parte de los adversarios.

En este contexto, las operaciones multidominio buscan integrar y coordinar las capacidades de los diferentes dominios de combate (terrestre, marítimo, aéreo, ciberespacio y espacio) para lograr un mayor grado de efectividad y eficiencia en el cumplimiento de los objetivos militares.

En la actualidad, varias Fuerzas Armadas de todo el mundo están adoptando la doctrina de las operaciones multidominio en sus estrategias militares. Por ejemplo, el ejército de los Estados Unidos ha desarrollado la "Operación multidominio" como una nueva forma de guerra que implica la convergencia de los dominios terrestre, marítimo, aéreo, ciberespacio y espacio, con el objetivo de mejorar la integración de las operaciones y la coordinación entre las diferentes ramas militares.

Con respecto a la adopción de la doctrina de operaciones multidominio por parte del ejército estadounidense, el General James McConville, Jefe de Estado Mayor del Ejército de los EE. UU., dijo lo siguiente: "La Operación multidominio es una nueva forma de guerra que involucra a todos los dominios de combate: terrestre, marítimo, aéreo, ciberespacio y espacio,

para sincronizar nuestros esfuerzos en el campo de batalla" (Fuente: U.S. Army, "Multidomain Operations: Evolution of Combined Arms for the 21st Century", 2018).

De igual forma, el ejército británico ha desarrollado la "Integración de los dominios", que se centra en la combinación de las capacidades militares en los diferentes dominios de combate para lograr una mayor efectividad y eficiencia.. AL respecto el General Sir Mark Carleton-Smith, jefe del Estado Mayor del Ejército británico, dijo lo siguiente: "La integración de los dominios es esencial para la supervivencia y el éxito de la fuerza, y se trata de aprovechar nuestras capacidades militares en los diferentes dominios de combate para lograr una mayor efectividad y eficiencia" (Fuente: Royal United Services Institute, "Integrating the Domains: An Agenda for Reforming UK Military Jointness", 2018).

Asimismo, el ejército australiano ha adoptado la doctrina de "Operaciones multidominio" para mejorar su capacidad de defensa y protección de los intereses nacionales. el Teniente General Rick Burr, Jefe del Ejército australiano, opina que: "Las operaciones multidominio se centran en integrar nuestras capacidades militares en los diferentes dominios de combate para lograr una mayor efectividad y eficiencia en la defensa y protección de nuestros intereses nacionales" (Fuente: Australian Army, "Multidomain Operations Concept", 2018).

Como se puede apreciar las operaciones multidominio se han convertido en una tendencia en la planificación militar moderna, y están siendo adoptadas por varias Fuerzas Armadas en todo el mundo para mejorar su capacidad de defensa y enfrentar los nuevos desafíos del entorno operativo actual.

Aplicación doctrinaria

Las operaciones multidominio son una doctrina militar que se centra en integrar y sincronizar las capacidades militares en los diferentes dominios de combate (terrestre, marítimo, aéreo, ciberespacial y espacial) para lograr una mayor efectividad y eficiencia en la defensa y protección de los intereses nacionales.

Actualmente, las operaciones multidominio se aplican en diversos contextos, incluyendo:

Operaciones multidominio en la seguridad y defensa

Son aquellas en donde se requiere una integración de las capacidades militares en los diferentes dominios de combate para proteger los intereses nacionales y garantizar la seguridad de la población.

Las operaciones multidominio se han convertido en una doctrina militar importante para lograr una mayor efectividad y eficiencia en la defensa y protección de los intereses nacionales en diferentes contextos militares y de seguridad.

Operaciones militares en entornos urbanos

Las operaciones multidominio se han utilizado en operaciones militares en zonas urbanas, donde se requiere una integración de las capacidades militares terrestres, aéreas y ciberespaciales para lograr objetivos militares y minimizar el daño colateral.

Operaciones militares en entornos marítimos: las operaciones multidominio se han utilizado en operaciones militares en entornos marítimos, donde se requiere una integración de las capacidades militares marítimas, aéreas y espaciales para lograr objetivos militares, como el control de la navegación y la protección de los intereses nacionales.

Operaciones militares en el espacio aéreo

Las operaciones multidominio en el entorno del espacio aéreo se refieren al uso coordinado y sinérgico de capacidades de múltiples dominios, incluyendo el aire, el espacio, la ciberesfera y el espectro electromagnético, para lograr objetivos militares en el ámbito aéreo.

En el contexto de la defensa aérea, las operaciones multidominio pueden implicar el uso de radares terrestres y satelitales, aviones de combate, sistemas de defensa aérea y misiles tierra-aire, así como capacidades de ciberdefensa para garantizar la seguridad de los sistemas de comando y control. En una situación de conflicto, las operaciones multidominio en el espacio aéreo también pueden involucrar la colaboración entre diferentes Fuerzas Armadas, como la Fuerza Aérea, la Armada y el Ejército, para garantizar el control y la protección del espacio aéreo en un área determinada.

Además, en el ámbito de operaciones internas, las operaciones multidominio en el espacio aéreo también pueden incluir la coordinación entre las Fuerzas Armadas y las agencias gubernamentales y organizaciones civiles en situaciones de emergencia, como la lucha contra incendios forestales o la búsqueda y rescate de personas en áreas remotas.

En general, las operaciones multidominio en el espacio aéreo son esenciales para garantizar la seguridad nacional y la protección de la soberanía del espacio aéreo del país, y deben ser desarrolladas y aplicadas de manera integrada y coordinada para maximizar su eficacia.

Operaciones militares en entornos ciberespaciales

Las operaciones multidominio se han utilizado en operaciones militares en entornos ciberespaciales, donde se requiere una integración de las capacidades militares ciberespaciales, terrestres y aéreas para lograr objetivos militares, como la protección de la infraestructura crítica y la defensa contra ciberataques.

Doctrina Integral de Operaciones Multidominio en la Seguridad y Defensa Nacional: Cimientos y Fundamentos

Introducción

La Doctrina de Operaciones Multidominio representa un paradigma estratégico esencial en el ámbito de la seguridad y defensa nacional para las Fuerzas Armadas del Ecuador. Este enfoque reviste una trascendencia indiscutible en el contexto de la preservación de la soberanía, la integridad territorial y los intereses vitales del Estado ecuatoriano, además de la salvaguardia de la seguridad ciudadana y el patrimonio nacional.

Objetivo

El núcleo rector de las operaciones militares multidominio en el marco de la seguridad y defensa se despliega con el propósito inequívoco de garantizar la defensa de la nación ecuatoriana. Estas operaciones, concebidas como un esfuerzo conjunto de las tres ramas de las Fuerzas Armadas, potencialmente en coordinación con la Policía Nacional y otras entidades estatales, se inscriben de manera inseparable en las políticas y estrategias nacionales de seguridad. El objetivo primordial radica en la protección integral de la población y la preservación de los intereses fundamentales del país.

Responsabilidades y Roles

Las Fuerzas Armadas del Ecuador asumen una serie de roles y responsabilidades de alta trascendencia en la materialización de esta doctrina:

- El Comando Conjunto de las Fuerzas Armadas desempeña un papel central al planificar, ejecutar y supervisar las operaciones militares multidominio, colaborando activamente con las demás instituciones estatales para asegurar la seguridad nacional.
- El Comando Operacional Conjunto ostenta la responsabilidad de liderar y coordinar las operaciones militares en el ámbito territorial del Ecuador.

- La colaboración estrecha con la Policía Nacional y otras entidades estatales se establece como una premisa ineludible para la planificación, ejecución y coordinación de las operaciones de seguridad y defensa, con la protección de la población y los intereses del Estado como eje central.

Las tres ramas de las Fuerzas Armadas, a saber: el Ejército, la Armada y la Fuerza Aérea, deben estar en estado de constante preparación para emprender operaciones en tierra, mar y aire en respuesta a cualquier amenaza que atente contra la seguridad nacional.

Planificación y Ejecución de Operaciones

Las operaciones militares multidominio en el contexto de la seguridad y defensa se sustentan en una metodología eficiente, abarcando los siguientes aspectos:

- Evaluación de la amenaza: Se realiza una evaluación exhaustiva de la amenaza, considerando sus implicaciones para la seguridad nacional.
- Planificación de operaciones: Se elabora un plan detallado de operaciones que abarca los objetivos, tareas y recursos esenciales para la ejecución de la operación.
- Coordinación con otras instituciones: La cooperación interinstitucional se consolida como un pilar fundamental para garantizar el éxito de la operación.
- Ejecución de la operación: Las operaciones se llevan a cabo con celeridad, precisión y efectividad, priorizando la protección de la población y el patrimonio nacional.
- Evaluación de la operación: Posterior a la conclusión de la operación, se efectúa un análisis exhaustivo con el propósito de identificar lecciones aprendidas y optimizar las prácticas futuras.

Interoperabilidad

La interoperabilidad, vital en la ejecución exitosa de las operaciones militares multidominio en la seguridad y defensa, se fomenta mediante la creación de protocolos y procedimientos estandarizados para la planificación, ejecución y supervisión de operaciones

militares. Esto se hace en congruencia con la norma técnica de interoperabilidad, con un enfoque adaptado a las particularidades del ámbito de seguridad y defensa. Además, se promueve la convergencia de sistemas de comunicaciones y tecnologías de la información no solo entre las Fuerzas Armadas, sino también en colaboración con otras instituciones gubernamentales cuando sea necesario.

La Fundamentación Estratégica de las Operaciones Militares Multidominio en Entornos Urbanos para las Fuerzas Armadas del Ecuador

Introducción

La Doctrina para las Operaciones Militares en Entornos Urbanos (OMEU) representa un pilar fundamental en el abordaje de los desafíos contemporáneos de seguridad y defensa que enfrenta la nación ecuatoriana. Este marco conceptual se forja con la finalidad imperante de salvaguardar la vida y bienestar de la población, proteger los intereses nacionales y mitigar los impactos colaterales en el escenario urbano durante operaciones militares. En este contexto, un análisis exhaustivo de los principios y componentes de esta doctrina es esencial

Objetivos de las OMEU

Las OMEU, en su expresión más pura, conciben un propósito inequívoco: garantizar la seguridad de la población civil, salvaguardar los intereses nacionales y minimizar los efectos colaterales en el contexto urbano durante operaciones militares. Esta premisa se sustenta en la premisa de que, en el siglo XXI, los entornos urbanos concentran una parte significativa de la población y los activos críticos de un país, lo que exige una aproximación estratégica cuidadosamente estructurada.

Integración de las capacidades militares

En pos de alcanzar una eficacia óptima, las OMEU deben orquestar de manera sinérgica las capacidades militares en múltiples dominios, abarcando terrestre, aéreo,

ciberspacial y espacial. Este enfoque multidominio procura optimizar el rendimiento operativo y el cumplimiento de los objetivos militares.

Operaciones conjuntas

El éxito de las OMEU descansa en la ejecución conjunta, donde las tres ramas de las Fuerzas Armadas del Ecuador (Fuerza Terrestre, Fuerza Naval y Fuerza Aérea) operan en coordinación armónica, buscando sinergias operativas y mayor eficacia.

Coordinación Interinstitucional:

En el ámbito de operaciones de índole interna, las OMEU deben forjar vínculos estrechos con otras instituciones del Estado, especialmente la Policía Nacional. Esta cooperación es crucial para garantizar la seguridad de la población y evitar la duplicidad de esfuerzos.

Interoperabilidad

La interoperabilidad, elemento vital, impulsa la efectividad de las operaciones conjuntas y la coordinación interinstitucional. Se hace imperativo establecer protocolos y procedimientos uniformes y, cuando sea necesario, mantener la interoperabilidad con otras instituciones gubernamentales.

Protección de la Población Civil

Las OMEU deben imperativamente incluir medidas para resguardar a la población civil, minimizando el daño colateral y evitando cualquier violación de los derechos humanos. La protección de la población es una responsabilidad ineludible.

Apoyo a Otras Instituciones del Estado

En situaciones de emergencia, como desastres naturales, las Fuerzas Armadas del Ecuador deben brindar apoyo a otras instituciones del Estado, garantizando la seguridad de la población y protegiendo los intereses nacionales.

Inteligencia militar

El componente de inteligencia militar asume una importancia central en las OMEU. La obtención, análisis y procesamiento de información habilitan la toma de decisiones más informadas y eficaces. La cooperación y coordinación entre fuerzas y organismos involucrados se erige como un requisito ineludible. El desarrollo de capacidades en tecnologías de información y ciberseguridad es esencial para resguardar la confidencialidad de la información.

Gestión de la Información

La gestión efectiva de la información emerge como un elemento clave en la realización de operaciones militares en entornos urbanos. Facilita el conocimiento situacional y la coordinación de las fuerzas. Se hace imperativo contar con sistemas de información integrados y personal altamente capacitado.

Seguridad de la Información

La seguridad de la información adquiere un peso crucial en las OMEU para salvaguardar datos sensibles y evitar la exposición a fuerzas enemigas o terceros no autorizados. Políticas y procedimientos sólidos, junto con tecnologías seguras, son elementos fundamentales en esta ecuación.

Doctrina para las Operaciones Militares Multidominio en entornos aéreos de las Fuerzas Armadas del Ecuador

La doctrina para las Operaciones Militares Multidominio en entornos aéreos de las Fuerzas Armadas del Ecuador constituye un componente esencial en la salvaguardia de la soberanía y la seguridad nacional de nuestra nación. Estas operaciones revisten una importancia primordial al posibilitar la ágil y eficaz movilización de nuestras fuerzas y la distribución de recursos en regiones de complicado acceso geográfico. El éxito en este empeño radica en la cooperación y coordinación sinérgica entre las tres ramas de las Fuerzas Armadas, a saber, el Ejército, la Armada y la Fuerza Aérea, así como su colaboración con la Policía Nacional, en una sinfonía de interoperabilidad, inteligencia, y gestión de información.

Objetivos de las Operaciones Militares Multidominio en entornos aéreos

- Garantizar la soberanía y la integridad territorial del Ecuador.
- Proteger a la población civil y sus bienes en situaciones de conflicto y desastres naturales.
- Contribuir a la seguridad ciudadana y el mantenimiento del orden interno.
- Apoyar a otras instituciones del Estado en situaciones de emergencia y catástrofes naturales.
- Desarrollar capacidades y tecnologías acordes con los avances científicos y tecnológicos para enfrentar las nuevas amenazas.

Características de las Operaciones Militares Multidominio en entornos aéreos

Las características de las Operaciones Militares Multidominio en entornos aéreos nos ilustran su complejidad y sus demandas. Son operaciones de carácter conjunto, donde la colaboración entre las tres ramas de las Fuerzas Armadas y la Policía Nacional se convierte en imperativo. Asimismo, exigen la utilización de equipamiento y tecnologías de punta para la movilización y transporte en entornos aéreos desafiantes. Requieren, por tanto, un meticuloso entrenamiento y capacitación del personal militar y policial involucrado, una planificación minuciosa y una coordinación eficiente entre todas las instituciones partícipes. Debido a la naturaleza cambiante de estos escenarios, la gestión de información se erige como elemento esencial para el éxito de las operaciones.

- Son operaciones conjuntas entre las tres ramas de las Fuerzas Armadas y con la Policía Nacional.
- Requieren la utilización de equipos y tecnologías avanzadas para la movilización y el transporte en entornos aéreos.
- Requieren de un adecuado entrenamiento y capacitación para el personal militar y policial involucrado.

- Exigen una planificación rigurosa y una adecuada coordinación entre las instituciones involucradas.
- Se realizan en contextos de incertidumbre y variabilidad, por lo que es necesario contar con una gestión de la información adecuada y eficiente.

Fases de las Operaciones Militares Multidominio en entornos aéreos

Las fases de las Operaciones Militares Multidominio en entornos aéreos, a saber, planificación, preparación, ejecución y evaluación, delinean un ciclo indispensable para la ejecución efectiva de estas operaciones. La planificación estratégica y táctica, la formación y adiestramiento de las fuerzas involucradas, el despliegue y la protección de la población civil, y la evaluación constante de las acciones llevadas a cabo, convergen en un proceso sinérgico y continuo.

- **Fase de planificación:** en esta fase se realiza la planificación estratégica y táctica de la operación, se determinan los recursos necesarios y se establecen los objetivos y metas.
- **Fase de preparación:** en esta fase se realiza el entrenamiento y capacitación del personal militar y policial involucrado, se preparan los equipos y materiales necesarios y se realiza la coordinación interinstitucional.
- **Fase de ejecución:** en esta fase se lleva a cabo la operación propiamente dicha, se realiza el transporte y movilización de las tropas, materiales y equipos, y se protege a la población civil en caso de ser necesario.
- **Fase de evaluación:** en esta fase se realiza una evaluación exhaustiva de la operación, se identifican los errores y aciertos, y se establecen las lecciones aprendidas para mejorar en futuras operaciones.

Importancia de la Aviación del Ejército en las Operaciones Militares en entornos aéreos multidominio

La aviación del ejército es una de las ramas más importantes de las Fuerzas Armadas del Ecuador y juega un papel fundamental en las operaciones militares tanto en el ámbito interno como en las operaciones de frontera. La aviación del ejército se encarga del transporte de tropas y suministros, el apoyo logístico y la vigilancia aérea. Además, cuenta con una gran experiencia en la lucha contra el narcotráfico y el terrorismo, lo que la convierte en un recurso estratégico para el país.

En este sentido, la doctrina para las operaciones militares multidominio en entornos aéreos debe considerar la importancia de la aviación del ejército y establecer las directrices para su empleo en el marco de las operaciones conjuntas con las otras ramas de las Fuerzas Armadas y la Policía Nacional. También es necesario que se establezcan procedimientos de coordinación para garantizar la interoperabilidad de las diferentes plataformas aéreas y la gestión de la información en tiempo real.

De igual manera, la doctrina debe considerar el desarrollo de nuevas capacidades y tecnologías para la aviación del ejército, como la utilización de drones y otras aeronaves no tripuladas, que pueden ser utilizadas para misiones de vigilancia y reconocimiento.

También es importante tener en cuenta la necesidad de capacitar y entrenar adecuadamente al personal de la aviación del ejército, para garantizar su eficacia y seguridad en las operaciones militares.

Por tanto, la doctrina para las Operaciones Militares Multidominio en entornos aéreos debe encarar la importancia de la Aviación del Ejército y fijar las directrices para su integración efectiva en operaciones conjuntas. La coordinación y interoperabilidad de las distintas plataformas aéreas, así como la gestión de información en tiempo real, se convierten en imperativos. La adopción de tecnologías emergentes, como drones y aeronaves no tripuladas, debe ser contemplada para misiones de vigilancia y reconocimiento. Por último, no podemos soslayar la necesidad de un adiestramiento y capacitación rigurosos para el personal de la Aviación del Ejército, garantizando su eficacia y seguridad en las operaciones militares.

Doctrina para las Operaciones Militares Multidominio en entornos marítimos de las Fuerzas Armadas del Ecuador

Objetivo

Las operaciones marítimas son aquellas que se realizan en el medio acuático, tanto en aguas territoriales como en aguas internacionales, con el objetivo de proteger los intereses nacionales, garantizar la seguridad en el mar y contribuir al mantenimiento de la paz y la estabilidad regional. Las operaciones marítimas pueden ser llevadas a cabo por las tres ramas de las Fuerzas Armadas del Ecuador en coordinación con otras instituciones del Estado, y su interoperabilidad es fundamental para el éxito de las misiones.

Principios de las operaciones multidominio marítimas

Las operaciones marítimas se deben llevar a cabo con los siguientes principios en mente:

Unidad de mando: Las operaciones marítimas deben ser dirigidas por una autoridad única y claramente definida.

Cooperación y coordinación: Las operaciones marítimas deben ser llevadas a cabo en colaboración con otras instituciones del Estado y organismos internacionales para garantizar la eficacia en la respuesta a las amenazas y desafíos marítimos.

Seguridad: Las operaciones marítimas deben ser llevadas a cabo con un enfoque en la seguridad de las fuerzas involucradas y de la población civil.

Flexibilidad: Las operaciones marítimas deben ser capaces de adaptarse rápidamente a situaciones cambiantes.

Sorpresa: Las operaciones marítimas deben ser planeadas y ejecutadas de manera que sorprendan al enemigo o a los actores no estatales que puedan amenazar los intereses nacionales.

Funciones de las operaciones marítimas:

Las operaciones marítimas tienen las siguientes funciones

- **Control y vigilancia del espacio marítimo:** Esta función se refiere a la detección y seguimiento de embarcaciones y aeronaves en el mar, así como a la inspección de buques para garantizar el cumplimiento de las normas y reglamentos internacionales.
- **Protección y seguridad marítima:** Esta función se refiere a la protección de las infraestructuras marítimas, así como a la prevención y respuesta a los actos de piratería, terrorismo y otros delitos transnacionales en el mar.
- **Apoyo a las operaciones de la Armada:** Esta función se refiere a la prestación de apoyo logístico y de transporte a las operaciones de la Armada en el mar, incluyendo la transferencia de personal y material entre buques.
- **Ayuda humanitaria y respuesta a desastres:** Esta función se refiere a la participación en operaciones de búsqueda y rescate, evacuación de civiles en peligro y ayuda humanitaria en el mar.
- **Inteligencia marítima:** La inteligencia marítima es esencial para el éxito de las operaciones marítimas. La recopilación, análisis y difusión de información sobre las actividades marítimas de los actores nacionales e internacionales es crítica para la toma de decisiones. La inteligencia marítima se puede obtener a través de diferentes fuentes, como la vigilancia aérea y marítima, el análisis de imágenes y la cooperación internacional.
- **Gestión de la información:** La gestión de la información es vital en las operaciones militares en entornos marítimos, ya que permite a los comandantes y al personal tomar decisiones informadas en tiempo real. La recopilación, análisis y distribución de información debe ser precisa, oportuna y segura. Los recursos tecnológicos de información y comunicaciones deben ser eficientes y

contar con medidas de protección de la información sensible. La seguridad de la información es crucial para prevenir la divulgación no autorizada de información clasificada y garantizar la confidencialidad de las operaciones.

- **Interoperabilidad:** La interoperabilidad es esencial para garantizar la cooperación y coordinación efectiva entre las diferentes ramas de las Fuerzas Armadas y otras instituciones del Estado. La interoperabilidad se logra mediante la estandarización de los procedimientos y protocolos de comunicaciones, el uso de sistemas de información comunes, la integración de equipos y la formación conjunta y el adiestramiento. La interoperabilidad debe incluir la capacidad de trabajar con fuerzas aliadas y organizaciones internacionales, lo que garantiza la capacidad de las Fuerzas Armadas para contribuir a la seguridad y defensa de la región.

La doctrina para operaciones militares multidominio en entornos marítimos debe garantizar la coordinación y colaboración entre las diferentes ramas de las Fuerzas Armadas y otras instituciones del Estado, la interoperabilidad, la inteligencia militar, la gestión de la información y la seguridad de la información.

Doctrina para las Operaciones Militares Multidominio para el ciberespacio de las Fuerzas Armadas del Ecuador

Las operaciones en el ciberespacio se han vuelto cada vez más importantes en el entorno militar actual. La capacidad de los adversarios para interrumpir las operaciones, dañar sistemas y obtener información sensible a través de actividades cibernéticas hostiles ha llevado a la necesidad de desarrollar una doctrina militar para operaciones en este entorno. Esta doctrina busca proporcionar una guía para la planificación, conducción y ejecución de

operaciones militares en el ciberespacio, en coordinación con las operaciones en otros dominios y la colaboración con otras instituciones del Estado.

Conceptos clave

Ciberespacio: Es el medio que se usa para almacenar, procesar y transmitir información a través de redes informáticas, sistemas y dispositivos interconectados.

Operaciones cibernéticas: Son aquellas acciones destinadas a proteger, explotar, negar, interrumpir, degradar o destruir los sistemas de información del adversario y/o para asegurar la información propia.

Ciberseguridad: Es la capacidad de proteger los sistemas informáticos, las redes y la información contra accesos no autorizados, uso, divulgación, interrupción, modificación o destrucción.

Interoperabilidad: La capacidad de interactuar, operar y compartir información entre diferentes sistemas, unidades o fuerzas.

Principios básicos

- La operación en el ciberespacio se considera una operación militar y se planifica, prepara, ejecuta y evalúa como tal.
- Las operaciones en el ciberespacio deben ser coordinadas con las operaciones en otros dominios y otras instituciones del Estado.
- Las operaciones en el ciberespacio requieren un enfoque de seguridad integral que incluya la protección de la información, los sistemas y las redes, y la preparación para responder a incidentes de seguridad cibernética.
- La interoperabilidad entre las Fuerzas Armadas y otras instituciones es esencial para el éxito de las operaciones en el ciberespacio.

- La inteligencia cibernética es fundamental para la planificación y ejecución de operaciones en el ciberespacio.

Objetivos de las operaciones cibernéticas:

- Proteger la información y los sistemas críticos.
- Explotar la información del adversario.
- Negar, interrumpir, degradar o destruir los sistemas de información del adversario.
- Asegurar la información propia.

Fases de las operaciones cibernéticas:

- Planificación: Identificación de objetivos, análisis de vulnerabilidades, identificación de recursos y establecimiento de objetivos de efectos.
- Preparación: Selección y entrenamiento de personal, establecimiento de infraestructura y recursos, y desarrollo de herramientas y técnicas.
- Ejecución: Conducción de operaciones y monitoreo de resultados.
- Evaluación: Evaluación de efectividad, identificación de mejoras y actualización de recursos y técnicas.

Responsabilidades y roles

- Las Fuerzas Armadas del Ecuador, en coordinación con otras instituciones del Estado, deben garantizar la protección de las infraestructuras críticas y los sistemas de información y comunicaciones en el ciberespacio.
- Las Fuerzas Armadas del Ecuador deben contar con capacidades para la identificación temprana y la respuesta rápida a amenazas en el ciberespacio, en coordinación con otras instituciones del Estado y los sectores privado y académico.

- La responsabilidad de la defensa en el ciberespacio debe ser compartida entre las diferentes ramas de las Fuerzas Armadas, y su gestión debe estar centralizada en una unidad especializada en ciberdefensa.
- Las Fuerzas Armadas del Ecuador deben contar con programas de formación y entrenamiento en ciberdefensa para garantizar la preparación del personal militar en este ámbito.
- Las Fuerzas Armadas del Ecuador deben establecer alianzas estratégicas con otros países y organizaciones internacionales en materia de ciberdefensa, con el fin de compartir información y recursos y mejorar la capacidad de respuesta ante amenazas en el ciberespacio.

La doctrina general para las operaciones militares en el ciberespacio para las Fuerzas Armadas del Ecuador debe estar enfocada en la protección de los intereses y la soberanía del país en este ámbito, mediante la coordinación y cooperación entre las diferentes ramas de las Fuerzas Armadas, la Policía Nacional y otras instituciones del Estado, así como con el sector privado y académico. Además, es importante la interoperabilidad, la inteligencia y la gestión de la información para garantizar una respuesta rápida y efectiva ante amenazas en el ciberespacio.

Mecanismos para la implementación de la propuesta doctrinaria

La efectiva implementación de una propuesta doctrinaria es fundamental para el fortalecimiento y la adaptación de cualquier entidad o institución a los desafíos cambiantes del entorno. En este contexto, se exploran y analizan los "Mecanismos para la Implementación de la Propuesta Doctrinaria", un proceso crucial que implica una planificación cuidadosa, coordinación eficiente y la adaptación constante para garantizar el éxito y la relevancia de la doctrina propuesta. A continuación, se examinan detalladamente los elementos clave que

permiten traducir una propuesta doctrinaria en acción efectiva, con un enfoque particular en su aplicación doctrinaria.

Tabla 12

Mecanismos de implementación

Etapa	Descripción del Proceso
Evaluación de Capacidades Militares	Realizar una evaluación exhaustiva de las capacidades militares actuales de las Fuerzas Armadas del Ecuador, identificando fortalezas y debilidades relacionadas con operaciones multidominio.
Plan de Implementación	Desarrollar un plan de implementación con objetivos claros, plazos y recursos necesarios, alineados con las políticas de seguridad y defensa del Estado y las capacidades técnicas y humanas de las Fuerzas Armadas.
Fases de Implementación	Establecer fases de implementación gradual y progresiva para permitir a las Fuerzas Armadas desarrollar nuevas capacidades y entrenamiento especializado en operaciones multidominio.
Actualización de Planes y Estrategias	Actualizar los planes y estrategias de defensa del país para garantizar la coherencia y complementariedad con la nueva doctrina multidominio.
Mecanismos de Monitoreo y Evaluación	Establecer mecanismos de monitoreo y evaluación para medir el impacto y la eficacia de la nueva doctrina en la seguridad y defensa del Estado.
Coherencia con el Marco Legal	Garantizar que la implementación de la nueva doctrina sea coherente con la Constitución y las leyes de la República del Ecuador, respetando los derechos humanos y la soberanía del país.

Nota. Los mecanismos de implementación de la propuesta son el resultado del análisis de las estrategias planteados por la propuesta y la investigación previa.

La implementación de esta propuesta requerirá una gestión cuidadosa y un compromiso continuo con la adaptación y mejora de las capacidades militares en un entorno estratégico en constante cambio.

Validación de la propuesta

La validación de la propuesta doctrinaria de operaciones multidominio en las Fuerzas Armadas del Ecuador se sustenta en un análisis FODA, que ofrece un marco analítico integral para evaluar su viabilidad y potencial impacto. A continuación, se profundiza en este análisis, destacando los aspectos cruciales en cada categoría.

Tabla 13

Cuadro resumen análisis FODA de la propuesta

Fortalezas	Oportunidades
- Investigación Rigurosa	- Enfrentar Nuevas Amenazas
- Adaptación a la Realidad Local	- Coordinación Reforzada
- Enfoque en Interoperabilidad e Inteligencia	- Mejora de la Imagen Institucional
Debilidades	Amenazas
- Inversión Significativa	- Falta de Recursos
- Resistencia al Cambio	- Presencia de Grupos Ilegales
- Limitación de Recursos	- Posibles Desvíos de Recursos

Nota. El resumen del FODA corresponde a la validación de la propuesta en todo su contexto

Fortalezas:

- **Investigación Rigurosa:** La base de la propuesta reside en una investigación minuciosa y actualizada sobre las operaciones multidominio empleadas en el conflicto Rusia-Ucrania. Esta sólida base proporciona una comprensión profunda de estas operaciones y su relevancia en la doctrina militar.

- **Adaptación a la Realidad Local:** La propuesta se ajusta a las realidades y necesidades específicas de las Fuerzas Armadas del Ecuador. Esto abre la puerta al desarrollo de nuevas capacidades y a la modernización de la doctrina militar, alineándola con las amenazas contemporáneas.
- **Enfoque en Interoperabilidad e Inteligencia:** La propuesta reconoce la importancia crucial de la interoperabilidad, la inteligencia y la gestión de la información, elementos esenciales para el éxito de las operaciones multidominio.

Oportunidades:

- **Enfrentar Nuevas Amenazas:** La implementación de la propuesta podría fortalecer la capacidad de las FFAA del Ecuador para abordar amenazas emergentes, incluyendo operaciones asimétricas y ciberdefensa, en consonancia con los desafíos del siglo XXI.
- **Coordinación Reforzada:** La propuesta puede contribuir a mejorar la coordinación entre las distintas ramas de las FFAA y otras instituciones del Estado, promoviendo una respuesta más eficaz en materia de defensa y seguridad nacional.
- **Mejora de la Imagen Institucional:** La adopción de la propuesta podría elevar la imagen y reputación de las FFAA del Ecuador como una institución moderna y eficiente, lo que podría generar un mayor respaldo tanto a nivel nacional como internacional.

Debilidades:

- **Inversión Significativa:** La implementación de la propuesta podría demandar una inversión sustancial en tecnología y capacitación para el personal militar, lo que podría generar altos costos y enfrentar resistencias por parte de sectores políticos o sociales.

- Resistencia al Cambio: La reluctancia al cambio en algunas facciones de las FFAA y la falta de voluntad política para llevar a cabo reformas podrían obstaculizar la ejecución efectiva de la propuesta.
- Limitación de Recursos: La falta de recursos y presupuesto para la implementación y mantenimiento de las nuevas capacidades podría limitar la efectividad de la propuesta, generando desafíos operativos.

Amenazas:

- Falta de Recursos: La insuficiencia de recursos y presupuesto podría llevar al fracaso de la implementación de la propuesta y afectar negativamente la percepción de las FFAA del Ecuador.
- Presencia de Grupos Ilegales: La presencia de grupos armados ilegales y la inseguridad en ciertas regiones del país podrían dificultar la efectiva implementación de la propuesta.
- Posibles Desvíos de Recursos: La eventualidad de conflictos internacionales o desastres naturales podría desviar los recursos y la atención de las FFAA del Ecuador de la implementación exitosa de la propuesta.

El análisis FODA arroja una luz positiva sobre la propuesta doctrinaria de operaciones multidominio en el contexto de las FFAA del Ecuador. Este enfoque estratégico ofrece un potencial sustancial para fortalecer la capacidad de defensa y seguridad del país, alineándose con las demandas del entorno estratégico actual.

En este contexto de investigación, se ha identificado que las fortalezas de esta propuesta radican en su capacidad para abordar amenazas no convencionales y su enfoque multidimensional que permite una respuesta más eficaz a los desafíos contemporáneos. Además, ofrece oportunidades para mejorar la coordinación interinstitucional y la interoperabilidad entre las diferentes ramas de las FFAA y la Policía Nacional.

Sin embargo, es crucial reconocer que la implementación efectiva de esta doctrina multidominio no será sin sus desafíos. Requerirá un compromiso financiero significativo por parte del Estado ecuatoriano para modernizar las capacidades militares y proporcionar el equipamiento necesario. Además, se necesitará una voluntad política firme para superar posibles resistencias internas y garantizar el respaldo necesario para llevar a cabo los cambios requeridos.

La gestión cuidadosa de los recursos también será esencial en un entorno de seguridad que presenta múltiples desafíos, incluyendo amenazas transnacionales como el narcotráfico y el crimen organizado. La asignación eficiente de recursos y una planificación estratégica sólida serán elementos críticos para el éxito de esta implementación.

Si bien el análisis FODA señala un potencial significativo en la propuesta doctrinaria de operaciones multidominio, su implementación requerirá un enfoque integral que aborde tanto las fortalezas como las debilidades. Esto implica un compromiso sostenido y una gestión estratégica de recursos para garantizar la eficacia y la relevancia de esta doctrina en la defensa y seguridad del Ecuador.

Capítulo V

Conclusiones y Recomendaciones

Conclusiones

Las operaciones multidominio son una estrategia de guerra que ha evolucionado a lo largo del tiempo, con el objetivo de lograr una ventaja competitiva en el campo de batalla mediante la coordinación de diferentes dominios, tales como tierra, aire, mar, ciberespacio y espacio.

La guerra Rusia-Ucrania ha sido un escenario en el que se han utilizado con éxito las operaciones multidominio, lo que ha permitido a Rusia alcanzar sus objetivos en el conflicto. Esto demuestra la importancia de esta estrategia en los conflictos actuales y futuros.

El análisis de las operaciones multidominio en la guerra Rusia-Ucrania ha permitido identificar los elementos clave de esta estrategia, tales como la integración de las capacidades de las diferentes ramas militares, la coordinación interagencial, la interoperabilidad y la gestión efectiva de la información.

La implementación de una propuesta doctrinaria de operaciones multidominio en las FFAA del Ecuador es necesaria para adaptarse a los nuevos desafíos y amenazas en el campo de batalla y mejorar la capacidad de respuesta de las Fuerzas Armadas.

La propuesta doctrinaria desarrollada para las FFAA del Ecuador debe considerar la necesidad de operaciones conjuntas con las tres ramas de las Fuerzas Armadas ecuatorianas, la coordinación con las operaciones coordinadas con la Policía Nacional y el apoyo que las FFAA dan a otras instituciones del estado, así como la necesidad de interoperabilidad, la inteligencia y la gestión de la información.

La implementación de una propuesta doctrinaria de operaciones multidominio es fundamental para mejorar la capacidad de respuesta de las FFAA del Ecuador y enfrentar con

éxito las nuevas amenazas y desafíos en el campo de batalla. La experiencia de la guerra Rusia-Ucrania ha demostrado la importancia de esta estrategia en los conflictos actuales y futuros, por lo que es necesario que las Fuerzas Armadas ecuatorianas adopten y desarrollen esta doctrina para mejorar su capacidad de defensa y seguridad del Estado ecuatoriano.

Recomendaciones

Las Fuerzas Armadas del Ecuador deben incluir en su doctrina militar las operaciones multidominio, ya que este enfoque permite una mayor eficacia en la conducción de las operaciones militares.

Es necesario desarrollar nuevas capacidades y tecnologías que permitan la implementación efectiva de las operaciones multidominio en el contexto ecuatoriano, teniendo en cuenta la diversidad geográfica y las amenazas actuales.

Se recomienda una mayor integración entre las Fuerzas Armadas y la Policía Nacional para garantizar la coordinación y colaboración efectiva en operaciones multidominio.

La inteligencia militar y la gestión de la información deben ser elementos clave en la planificación y ejecución de las operaciones multidominio, por lo que se debe fortalecer la capacitación en estas áreas.

Es fundamental garantizar la interoperabilidad entre las tres ramas de las Fuerzas Armadas ecuatorianas para permitir una colaboración efectiva y una coordinación adecuada en la ejecución de operaciones multidominio.

Bibliografía

- Barro, A. (2022). En el sur de Ucrania, los rusos no se enfrentan a contraofensivas, sino a una insurgencia. *El Confidencial*, en línea. Obtenido de https://www.elconfidencial.com/mundo/2022-05-30/guerra-rusia-ucrania-insurgencia-ucraniana-en-el-este_3433712/
- Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, 8-23.
- Battaglino, J. (2022). La guerra entre Rusia y Ucrania y sus implicancias para la defensa en América del Sur. *EGN*, 1-21. Obtenido de <https://revistadaegn.com.br/index.php/revistadaegn/article/download/1056/986>
- Blinder, D. (2021). Realismo y Relaciones Internacionales: una observación desde la historia de la ciencia y la epistemología. *Estudios internacionales*, 53(198), 119-137.
doi:<http://dx.doi.org/10.5354/0719-3769.2021.58346>
- Bolaños, I., Jiménez, A., & Noboa, M. (2022). Fuerza Aérea Ecuatoriana: En camino al multidominio. Un análisis transdisciplinario en complejidad. *Seguridad Operacional y Logística Aeronáutica*, 17(12), 1-13.
- CESEDEN. (2012). *Enfoque multidisciplinar en los conflictos híbridos*. Madrid: Ministerio de Defensa de España.
- Comando Conjunto de Fuerzas Armadas. (2016). *Fortalecimiento del Sistema de Inteligencia Militar 2010-2015*. Quito: MIDENA.
- Comando Conjunto de Fuerzas Armadas. (2019). *Plan Estratégico Institucional de las Fuerzas Armadas*. Quito: Ministerio de Defensa Nacional.

- Comando Conjunto de Fuerzas Armadas. (2019). *Planificación por capacidades militares*. Quito: Ministerio de Defensa Nacional.
- Comando Conjunto de Fuerzas Armadas. (2021). *Plan Estratégico de Fuerzas Armadas 2021-2025*. Quito: Ministerio de Defensa Nacional.
- Comando Conjunto de Fuerzas Armadas. (2021). *Transformación de Capacidades de Fuerzas Armadas*. Quito: MIDENA.
- Comando de Educación y Doctrina Militar Terrestre. (2020). *Manual Fundamental del Ejército. Sistemas Operativos del Campo de Batalla*. Quito: Comando de Educación y Doctrina Militar Terrestre.
- dela Herrán, A. (2011). Complejidad y transdisciplinariedad. *Formación Profesional. Skepsis*, 294-320.
- DW. (2022). El impacto de los drones ucranianos en la guerra de Rusia. *DW*. Obtenido de <https://www.dw.com/es/el-impacto-de-los-drones-ucranianos-en-la-guerra-de-rusia/a-64051757>
- Ecuador. (2008). *Constitución de la República del Ecuador*. Quito: Asamblea Nacional.
- Ecuador. (2018). *Constitución del Ecuador*. Obtenido de Asamblea Nacional del Ecuador: <https://educacion.gob.ec/wp-content/uploads/downloads/2012/08/Constitucion.pdf>
- Ecuador. (2019). *Ley de reforma a la Ley orgánica de Ciencia y tecnología e Innovación*. Quito: Semplades.
- Ejército Ecuatoriano. (2018). Reseña Histórica. *Revista del Ejército Ecuatoriano*. , 28-35.
- Fuerza Terrestre. (2022). *Plan de Gestión de la Fuerza Terrestre al año 2033*. Quito: Ministerio de Defensa.
- Gallardo, Y. (2020). Recolección de la información. En Y. Gallardo, & A. Moreno, *Aprende a Investigar*. (págs. 5-152). Bogotá: ARFO EDITORES.
- Gniesco, M. C. (2019). Operaciones multidominio. *12(1)*, 38-45.

- González, M. (2017). El Departamento de Defensa de los Estados Unidos y el uso de las capacidades basadas en Internet: ¿un nuevo campo de batalla? *UH*, 79-96.
- Hernández Sampieri, R. (2014). *Metodología de la Investigación*. México: Mc Graw Hill.
- Hernández, R. (2016). *Metodología de la Investigación*. Buenos Aires: Mc Graw Hill.
- IEEE. (2018). *Doctrina para el empleo de las FAS*. Madrid: Ministerio de Defensa de España.
- IEEE. (2018). La Guerra Híbrida. *Cuaderno de estrategia*, 35-65.
- Leiva, R., & Versalovic, B. (2020). Efectos de las operaciones. *Revista Ensayos Militares*, 57-80.
- Martínez, G. (2022). El enfrentamiento avanzado, las operaciones multidominio. *GLobal Strategy*, 2-16. Obtenido de <https://global-strategy.org/el-enfrentamiento-avanzado-las-operaciones-multidominio/>
- Ministerio de Defensa de España. (2020). *Nota conceptual. operaciones Multidominio*. Obtenido de Centro Conjunto de Desarrollo de Conceptos: https://emad.defensa.gob.es/Galerias/CCDC/files/OPERACIONES_MULTIDOMINIO.PDF
- Organizacion del Tratado del Atlántico Norte. (2019). *Amenazas Híbridas*. Bruselas: Organizacion del Tratado del Atlántico Norte.
- Oropesa, F. (2022). Panorama de la guerra entre Rusia y Ucrania. *Global Affairs and Strategy Studies*, 1-17.
- Paz, A. (2012). El conflicto híbrido una nueva forma de guerra. *Estudios internacionales*, 11-24.
- Perkins, D. (2018). Preparándonos para combatir hoy. Las Operaciones Multidominio y el Manual de Campaña 3-0. *Military Review*, 12-21.
- Revista de la Academia de Guerra del Ejército Ecuatoriano. (2019). Operaciones Multidominio. *Revista de la Academia de Guerra del Ejército Ecuatoriano*, 39-45.
- Tidy, J. (20 de 4 de 2023). *La otra guerra inclemente que libran Ucrania y Rusia*. Obtenido de BBC News Mundo: <https://www.bbc.com/mundo/noticias-internacional-65266795>

Tzu, S. (2015). *El Arte de la Guerra* . Barcelona: e-artnow.

U.S. Army. (2021). *The U.S. Army in Multi-Domain Operations 2028*. Washington: U.S. Army.

Vásquez, M. (2021). Doctrina y estructura militar ecuatoriana: de cara o de espaldas a las amenazas del siglo XXI. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, 109-121.