TRABAJO FINAL INTEGRADOR

Título: ““Las Operaciones de información en el nivel táctico (CTTO)””.

Que para acceder al título de Especialista en Conducción Superior de OOMMTT, presenta el Mayor MAURICIO RODRIGO GUERRERO.

Director de TFI: CN GASTON VALLEJOS

Ciudad Autónoma de Buenos Aires, de Febrero de 2025.

Resumen

El análisis de los conflictos ha evolucionado, dejando atrás el enfoque exclusivo en la guerra para adoptar una comprensión más amplia y profunda del entorno operacional, caracterizado por una constante transformación. Este cambio responde al avance científico, los desarrollos tecnológicos y la implementación de enfoques innovadores, que han generado un entorno operacional complejo compuesto por múltiples dimensiones: informativa, cognitiva, física y de datos.

El presente estudio propone el diseño de una organización específica dentro del Componente Terrestre del Teatro de Operaciones (CTTO), orientada a coordinar las Capacidades Relacionadas con la Información (CRI) en apoyo a las operaciones militares. Dicha organización estaría compuesta por especialistas en cada capacidad y contaría con un oficial de información integrado en el Estado Mayor del CTTO, quien tendría la responsabilidad de coordinar las CRI dentro de un plan de operaciones de información.

El objetivo principal de este trabajo es diseñar una estructura organizativa que se ajuste a las realidades operativas de las Fuerzas Armadas, considerando las leyes nacionales, doctrinas internacionales y lecciones históricas. Este enfoque busca influir en el entorno informativo del adversario, proteger el entorno informativo propio y contribuir al éxito del CTTO.

Palabras clave: Fuerzas Armadas, Operaciones de Información.

Tabla de contenidos

Introducción

"El arte supremo de la guerra es someter al enemigo sin luchar

SUN TZU"

Formulación del Problema

El problema central de esta investigación radica en la ausencia de un Órgano de Operaciones de Información (OOI) que permita coordinar e integrar de manera efectiva las capacidades relacionadas con la información, necesarias para garantizar un apoyo eficiente al Componente Terrestre del Teatro de Operaciones (CTTO) y contribuir al logro de sus objetivos operacionales.

Los aspectos para tratar en esta investigación incluyen:

1. **Identificación de Capacidades Clave:** Determinar las capacidades esenciales relacionadas con la información que son necesarias para respaldar las operaciones del CTTO. Esto incluirá la recopilación, análisis, difusión y protección de información relevante para la toma de decisiones.

2. **Análisis del Entorno Operacional:** Evaluar el ambiente operacional en el que el CTTO opera, considerando las amenazas, desafíos y dinámicas actuales. Esto permitirá ajustar las capacidades del OOI para adaptarse a las condiciones cambiantes.

3. **Diseño Organizativo:** Diseñar la estructura organizativa del OOI, definiendo roles, responsabilidades y relaciones con otras unidades dentro del CTTO. Esto garantizará una coordinación efectiva de las capacidades de información.

4. **Marco Legal y Doctrinario:** Analizar y establecer el sustento normativo y doctrinario para la creación y funcionamiento del Órgano de Operaciones de Información (OOI). Este marco debe contemplar las leyes nacionales, acuerdos internacionales y doctrinas militares aplicables, garantizando que la organización opere dentro de los principios legales y

estratégicos establecidos, alineada con las necesidades del Componente Terrestre del Teatro de Operaciones (CTTO).

5. **Integración Multidisciplinaria:** Incorporar especialistas en áreas clave como inteligencia, ciberseguridad, guerra de información y comunicaciones estratégicas, asegurando un enfoque integral y colaborativo que permita abordar de manera efectiva las múltiples dimensiones de las operaciones de información.

6. **Plan de Operaciones de Información:** Plan de Operaciones de Información: Diseñar un plan operativo que defina de manera detallada cómo el OOI apoyará al CTTO en el logro de sus objetivos operacionales, mediante el uso coordinado y efectivo de las capacidades relacionadas con la información. Este plan debe alinearse con las doctrinas militares y considerar las necesidades específicas del entorno operacional, esta investigación se enfoca en la creación de un OOI funcional y adaptado a las exigencias del CTTO, con el objetivo de fortalecer significativamente su capacidad para enfrentar las complejidades del entorno informativo y cumplir con éxito sus objetivos operativos.

¿Cuál es la mejor manera de diseñar y estructurar un Órgano de Operaciones de Información a nivel del Componente Terrestre del Teatro de Operaciones (CTTO) que coordine e integre eficazmente las capacidades relacionadas con la información, con el propósito de influir negativamente en la toma de decisiones del adversario y, al mismo tiempo, garantizar la protección sólida de nuestro propio entorno informativo?

Antecedentes y justificación de la investigación

Desde tiempos antiguos, el dominio del entorno informativo ha sido un factor decisivo en la guerra. Sun Tzu, en su obra El arte de la guerra, resalta: “Todo el arte de la guerra se basa en el engaño” y “el supremo arte de la guerra es someter al enemigo sin luchar” (2003, p. 8). Estas reflexiones destacan la importancia de influir en el adversario, debilitando su capacidad de decisión sin recurrir directamente a la fuerza.

En el contexto actual, caracterizado por una proliferación de medios de comunicación social y un acceso cada vez más amplio a fuentes de información, se vuelve imprescindible gestionar de manera adecuada este ámbito. Este manejo permite a las fuerzas militares no solo operar eficazmente en su entorno operativo, sino también obtener ventajas estratégicas significativas en un entorno regional e internacional (Biblio, 2017, p. 8).

Los avances tecnológicos en telecomunicaciones e informática han transformado los sistemas de comando y control (C2), impulsando cambios constantes en las estructuras organizativas, la doctrina vigente y los procesos de formación de los profesionales militares. Esto plantea nuevos desafíos, como la necesidad de reformular enfoques estratégicos y garantizar la protección y gestión de la información en un entorno de combate cada vez más complejo, donde la información es el recurso más valioso para la toma de decisiones (Galizia, 2013, p. 113).

Los sistemas de comando, control, comunicaciones, inteligencia, vigilancia y reconocimiento (C3I2) dependen de un flujo ininterrumpido de información, transportada, procesada y presentada de manera eficiente. Las tecnologías avanzadas aplicadas a estos sistemas son esenciales para dominar la batalla informativa, proporcionando una ventaja tecnológica y organizativa sobre el oponente. Esto implica abastecimiento continuo, procesamiento rápido y difusión estratégica, mientras se niega al adversario acceso a estos recursos. La guerra informativa, en este sentido, combina enfoques ofensivos y defensivos (Galizia, 2013).

El Ejército de los Estados Unidos ha adoptado una doctrina que integra capacidades relacionadas con la información en las operaciones militares, con el objetivo de influir, desestabilizar o incluso usurpar la toma de decisiones de los adversarios, al tiempo que protege las propias capacidades de decisión (Sheiffer, 2018). Esta doctrina enfatiza que ninguna unidad militar puede ignorar la necesidad de preparar el entorno informativo para alcanzar sus objetivos operacionales. La globalización y la urbanización han convertido los futuros campos de batalla en escenarios poblados, donde los adversarios combinan operaciones ciberespaciales, guerra electrónica y desinformación para desestabilizar la toma de decisiones de las fuerzas amigas (Sheiffer, 2018).

En este contexto, las operaciones de información (OI) dejan de ser un tipo específico de operación para convertirse en un esfuerzo coordinado que sincroniza herramientas y actividades en tres dimensiones del ciclo de decisión: cognitiva (mente), informativa (sistemas y datos) y física (infraestructura y líderes). Esta evolución subraya la necesidad de desarrollar capacidades integradoras que permitan influir en los oponentes, proteger el entorno propio y asegurar una ventaja operativa (Gómez Arriagada, 2015).

El entorno informativo contemporáneo se ha vuelto más complejo debido a los avances en tecnología, redes y bases de datos civiles y militares, que ofrecen vastas cantidades de información a los usuarios. Dominar este entorno permite a las fuerzas armadas lograr una ventaja operativa mientras se niegan estas capacidades al adversario (Santa Cruz, 2021).

La información se ha convertido en un componente primordial en los escenarios militares actuales, permitiendo influir, interrumpir o degradar las capacidades del adversario

en las dimensiones física, cognitiva e informativa. Esta situación exige un elemento integrador de capacidades relacionadas con la información que pueda influir en audiencias amigas, adversarias y neutrales, degradando la libertad de acción del oponente mientras protege las capacidades propias de toma de decisiones (Borges Da Silva, 2014).

Estados Unidos, pionero en esta área, ha desarrollado una doctrina que integra operaciones psicológicas, guerra electrónica, cibernética, inteligencia y comunicación social, adaptándose a los escenarios de conflicto presentes y futuros. Este enfoque enfatiza la necesidad de sincronizar capacidades técnicas y humanas para convertirlas en ventajas operativas en el campo de batalla (Borges Da Silva, 2014).

La información es un componente primordial en el escenario militar contemporáneo y una poderosa herramienta para influenciar, interrumpir o afectar la capacidad del adversario de tomar y compartir sus decisiones, sea en su dimensión física, humana o informacional. Por lo tanto, surge la necesidad de un elemento integrador de las capacidades relacionadas con la información, que reúna diversos caminos destinados a informar audiencias amigas, influenciar públicos adversarios y neutrales, y a desgastar la toma de decisiones de oponentes potenciales, degradando su libertad de acción, y al mismo tiempo, protegiendo el nuestro proceso de toma de decisiones. (Borges Da Silva, 2014)

En este contexto surgieron las Operaciones de Información (OI), como herramienta de apoyo a toma de las decisiones, por medio de la integración de diversas áreas, tales como: Comunicación Social, Operaciones de Apoyo a Información (Operaciones Psicológicas), Guerra Electrónica, Guerra Cibernética e Inteligencia. Los Estados Unidos de América (EEUU), en virtud de sus características bélicas y mediante el empleo de sus medios militares

actuales, fueron los primeros en detectar esta necesidad y crear una doctrina de empleo en esa área tan importante, que está íntimamente ligada a los escenarios de los conflictos presentes y futuros. (Borges Da Silva, 2014)

Objetivos

Para dar respuesta al problema que inició la investigación, se alcanzaron los siguientes objetivos:

Objetivo general

" Diseñar y establecer un Órgano de Operaciones de Información (OOI) destinado a proporcionar orientación y apoyo al comandante del Componente Terrestre del Teatro de Operaciones (CTTO) durante el proceso de toma de decisiones, asegurando la integración efectiva de las distintas capacidades relacionadas con la información en el marco de las operaciones de información"

Objetivos Particulares

Objetivo Particular Número Uno

" Analizar la doctrina vigente y las normativas legales aplicables para delimitar el ámbito de acción y las responsabilidades del Órgano de Operaciones de Información (OOI) en el contexto del Componente Terrestre del Teatro de Operaciones (CTTO)."

Objetivo Particular Número Dos

" Identificar y evaluar las capacidades relacionadas con la información esenciales que debe poseer el OOI, considerando las necesidades específicas del Ejército y los requisitos derivados de los escenarios operacionales actuales y futuros. "

Objetivo Particular Número Tres

"Diseñar un esquema estructural del OOI, definiendo roles, competencias y relaciones funcionales, con el propósito de garantizar un apoyo eficaz y coordinado al comandante del CTTO en la conducción de las operaciones de información."

Metodología Empleada

La investigación se desarrolló bajo un enfoque deductivo, partiendo de un objetivo general y tres objetivos específicos. Cada capítulo de la investigación fue diseñado para abordar uno o más de estos objetivos, lo que permitió obtener conclusiones parciales que contribuyeron de manera progresiva al cumplimiento de los objetivos específicos. Al finalizar, las conclusiones generales se estructuraron para responder directamente al objetivo general planteado.

El diseño de la investigación fue de tipo explicativo, con el propósito de profundizar en el conocimiento sobre el tema estudiado y responder a la pregunta de investigación. Este enfoque permitió identificar y analizar las relaciones entre los diferentes elementos involucrados, proporcionando una comprensión integral de la problemática.

Para validar los hallazgos, se emplearon las siguientes técnicas:

1. Análisis bibliográfico y documental:

Se realizó una revisión exhaustiva de la doctrina militar, normativas legales, documentos oficiales y literatura académica relacionada con el tema. Este análisis permitió establecer una base teórica sólida y un contexto claro para abordar la problemática planteada.

2. Análisis lógico:

Los elementos del estudio fueron desglosados y examinados de manera sistemática, lo que facilitó su comparación, interpretación y síntesis. Este proceso permitió estructurar argumentos claros y fundamentados, alineados con los objetivos de la investigación.

Capítulo I

Análisis de la Doctrina y Marco Legal de las Operaciones de Información en el Contexto Militar Actual"

"La suprema excelencia en la guerra es someter al enemigo sin luchar."

Sun Tzu

Propósito del Capítulo

Este capítulo tiene como propósito analizar y evaluar las doctrinas nacionales e internacionales relevantes en el ámbito de las operaciones de información, prestando especial atención a los marcos conceptuales y normativos adoptados por países líderes en este campo. Asimismo, se examinará la doctrina actualmente vigente en nuestras Fuerzas Armadas, con el objetivo de identificar los fundamentos operativos y tácticos que rigen estas operaciones.

Adicionalmente, se revisarán las normativas legales aplicables, tanto a nivel nacional como internacional, para determinar la existencia y suficiencia de un marco legal que respalde la propuesta de creación de un Órgano de Operaciones de Información (OOI). Este análisis busca establecer una base conceptual y legal sólida que sustente el diseño de la organización propuesta y garantice su alineación con las necesidades operativas y doctrinales del Componente Terrestre del Teatro de Operaciones (CTTO).

En síntesis, el capítulo contribuirá a la investigación proporcionando un marco doctrinario y normativo claro, que facilite la implementación efectiva de las operaciones de

información en el contexto militar actual y asegure su conformidad con los principios legales y tácticos.

Sección I: Análisis de la Doctrina en Contexto Internacional, Regional y Nacional

Esta sección examina las doctrinas de operaciones de información desarrolladas por países líderes, organizaciones internacionales y nuestra nación, con énfasis en su aplicación en el nivel táctico. El objetivo es identificar principios y prácticas que puedan integrarse en la propuesta del OOI para el CTTO

Estados Unidos:

La doctrina de operaciones de información de las Fuerzas Armadas de los Estados Unidos enfatiza la integración de capacidades relacionadas con la información en operaciones conjuntas y tácticas. Entre los elementos clave destacan:

Definición de Operaciones de Información: El reglamento establece una definición clara de operaciones de información como acciones planificadas para influir en la percepción, comprensión y comportamiento de las audiencias objetivo, en consonancia con los objetivos estratégicos.

Tres Pilares de las Operaciones de Información: Se enfatiza que las operaciones de información se basan en tres pilares fundamentales: las operaciones militares de información, las operaciones psicológicas y las operaciones cibernéticas.

Principios Fundamentales: El reglamento establece principios clave para la ejecución de operaciones de información, como la legalidad, la legitimidad, la proporcionalidad y la transparencia.

Planificación y Ejecución: Detalla los procesos de planificación y ejecución de operaciones de información, incluida la importancia de la coordinación interinstitucional y la evaluación de los resultados**.**

Operaciones Psicológicas: Explica la naturaleza de las operaciones psicológicas y su papel en las operaciones de información, incluida la influencia en las percepciones y comportamientos de las audiencias objetivo.

Operaciones Cibernéticas: Aborda las operaciones cibernéticas como parte integral de las operaciones de información, destacando la importancia de la ciberseguridad y la ciberdefensa.

Planificación Integrada: Promueve la planificación integrada de las operaciones de información con otras actividades militares y estratégicas.

Evaluación y Medición de Efectos: Destaca la necesidad de evaluar y medir los efectos de las operaciones de información para ajustar y mejorar la planificación y ejecución.

Coordinación con Organizaciones Aliadas y Agencias Gubernamentales: Reconoce la importancia de la coordinación con aliados y agencias gubernamentales en operaciones de información conjuntas e interinstitucionales.

Legalidad y Ética: Hace hincapié en la importancia de llevar a cabo operaciones de información de manera legal y ética, en consonancia con las leyes y normas internacionales.

Las capacidades relacionadas con la información son fundamentales en la doctrina militar de los Estados Unidos para las operaciones de información. A continuación, menciono y explico algunas de las principales capacidades relacionadas con la información utilizadas por la doctrina estadounidense:

Capacidades relacionadas con la información

Recopilación de Inteligencia: Esta capacidad implica la recopilación sistemática de información relevante de fuentes abiertas y clasificadas para comprender el entorno operativo y las amenazas. Incluye la vigilancia electrónica, el reconocimiento de señales, la obtención de inteligencia humana (HUMINT), la inteligencia de fuente abierta (OSINT), entre otros.

Ciberseguridad: La ciberseguridad es fundamental para proteger las redes y sistemas de información críticos contra ataques cibernéticos. Esto incluye medidas defensivas, como firewalls y sistemas de detección de intrusiones, así como capacidades ofensivas para contrarrestar amenazas cibernéticas.

Operaciones Psicológicas: Las operaciones psicológicas buscan influir en las percepciones, creencias y comportamientos de las audiencias objetivo. Pueden incluir campañas de información, propaganda y esfuerzos para desacreditar las narrativas adversarias.

Operaciones Cibernéticas: Las operaciones cibernéticas ofensivas se utilizan para interrumpir, degradar o destruir las capacidades adversarias en el ciberespacio. Esto puede incluir la explotación de vulnerabilidades y ataques cibernéticos.

Guerra Electrónica: La guerra electrónica implica la manipulación y el control del espectro electromagnético para interrumpir las comunicaciones y los sistemas electrónicos adversarios. Incluye la interferencia electrónica y la contramedida electrónica.

Guerra de Información: La guerra de información se refiere a la lucha por el control de la narrativa y la influencia en la opinión pública. Esto puede involucrar la difusión de información precisa y la desacreditación de la información falsa o engañosa.

Gestión de la Información: Esta capacidad implica la gestión efectiva de grandes volúmenes de datos e información para tomar decisiones informadas en tiempo real. Incluye la recopilación, procesamiento, análisis y distribución de información relevante.

Seguridad de la Información: Garantizar la seguridad de la información es crítico para proteger los datos sensibles y las comunicaciones. Esto incluye la criptografía, la autenticación y medidas para prevenir fugas de información.

Operaciones de Apoyo de Información: Estas operaciones incluyen el apoyo a la toma de decisiones a través de la entrega oportuna de información precisa a los comandantes y líderes militares.

Coordinación Interinstitucional: La capacidad de trabajar de manera efectiva con agencias gubernamentales, aliados y organizaciones internacionales en operaciones de información conjuntas e interinstitucionales.

Estas capacidades relacionadas con la información son fundamentales en la doctrina militar de los Estados Unidos para garantizar la superioridad de la información, influir en el entorno operativo y tomar decisiones informadas durante las operaciones militares. La combinación y aplicación efectiva de estas capacidades varía según el escenario y los objetivos específicos de una operación determinada.

Reino Unido:

Si bien el Reino Unido no ha hecho pública una doctrina específica de Operaciones de Información comparable al reglamento de las Fuerzas Armadas de los Estados Unidos, sin embargo, podemos considerar algunos de los temas vigentes en lase la doctrina vigente de la mencionada nación, que guardan relación con las operaciones de información:

Seguridad de la Información: La protección de la información sensible y la ciberseguridad son elementos clave en las operaciones de información del Reino Unido.

Coordinación Interinstitucional: Las operaciones de información a menudo involucran la coordinación con agencias gubernamentales y organizaciones civiles, como parte de un enfoque integral.

Operaciones Psicológicas: La influencia en las percepciones y opiniones de las audiencias objetivo es un componente importante de las operaciones de información del Reino Unido.

Ciberseguridad: La capacidad de llevar a cabo operaciones cibernéticas defensivas y ofensivas es un aspecto crítico de las operaciones de información.

Evaluación de Efectos: La evaluación y medición de los efectos de las operaciones de información son esenciales para evaluar la efectividad y hacer ajustes según sea necesario.

Ética y Legalidad: El Reino Unido y otras fuerzas armadas occidentales suelen llevar a cabo operaciones de información dentro de los límites legales y éticos, en consonancia con las leyes y normas internacionales.

Rusia:

Concepto de Guerra Híbrida: Rusia ha desarrollado el concepto de "guerra híbrida," que combina operaciones militares convencionales con elementos de influencia política, cibernética y de información.

Troleo en Línea y Desinformación: Rusia ha sido acusada de utilizar granjas de trolls y campañas de desinformación en línea para influir en la percepción pública y socavar la confianza en Occidente.

Ataques Cibernéticos: Rusia ha llevado a cabo ataques cibernéticos con fines políticos y militares, como se vio en su presunta participación en ataques cibernéticos contra países occidentales.

Coordinación Militar y de Inteligencia: Las operaciones de información en Rusia a menudo involucran una estrecha coordinación entre las fuerzas armadas y las agencias de inteligencia.

Es importante destacar que la doctrina de operaciones de información de estos países orientales puede cambiar con el tiempo y en respuesta a las circunstancias geopolíticas. Además, otros países orientales pueden tener enfoques y estrategias diferentes.

Brasil:

El documento (EB 20 – MC – 10.213) publicado en 2014 define la actividad como la implementación de un enfoque metodológicamente unificado. Este enfoque involucra una variedad de capacidades relacionadas con la información, junto con otros elementos, con el propósito de comunicar y ejercer influencia sobre grupos y personas. Al mismo tiempo, se busca afectar el proceso de toma de decisiones del adversario y proteger nuestros propios intereses. Además, estas capacidades deben ser diseñadas para prevenir, dificultar o neutralizar los efectos de las acciones adversas en el ámbito de la información. Esto implica un análisis exhaustivo del entorno de la información y las operaciones relacionadas con la misma.

Particularmente, el entorno operativo se presenta como altamente dinámico, con la creciente prominencia de grupos transnacionales o insurgentes, ya sea con o sin apoyo político o material de actores globales. Esta dinámica aumenta la naturaleza difusa de las amenazas que deben abordarse en el contexto de la defensa y la seguridad. En cuanto a las características doctrinarias principales, se reconoce que, en los entornos contemporáneos, es crucial que tanto la opinión pública nacional como la internacional respalden la aplicación de la fuerza. Se enfatiza la influencia significativa de la opinión pública en las operaciones militares actuales, dado que se concede gran importancia a la legitimidad de la causa, la cual se deriva de la legalidad basada en normativas jurídicas.

La doctrina también reconoce que las operaciones militares se desarrollan en entornos cada vez más humanizados, lo que los convierte en espacios congestionados y complejos. La presencia de la población civil y una amplia variedad de otros actores dificulta la identificación de los contendientes y aumenta la probabilidad de que colaboren en acciones militares.

España:

El documento sobre operaciones de información entró en vigor en el año 2006. Entre sus características más destacadas, se establece lo siguiente:

1. Naturaleza de las Operaciones de Información: Estas operaciones constituyen una de las actividades operativas conjuntas que se llevan a cabo normalmente en el teatro de operaciones. Se desarrollan de manera continua y sin perder de vista los detalles de la operación en curso. Están coordinadas y bajo el control del mando operacional. Dentro de la conducción de las operaciones, el proceso de toma de decisiones desempeña un papel fundamental. Para lograr la superioridad en la información, es necesario proteger el propio proceso de toma de decisiones mientras se influye en el proceso del adversario.

2. Planificación y Aplicación: Las operaciones de información se planifican a nivel estratégico-operacional, pero se aplican en todos los niveles. Su conducción se basa en normas de seguridad, doctrina y procedimientos diseñados para proteger la información. Además, se tiene en cuenta la orientación política y militar sobre posibles acciones destinadas a influir en la información.

3. Tipos de Operaciones de Información: La doctrina abarca principalmente dos tipos de operaciones de información:

- Operaciones Ofensivas: Estas operaciones tienen como objetivo influir directamente en la toma de decisiones de un potencial adversario. Incluyen tácticas como la decepción, operaciones psicológicas, guerra electrónica, destrucción física y ataques a las redes de sistemas de información, lo que les confiere un carácter ofensivo.
- Operaciones Defensivas: En contraste, las operaciones defensivas buscan impedir o minimizar la influencia del adversario en el proceso de toma de decisiones. Se centran en proteger y defender la

información y los sistemas de información mediante la aplicación de normas y procedimientos que garantizan esta finalidad. Las actividades fundamentales incluyen la seguridad de las operaciones (OPSEC), contrarrestar la decepción y la propaganda del adversario, la contrainteligencia y la guerra electrónica.

Esta doctrina establece un marco estratégico y operativo para las operaciones de información, reconociendo su importancia tanto en el ámbito ofensivo como defensivo en la defensa y seguridad del país.

Defensivas: busca impedir o minimizar la influencia del adversario en el proceso de toma de decisiones, buscando primordialmente proteger y defender la información y los sistemas de información mediante el empleo de normas y procedimientos que facilitan dicha finalidad. Las actividades fundamentales son: seguridad de las operaciones (OPSEC), acciones contra la decepción y propaganda del adversario, contrainteligencia y guerra electrónica.

La doctrina emplea componentes y capacidades de la información relacionadas

Seguridad de las operaciones OPSEC: proporciona seguridad a una operación militar, mediante medidas activas y pasivas, negándole al enemigo el conocimiento de dispositivos capacidades e intenciones.

Decepción: son medidas dirigidas a inducir al error al enemigo mediante la manipulación, deformación o falsificación de evidencias para hacerlo actuar de manera contradictoria a sus intereses.

Operaciones psicológicas: Las operaciones psicológicas son un conjunto de acciones planificadas y coordinadas diseñadas para influir en las percepciones, actitudes, creencias y comportamientos de individuos, grupos o audiencias específicas, con el propósito de alcanzar objetivos tácticos o militares. Estas acciones se implementan a través de la difusión de información, mensajes o actividades cuidadosamente diseñados para generar efectos

psicológicos deseables, tales como el apoyo a una causa, la desmoralización del enemigo, la obtención de cooperación o la mitigación de amenazas.

En el núcleo de las operaciones psicológicas se encuentra la comprensión profunda del comportamiento humano y la dinámica social, lo que permite diseñar estrategias altamente adaptativas y contextualmente relevantes. Estas operaciones pueden incluir propaganda, campañas de persuasión, desinformación, guerra psicológica y otras técnicas que influyen en la psicología y el comportamiento humano en escenarios de conflicto militar o estrategias de comunicación.

Una característica clave de las operaciones psicológicas es su capacidad para actuar como una fuerza invisible, capaz de moldear percepciones y decisiones sin recurrir directamente a la confrontación física. Esta naturaleza intangiblemente poderosa resalta la importancia de la ética y la legitimidad, ya que el impacto psicológico puede extenderse más allá de los objetivos inmediatos, afectando comunidades enteras y percepciones globales.

Por lo tanto, las operaciones psicológicas no solo representan una herramienta para alcanzar ventajas tácticas, sino que también son un reflejo de la interacción entre la mente humana y los conflictos modernos. Su eficacia radica en la precisión con la que se identifican las vulnerabilidades psicológicas del adversario y en la adaptabilidad para abordar las cambiantes dinámicas del entorno operativo.

Guerra electrónica: La guerra electrónica constituye una disciplina clave en los conflictos modernos, centrada en el dominio y explotación del espectro electromagnético para influir decisivamente en el desarrollo de operaciones militares. Este campo abarca el uso estratégico de tecnologías avanzadas para detectar, interrumpir, degradar o neutralizar las comunicaciones, sistemas de radar, navegación y otros dispositivos electrónicos empleados tanto por el adversario como por fuerzas amigas.

El objetivo principal de la guerra electrónica es doble: por un lado, negar al enemigo la capacidad de utilizar eficazmente su infraestructura electrónica para coordinar operaciones, recolectar inteligencia o asegurar su movilidad; por otro, proteger y optimizar el uso del espectro por parte de las propias fuerzas, asegurando la superioridad en este dominio crítico. Esto incluye medidas ofensivas, como interferencia y supresión electrónica, y defensivas, como blindaje y contramedidas adaptativas, que se combinan para generar una ventaja operativa integral.

Una característica distintiva de la guerra electrónica es su adaptabilidad a entornos dinámicos y su capacidad para operar en sinergia con otras capacidades, como la ciberseguridad y la inteligencia, lo que amplifica sus efectos en el campo de batalla moderno. Más allá de la simple interrupción tecnológica, esta disciplina puede influir profundamente en la percepción, decisión y respuesta del adversario, integrándose como un elemento esencial de las operaciones conjuntas.

En un entorno donde la tecnología evoluciona rápidamente, la guerra electrónica no solo busca interrumpir, sino también moldear el entorno electromagnético en favor de los objetivos tácticos y operacionales. Este enfoque transforma el espectro electromagnético en un terreno de combate intangible pero crítico, donde la superioridad se traduce en una ventaja estratégica y táctica que puede definir el resultado de cualquier enfrentamiento.

La guerra electrónica se divide generalmente en tres áreas principales:

1. **Guerra Electrónica Ofensiva (EW, por sus siglas en inglés):** Esta fase involucra acciones destinadas a atacar y perturbar los sistemas electrónicos del enemigo. Esto puede incluir el uso de interferencia electrónica, ataques cibernéticos, y la emisión de señales falsas para engañar o confundir al adversario.

2. **Guerra Electrónica Defensiva (EW):** Esta área se enfoca en la protección de las propias capacidades electrónicas contra ataques enemigos. Esto implica la implementación de medidas de seguridad cibernética, contramedidas electrónicas y la detección y neutralización de amenazas electrónicas entrantes.

3. **Guerra Electrónica de Apoyo (EW):** Aquí, se utilizan capacidades electrónicas para respaldar operaciones militares en curso, como la supresión de defensas aéreas enemigas o la protección de sistemas de comunicación y navegación propios.

En resumen, la guerra electrónica es un componente indispensable de las operaciones militares contemporáneas, diseñada para garantizar la superioridad en el espectro electromagnético. Esta disciplina se fundamenta en la capacidad de controlar, interferir y manipular tecnologías y sistemas electrónicos, ya sea para interrumpir las capacidades del adversario o para proteger las propias infraestructuras críticas en un entorno de alta tecnología.

Más que una herramienta de apoyo, la guerra electrónica se ha convertido en un elemento estratégico que puede definir el éxito o fracaso de las operaciones militares. A través de medidas ofensivas, como la supresión de comunicaciones enemigas o el engaño electrónico, y defensivas, como la implementación de contramedidas avanzadas, esta capacidad asegura que las fuerzas amigas mantengan una ventaja operativa decisiva.

Además, su versatilidad le permite integrarse con otras capacidades clave, como la ciberseguridad, la inteligencia y la vigilancia, generando un efecto multiplicador en el campo de batalla. Este enfoque sinérgico transforma al espectro electromagnético en un terreno de combate dinámico, donde la innovación tecnológica y la adaptabilidad táctica son esenciales para lograr los objetivos.

En un mundo donde la tecnología avanza a un ritmo sin precedentes, la guerra electrónica representa no solo una ventaja táctica, sino también una garantía de resiliencia operativa, capaz de redefinir los parámetros de la competencia militar moderna.

Destrucción física: consiste en dañar o neutralizar objetivos o recursos militares del enemigo mediante acciones directas, utilizando medios como ataques aéreos, terrestres o navales. El propósito es eliminar o incapacitar la capacidad operativa de dichos recursos, reduciendo así la efectividad del adversario en el campo de batalla. En los últimos años, el desarrollo de tecnologías avanzadas, como los sistemas de drones armados, ha transformado significativamente este tipo de operaciones.

Por ejemplo, los drones de combate han demostrado ser herramientas altamente efectivas en la destrucción física de objetivos estratégicos, como centros de mando, almacenes de municiones, vehículos blindados y sistemas de defensa aérea. Un caso destacado es el uso de drones Bayraktar TB2 en conflictos recientes, donde han neutralizado vehículos blindados y sistemas antiaéreos mediante ataques de precisión. Estos drones, equipados con armamento guiado por láser, no solo minimizan el riesgo para las fuerzas propias, sino que también permiten operar en entornos altamente defendidos gracias a su capacidad para evadir radares enemigos.

Otro ejemplo notable es el ataque de drones estadounidenses MQ-9 Reaper en Siria, donde estos vehículos destruyeron instalaciones logísticas y refugios de líderes insurgentes. Estos ataques precisos, realizados desde una distancia segura, permitieron eliminar amenazas clave sin la necesidad de exponer tropas terrestres.

Además, en el conflicto en Nagorno-Karabaj, el uso de drones por parte de Azerbaiyán marcó un hito en la guerra moderna. Los drones destruyeron artillería, tanques y sistemas de defensa antiaérea armenios, cambiando el equilibrio en el campo de batalla y

demostrando cómo la destrucción física mediante tecnologías no tripuladas puede redefinir los enfrentamientos militares.

Este enfoque no solo enfatiza la precisión y letalidad, sino que también permite un impacto estratégico al reducir colateralidades y garantizar una superioridad tecnológica y operativa. La destrucción física mediante drones, como parte de operaciones integradas, no solo representa un avance en la eficacia militar, sino que también redefine las dinámicas de los conflictos modernos, donde la tecnología juega un papel protagónico en el éxito de las misiones.

Cooperación cívica militar: La cooperación cívico-militar es una interacción estructurada y planificada entre las fuerzas armadas y la población civil, diseñada para abordar desafíos comunes que surgen en contextos de crisis, conflictos o desastres naturales. Este enfoque busca combinar recursos y capacidades tanto civiles como militares para alcanzar objetivos mutuos que promuevan la estabilidad, el desarrollo y la seguridad de una región.

En situaciones de conflicto, esta cooperación puede incluir actividades como la provisión de asistencia humanitaria a comunidades afectadas, la reconstrucción de infraestructura crítica dañada, y el restablecimiento de servicios esenciales en áreas devastadas. En escenarios de paz o postconflicto, puede abarcar programas de desarrollo comunitario, fortalecimiento de la gobernanza local y apoyo a la resiliencia social frente a futuras amenazas.

Un ejemplo actual de cooperación cívico-militar es la respuesta de las fuerzas armadas en Ucrania durante el conflicto en curso. En este contexto, los militares no solo participan en la defensa del territorio, sino que también colaboran con organizaciones civiles para evacuar a la población, distribuir ayuda humanitaria, reparar infraestructura crítica como hospitales y redes eléctricas, y garantizar la seguridad en regiones liberadas. Estas acciones

no solo mejoran la situación inmediata de la población, sino que también refuerzan la confianza entre las comunidades y las fuerzas armadas.

Otro caso reciente es la colaboración de las fuerzas armadas de diversos países durante la pandemia de COVID-19. En varios lugares, los militares trabajaron junto a autoridades civiles para establecer hospitales de campaña, distribuir suministros médicos y garantizar la logística de las campañas de vacunación. Este ejemplo ilustra cómo la cooperación cívico-militar trasciende el ámbito de los conflictos armados, extendiéndose a desafíos globales que requieren esfuerzos coordinados y multifacéticos.

Esta cooperación no solo fortalece la relación entre las fuerzas armadas y la población civil, sino que también asegura que los esfuerzos realizados sean percibidos como legítimos y alineados con las necesidades de la comunidad. Al integrar estrategias y recursos, la cooperación cívico-militar se convierte en un pilar fundamental para la estabilidad operativa en entornos complejos y multidimensionales.

Información pública: La información pública comprende datos, hechos y conocimientos que son accesibles para cualquier persona, sin restricciones legales o técnicas que limiten su consulta. Esta categoría abarca una amplia gama de contenidos, incluyendo documentos oficiales del gobierno, estadísticas, leyes, reportes institucionales, noticias, investigaciones académicas y cualquier otro material disponible para el uso y análisis de la sociedad en general.

La accesibilidad de la información pública desempeña un papel fundamental en la transparencia y la rendición de cuentas de las instituciones gubernamentales, así como en el fortalecimiento de la participación ciudadana. Al permitir que la sociedad acceda a información relevante, se fomenta una mejor comprensión de las políticas públicas, se promueve el control ciudadano y se refuerzan los principios democráticos.

En el ámbito militar, la información pública tiene implicaciones estratégicas y tácticas. Por ejemplo, los comunicados oficiales relacionados con operaciones militares pueden influir en la percepción de la población y los actores internacionales. Durante conflictos armados, la difusión de información pública confiable es crucial para contrarrestar la desinformación y garantizar que los mensajes lleguen de manera efectiva a las audiencias clave.

Un caso reciente que ejemplifica la importancia de la información pública es la gestión de la pandemia de COVID-19. Los gobiernos, organizaciones internacionales y agencias de salud pública utilizaron plataformas digitales y tradicionales para compartir datos relacionados con contagios, vacunas y medidas de prevención. Este acceso masivo a información permitió a las comunidades tomar decisiones informadas y generó un espacio para el debate y la colaboración en la resolución de la crisis.

La gestión responsable de la información pública implica equilibrar el acceso abierto con la protección de datos sensibles que puedan comprometer la seguridad nacional, la privacidad individual o intereses estratégicos. En este sentido, la información pública no solo es una herramienta para la difusión de conocimiento, sino también un componente clave en la construcción de confianza entre los gobiernos, las instituciones y la sociedad.

Operaciones en las redes de sistemas de información: Las operaciones en las redes de sistemas de información comprenden una serie de acciones planificadas y ejecutadas en entornos digitales, como internet, redes de comunicación o infraestructuras críticas, con el propósito de influir en el flujo de información, proteger sistemas propios o comprometer los sistemas del adversario. Estas operaciones abarcan un amplio espectro de actividades, desde ciberdefensa y ciberataques hasta manipulación de datos y gestión estratégica de la información.

En el contexto militar, estas operaciones desempeñan un papel crucial en la obtención y mantenimiento de la superioridad en el dominio informativo. Por ejemplo, las operaciones cibernéticas ofensivas pueden neutralizar redes de mando y control del adversario, deshabilitar sistemas de defensa o interrumpir la comunicación entre unidades enemigas. Al mismo tiempo, la defensa cibernética asegura la integridad de las redes propias, previniendo ataques que podrían comprometer información sensible o paralizar operaciones estratégicas.

Un ejemplo significativo es el uso de operaciones cibernéticas durante conflictos modernos, como los ciberataques dirigidos a infraestructuras críticas para desestabilizar al adversario. Casos recientes han demostrado cómo estas acciones pueden bloquear sistemas financieros, redes eléctricas y centros de datos, impactando tanto en el frente militar como en la vida cotidiana de la población civil.

Además de los aspectos ofensivos y defensivos, estas operaciones también incluyen la gestión y análisis de grandes volúmenes de datos, utilizando herramientas avanzadas de inteligencia artificial y aprendizaje automático para anticipar movimientos del adversario, identificar vulnerabilidades y optimizar las decisiones tácticas en tiempo real.

Las operaciones en las redes de sistemas de información representan un componente integral de las estrategias militares modernas, ya que el dominio digital es un terreno de combate dinámico donde la velocidad, la precisión y la innovación tecnológica son determinantes. Este enfoque exige una coordinación efectiva entre expertos técnicos y mandos operativos, asegurando que las capacidades cibernéticas se integren plenamente en las operaciones conjuntas para alcanzar los objetivos tácticos y estratégicos.

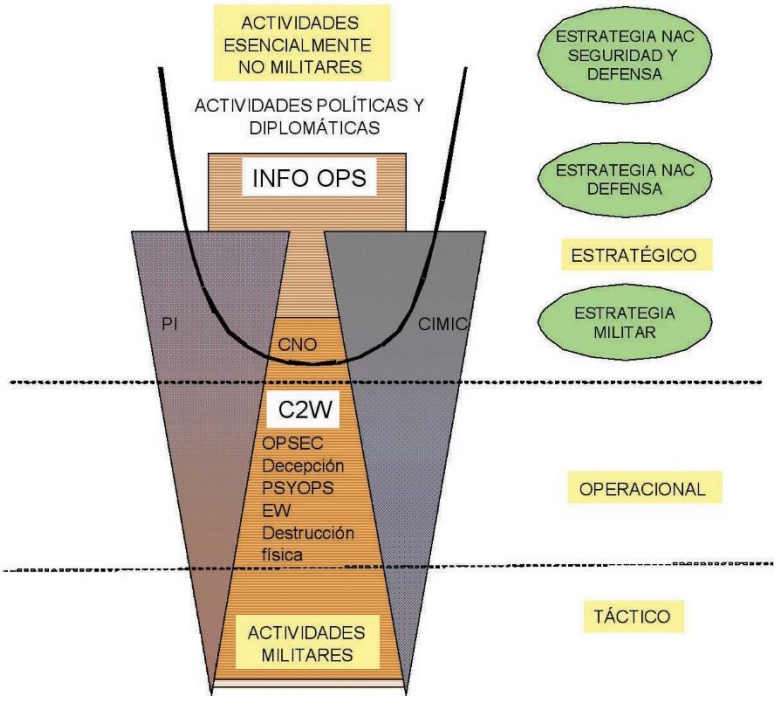


Figura 1: Integración de las actividades en los diferentes niveles de las operaciones de información.

Este gráfico muestra cómo las operaciones de información (INFO OPS) integran acciones políticas, diplomáticas y militares en distintos niveles. Desde estrategias nacionales hasta actividades tácticas, INFO OPS asegura la coordinación entre herramientas militares como guerra electrónica, operaciones psicológicas y destrucción física para alcanzar los objetivos estratégicos definidos por la seguridad y defensa nacional.

A continuación, se explican los elementos clave del gráfico de manera clara y sencilla:

Partes Principales del Gráfico:

Niveles Jerárquicos:

Estrategia Nacional de Seguridad y Defensa: Representa el nivel estratégico más alto, que abarca actividades esenciales no militares y políticas/diplomáticas. Aquí, las operaciones de información se integran con políticas de seguridad nacional.

Estrategia Nacional de Defensa y Militar: Se enfocan en cómo las fuerzas armadas implementan operaciones de información como parte de sus objetivos de defensa.

Niveles Operacional y Táctico: Es donde las actividades militares y las herramientas específicas de las operaciones de información se llevan a cabo directamente en el campo.

Actividades Relacionadas:

INFO OPS (Operaciones de Información): Actúa como un eje central que conecta actividades no militares, políticas y diplomáticas con las actividades militares, garantizando una sinergia entre todas las acciones.

Actividades Políticas y Diplomáticas: Incluyen acciones para influir en la percepción de aliados, oponentes y comunidades internacionales en contextos de conflicto o seguridad.

Actividades Militares: Estas se desarrollan en el nivel táctico y operacional e incluyen capacidades específicas como OPSEC (seguridad operativa), engaño, operaciones psicológicas (PSYOPS), guerra electrónica (EW) y destrucción física.

C2W (Command and Control Warfare):

Este es el componente táctico dentro de las operaciones de información. Agrupa capacidades específicas diseñadas para interrumpir la capacidad de mando y control del adversario:

OPSEC (Operaciones de Seguridad): Garantiza que la información crítica propia no sea accesible al enemigo.

Decepción: Manipula la percepción del adversario para que tome decisiones incorrectas.

PSYOPS: Influye en la moral y las decisiones de las fuerzas enemigas y audiencias específicas.

Guerra Electrónica (EW): Disruptiva en el espectro electromagnético para interferir en las comunicaciones y operaciones del adversario.

Destrucción Física: Ataca infraestructura clave para deshabilitar capacidades críticas.

Dimensiones del Impacto:

Las Actividades Esencialmente no Militares y Políticas/Diplomáticas actúan a niveles estratégicos para influir en audiencias amplias.

Las Actividades Militares y herramientas del C2W se concentran en objetivos tácticos y operativos, complementando las operaciones de información estratégicas.

NATO:

Doctrina de la OTAN para Operaciones de Información

La doctrina conjunta aliada para operaciones de información de 2009 establece los principios fundamentales que guían las acciones militares en el ámbito de la información, especialmente cuando se llevan a cabo operaciones en coaliciones multinacionales y fuerzas combinadas. Su enfoque central es garantizar la interoperabilidad, facilitando la integración entre aliados y otros actores durante la planificación, conducción y evaluación de operaciones.

Enfoque y Propósito de la Doctrina

La doctrina de la OTAN enfatiza que las operaciones de información (INFO OPS) son esenciales para alcanzar los objetivos militares en un entorno caracterizado por la evolución tecnológica, las sensibilidades políticas y la participación de actores no militares. Estas operaciones no son independientes, sino que se integran como parte fundamental en el proceso de selección de objetivos y en la planificación global de las campañas militares.

En particular, la doctrina destaca:

1- Un Enfoque Basado en Efectos:

Las operaciones de información no se limitan a acciones aisladas; buscan generar efectos sincronizados que influyan en el ciclo de toma de decisiones del adversario, tanto en el nivel estratégico como táctico. Este enfoque reemplaza la visión centrada en objetivos individuales, asegurando coherencia entre las actividades y maximizando el impacto en el campo de batalla.

2- La Información Operacional:

La información operacional, como función integral, combina medios letales y no letales para alcanzar los objetivos de la campaña. Su aplicación requiere una planificación meticulosa, especialmente en tres áreas interrelacionadas:

- **Influencia en las percepciones y actitudes del adversario:** A través de la manipulación de información y operaciones psicológicas, se busca debilitar la voluntad de lucha y distorsionar su capacidad de análisis y decisión.
- **Protección de la libertad de maniobra informativa de la Alianza:** Asegurando la defensa de los datos, redes y sistemas de información propios, fundamentales para el proceso de toma de decisiones.
- **Contrarrestar las capacidades de comando y control del enemigo:** Mediante acciones que afectan sus sistemas de inteligencia, vigilancia, adquisición de objetivos y armas, se limita significativamente su capacidad operativa.

Sensibilidad a Factores Políticos y Actores No Militares

La doctrina reconoce que el entorno de la información no es exclusivo del ámbito militar. Factores políticos, actores civiles, organizaciones no gubernamentales y la opinión pública juegan un papel determinante en la conducción de operaciones. Por ello, la sensibilidad y la adaptabilidad a estos elementos resultan fundamentales para asegurar el éxito y la legitimidad de las acciones.

La integración de capacidades militares y no militares permite generar sinergia operativa, evitando conflictos entre actividades y maximizando los efectos en el teatro de operaciones. Esta responsabilidad recae en el comandante, asistido por un jefe especializado en operaciones de información, quien se encarga de sincronizar todos los esfuerzos en la cadena de mando.

Aplicación en el Campo de Operaciones

La doctrina de la OTAN se enfoca principalmente en el nivel operativo, pero se aplica a todos los niveles de mando. Su implementación requiere el uso eficaz de tecnologías modernas y un enfoque innovador que permita:

- Mejorar la comprensión situacional del entorno informativo.
- Coordinar de manera efectiva acciones militares, políticas y civiles.
- Asegurar la coherencia en la planificación, ejecución y evaluación de las operaciones, garantizando que cada acción contribuya al objetivo general sin comprometer otras actividades.

La doctrina de la OTAN para operaciones de información establece un marco robusto y flexible que facilita la integración de capacidades en el entorno informativo. La clave de su éxito reside en la coordinación estrecha entre niveles de mando, la adaptación a factores políticos y no militares, y el uso combinado de medios letales y no letales. Este enfoque asegura la superioridad en el dominio informativo, permitiendo influir en el adversario, proteger los sistemas propios y alcanzar los objetivos operacionales con eficacia.

Argentina:

Guerra de la Información (GI) en el Contexto Militar Argentino

La Guerra de la Información (GI) es definida en el reglamento de Conducción para las Fuerzas Terrestres como una actividad estratégica que utiliza y gestiona la información para obtener una ventaja decisiva sobre el enemigo. Su alcance abarca un espectro amplio de acciones, desde la obtención y verificación de inteligencia táctica hasta la implementación de desinformación, con el propósito de influir y afectar la capacidad operativa del adversario.

Dimensiones de la Guerra de la Información

La GI no se limita a la recopilación de datos, sino que abarca múltiples dimensiones interrelacionadas:

Inteligencia Operacional: Proporciona una base confiable para la planificación y ejecución de las operaciones, asegurando la identificación y neutralización de amenazas en tiempo real.

Desinformación Estratégica: Busca confundir y desorientar al enemigo mediante la manipulación de información, afectando su toma de decisiones y su percepción del entorno operativo.

Protección Informativa: Garantiza la seguridad y confidencialidad de los sistemas de mando y control, previniendo la interferencia adversaria en las redes propias.

Comunicación Social Aplicativa al Combate (COSACO)

Dentro de las operaciones de GI, destaca la Comunicación Social Aplicativa al Combate (COSACO), concebida como una operación complementaria que reemplaza a las tradicionales Operaciones Psicológicas. COSACO se enfoca en técnicas y procedimientos de comunicación social destinados a asegurar la transmisión, recepción y correcta interpretación de mensajes críticos en el contexto operativo.

Objetivo: Contribuir directamente al cumplimiento de los objetivos tácticos y estratégicos de las fuerzas terrestres.

Características: COSACO incorpora elementos como la difusión de mensajes de cohesión para las tropas propias, campañas de influencia para ganar el apoyo de la población civil, y la contraprestación de propaganda enemiga.

Personal Especializado y Capacitado

La ejecución de la GI requiere de personal altamente capacitado, que actúe con precisión y conocimiento en áreas clave:

Organizaciones de Asuntos Civiles: Coordinan las relaciones con la población local para crear un entorno favorable a las operaciones militares.

Fuerzas Especiales (FFEE): Ejecutan misiones críticas que combinan inteligencia táctica y desinformación estratégica.

Elementos de Inteligencia: Analizan y procesan datos relevantes para anticipar movimientos del adversario.

Ingenieros y Comunicaciones: Apoyan mediante la construcción de redes seguras y la implementación de contramedidas electrónicas.

Marco Legal y Normativo

Es fundamental que las actividades de GI se desarrollen bajo un estricto cumplimiento de las normas legales nacionales e internacionales. Entre las regulaciones aplicables, destacan:

Constitución Nacional Argentina: Establece los límites y derechos fundamentales que deben ser respetados durante las operaciones informativas, garantizando el respeto por los derechos humanos y la privacidad.

Ley de Inteligencia Nacional (N.º 25.520): Define el marco para la recopilación y uso de información, prohibiendo actividades que vulneren los derechos civiles.

Tratados Internacionales: Incluyen compromisos en materia de derecho internacional humanitario, asegurando que las operaciones de GI no excedan los límites éticos y legales.

Sección II Análisis del Marco legal, nacional e internacional

En esta sección se analizan las principales leyes y normativas que sustentan la planificación y ejecución de las operaciones de información en las Fuerzas Armadas de la República Argentina. Este marco legal es esencial para garantizar que estas actividades se lleven a cabo en estricta concordancia con los principios constitucionales, el respeto a los derechos humanos y las normas internacionales.

Constitución Nacional Argentina

La Constitución Nacional establece los pilares fundamentales que regulan el empleo de las Fuerzas Armadas, asegurando su subordinación al poder civil y su operación dentro de los límites democráticos y legales. Algunas disposiciones clave incluyen:

Control Civil (Art. 21):

Las Fuerzas Armadas están subordinadas al gobierno civil, representado por el presidente y el Congreso. Esto asegura que las decisiones militares se tomen en un marco político y democrático.

Prohibición de Intervención en Asuntos Políticos (Art. 29):

Las Fuerzas Armadas no pueden involucrarse en actividades políticas internas ni influir en la toma de decisiones políticas.

Defensa Nacional (Art. 75, Inc. 25):

La participación en conflictos internacionales requiere la aprobación del Congreso, garantizando un control democrático sobre el uso de la fuerza fuera del territorio nacional.

Prohibición de Uso en Seguridad Interior (Art. 23):

Las Fuerzas Armadas no pueden intervenir en cuestiones de seguridad interna sin una declaración de estado de sitio por parte del Congreso. Esto asegura un uso limitado y supervisado de las capacidades militares en contextos internos.

Protección de los Derechos Humanos (Art. 18):

Todas las operaciones militares deben garantizar los derechos fundamentales, asegurando que ninguna actividad comprometa las garantías constitucionales de la población.

Ley de Defensa Nacional (Ley N.º 23.554)

La Ley de Defensa Nacional regula las actividades de las Fuerzas Armadas, estableciendo límites claros para preservar el orden democrático y la seguridad nacional:

Subordinación al Poder Civil:

Reafirma que las Fuerzas Armadas están bajo el control del Presidente y el Congreso, en línea con los principios constitucionales.

Restricción en Seguridad Interior:

Prohíbe el uso de las Fuerzas Armadas en cuestiones internas de orden público, excepto en casos de estado de sitio declarado por el Congreso.

Participación en Conflictos Internacionales:

Exige autorización parlamentaria para el uso de la fuerza en el extranjero, asegurando un proceso transparente y legítimo.

Respeto a los Derechos Humanos:

Garantiza que todas las actividades militares se desarrollen con pleno respeto a los derechos fundamentales.

Cooperación Civil-Militar:

Fomenta la colaboración con organismos civiles en emergencias, como desastres naturales, fortaleciendo el rol social de las Fuerzas Armadas.

Ley de Seguridad Interior (Ley N.º 24.059)

La Ley de Seguridad Interior regula el empleo de las Fuerzas Armadas y las fuerzas de seguridad en el ámbito interno, destacando:

Prohibición de Intervención en Asuntos Internos:

Las Fuerzas Armadas no pueden participar en actividades de seguridad pública, como el mantenimiento del orden o la represión de manifestaciones.

Declaración de Emergencia:

Solo en situaciones excepcionales, mediante el estado de sitio declarado por el Congreso, se permite la participación militar en seguridad interior.

Coordinación con Fuerzas de Seguridad:

Establece que, en caso de intervención autorizada, las Fuerzas Armadas deben coordinar sus acciones con las fuerzas de seguridad civiles.

Ley de Inteligencia Nacional (Ley N.º 25.520)

Esta ley regula las actividades de inteligencia para garantizar su legalidad y respeto a los derechos humanos:

Prohibición de Espionaje Interno:

Impide actividades de vigilancia hacia ciudadanos argentinos o residentes, protegiendo su privacidad.

Restricción de Actividades Políticas:

Prohíbe que las agencias de inteligencia participen en asuntos partidarios o influyan en procesos democráticos.

Respeto a los Derechos Humanos:

Todas las actividades deben ser proporcionales, necesarias y respetar los derechos fundamentales.

Autorización Judicial:

Cualquier interceptación de comunicaciones requiere autorización judicial expresa.

Resolución 381/2006

Esta normativa complementa la Ley de Inteligencia Nacional, estableciendo disposiciones específicas para las actividades de inteligencia:

Prohíbe la obtención de información sobre individuos basada en raza, religión, acciones privadas u opinión política.

Restringe la divulgación de información adquirida en funciones de inteligencia sin autorización judicial.

Prohíbe la influencia en cuestiones políticas, militares o sociales internas.

Conclusiones Parciales

Del análisis de las prescripciones legales y la doctrina internacional y nacional, se desprenden conclusiones clave que permiten comprender la necesidad y viabilidad de las Operaciones de Información (OI) en las Fuerzas Armadas de la República Argentina.

Pilares Fundamentales: Doctrina y Marco Legal

Las operaciones de información se sustentan sobre dos pilares esenciales:

La doctrina, que orienta las estrategias y el empleo de las capacidades.

El marco legal, que define los límites y garantías necesarias para ejecutar estas operaciones con legitimidad y transparencia.

Ambos elementos son indispensables para consolidar un enfoque moderno y profesional que permita a las Fuerzas Armadas adaptarse a los desafíos del entorno informativo actual.

Lecciones de la Doctrina Internacional

El análisis comparativo con las doctrinas de países líderes en la materia (EE. UU., Reino Unido, Rusia, Brasil y OTAN) revela una tendencia clara y consistente:

Las Operaciones de Información son abordadas desde niveles estratégicos y tácticos.

Se prioriza la coordinación integrada entre agencias y capacidades, con énfasis en dominar el entorno de la información en sus tres dimensiones:

Cognitiva: Influencia en la percepción y toma de decisiones del adversario.

Física: Protección y destrucción de sistemas críticos.

Datos: Control del flujo y uso estratégico de la información.

La creación de una célula especializada en operaciones de información, integrada en los Estados Mayores, permite una sincronización efectiva de las capacidades, con un oficial de información encargado de la planificación y ejecución de estas actividades.

La Doctrina Nacional: Un Espacio por Desarrollar

A diferencia de las doctrinas internacionales, las Fuerzas Armadas de la República Argentina aún no han profundizado en el desarrollo de una doctrina específica sobre Operaciones de Información. Esto representa tanto un desafío como una oportunidad:

Desafío, porque la falta de lineamientos claros limita la capacidad de respuesta en el entorno actual.

Oportunidad, porque existe un potencial significativo para implementar doctrinas innovadoras adaptadas a nuestra realidad operativa y legal.

El Marco Legal: Viabilidad y Respaldo

Desde la perspectiva legal, se identifica que las operaciones de información cuentan con un respaldo normativo válido, sujeto a ciertas restricciones y condiciones:

La Constitución Nacional, en la cúspide de la Pirámide de Kelsen, otorga las herramientas necesarias para situaciones excepcionales, como la declaración del estado de sitio en escenarios de guerra.

La Ley de Inteligencia Nacional (N.º 25.520) no prohíbe de manera explícita las operaciones de información.

Ninguna normativa actual establece una prohibición expresa al entrenamiento y capacitación de las fuerzas en este ámbito.

Si bien el marco legal vigente presenta restricciones para su empleo en tiempos de paz, estas podrían ser revisadas o flexibilizadas en el futuro con el fin de fortalecer las capacidades de las Fuerzas Armadas en el entorno informativo.

Las Operaciones de Información son una necesidad estratégica ineludible en el contexto militar contemporáneo. A través de un órgano especializado, respaldado por un marco legal sólido y una doctrina modernizada, nuestras Fuerzas Armadas pueden:

A- Proteger el entorno informativo propio.

B- Debilitar las capacidades del adversario.

C- Ejercer influencia efectiva en las decisiones del enemigo.

La adaptación doctrinaria y la correcta utilización de las herramientas legales existentes permitirán que estas operaciones se ejecuten de manera legítima, profesional y efectiva, contribuyendo así al éxito en el teatro de operaciones terrestre y garantizando la defensa de los intereses nacionales.

Figura 2: Pirámide de Kelsen Jerarquía normativa

La Pirámide de Kelsen como Ejemplo en el Marco Legal de las Operaciones de Información

La Pirámide de Kelsen es fundamental para comprender la jerarquía normativa en nuestro país. En su cúspide se encuentra la Constitución Nacional, una norma pétrea e inquebrantable, que prevalece por sobre todas las demás leyes, tratados y directivas. Esta supremacía constitucional establece los límites y principios que deben guiar cualquier acción del Estado, incluidas las Operaciones de Información (OI). En caso de peligrar la soberanía nacional, la Constitución habilita mecanismos excepcionales que permiten ajustar temporalmente las leyes y reglamentos inferiores. Es decir:

Primacía Constitucional: En situaciones de extrema gravedad, como un conflicto que comprometa la soberanía nacional, la Constitución Nacional ofrece herramientas como la declaración del estado de sitio (Art. 23) o la movilización de las Fuerzas Armadas (Art. 75, Inc. 25). Esto suspende temporalmente normas y restricciones, dando prioridad absoluta a la defensa del Estado y su integridad.

Adaptación del Marco Legal: Las leyes nacionales y tratados, aunque subordinados a la Constitución, se ajustan para garantizar la protección de la Nación. En este sentido, las Operaciones de Información se convierten en una herramienta clave para defender el entorno informativo, proteger nuestro proceso de toma de decisiones y debilitar las capacidades del adversario.

Flexibilidad Normativa: Los niveles inferiores de la pirámide, como leyes específicas o reglamentos militares, están diseñados para adaptarse rápidamente a los lineamientos superiores de la Constitución en tiempos de crisis, siempre respetando su esencia y objetivos.

Capítulo II

Evaluar las capacidades relacionadas con la información necesarias que un órgano de operaciones de información debe poseer, considerando las particularidades y requisitos específicos del Ejército (EA).

Propósito del capitulo

El análisis del primer capítulo resalta la importancia del marco legal para el uso de herramientas que controlen y dominen el entorno de la información, especialmente en la dimensión cognitiva, que abarca las emociones y voluntades de las tropas, el enemigo y la población, ya sea amiga, neutral o adversaria. Esta dimensión es un espacio complejo que requiere defensa y comprensión para evitar crisis sociales, económicas o inestabilidad interna durante un conflicto.

Este capítulo tiene como objetivo identificar y analizar las capacidades relacionadas con la información que se adapten a las particularidades legales y operativas de nuestro país, permitiendo planificar operaciones que contribuyan al éxito del Componente Terrestre del Teatro de Operaciones (CTTO). Estas capacidades deben generar ventajas operativas en el campo de batalla y en el ámbito estratégico mediante una sincronización y coordinación eficiente, respaldadas por la intención del comando superior y dirigidas por un órgano especializado con personal capacitado en diversas áreas.

Argentina, como octava superficie mundial, enfrenta desafíos estratégicos debido a su baja densidad demográfica, discontinuidad territorial, escasez de recursos y territorio ocupado por una potencia extrarregional. En este contexto, se concluye que es fundamental generar multiplicadores de fuerzas que permitan degradar al adversario desde la mayor distancia

posible, integrando el entorno de la información como una capa clave en las operaciones multidominio.

Para ello, se consideran cinco núcleos temáticos clave:

Estructura Social: Factores demográficos y psicosociales.

Condiciones de Vida: Impacto de la pobreza, educación y salud.

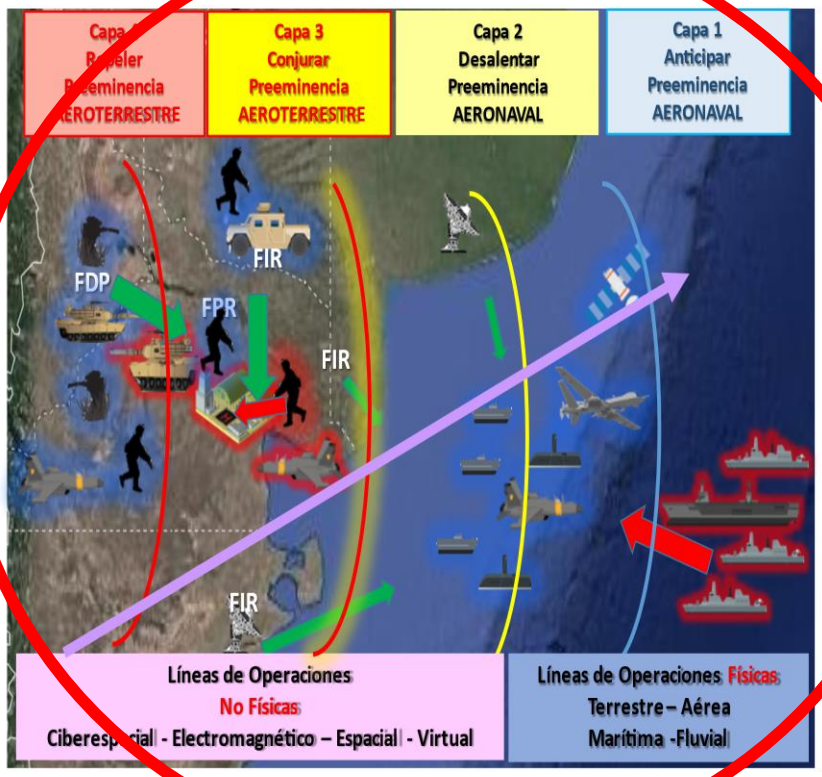
Consumos Culturales: Influencias de medios de comunicación y valores regionales.

Conectividad: Uso de redes digitales y acceso a la información.

Desarrollo Tecnológico: Innovación aplicada a operaciones de información.

El análisis de estos núcleos permitirá adaptar las capacidades de información a las particularidades socioculturales y geográficas de cada región del país, facilitando operaciones efectivas y legítimas antes, durante y después de un conflicto.

Finalmente, este enfoque busca integrar de manera permanente el entorno de la información en la estrategia militar, aprovechando las capacidades relacionadas con la información como herramientas fundamentales para anticipar, desalentar, conjurar y repeler amenazas, en consonancia con la doctrina y las normativas legales vigentes.



El entorno de la información y sus tres dimensiones:

a- Cognitiva

b- Física

c- Datos

Formando parte del espacio en el que se establecen las operaciones multidominio

El entorno de la información

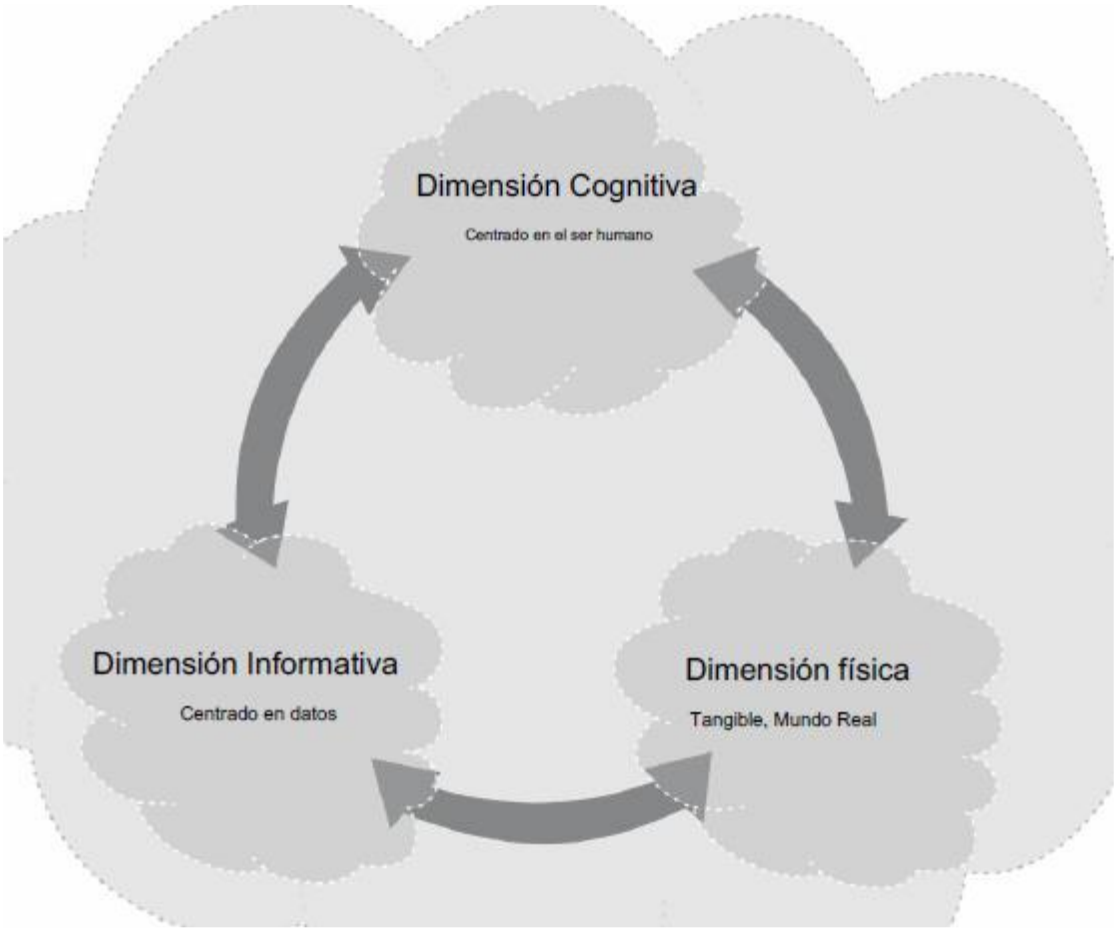


Figura 3: El entorno de la información y las tres dimenciones que lo conforman

Explicación del Gráfico: El Entorno de la Información

El gráfico ilustra las tres dimensiones clave del entorno de la información, que interactúan continuamente entre sí:

Dimensión Cognitiva:

Se centra en las percepciones, emociones y decisiones humanas.

Es la dimensión donde se influye en la voluntad y comportamiento de las tropas, el enemigo y la población.

Dimensión Informativa:

Focalizada en los datos, su flujo, almacenamiento y procesamiento.

Abarca la gestión de la información digital y los sistemas de comunicación.

Dimensión Física:

Representa el mundo tangible, como infraestructura, dispositivos y sistemas físicos.

Es el medio donde se ejecutan y materializan las acciones.

Estas dimensiones trabajan de manera integrada para influir, proteger y operar en el entorno informativo de manera efectiva.

CRI (capacidades relacionadas con la información):

COSACO (comunicación social aplicativa al combate): La Comunicación Social Aplicativa al Combate (COSACO) es una capacidad esencial dentro del conjunto de las Capacidades Relacionadas con la Información (CRI). Su objetivo principal es garantizar la transmisión, recepción y correcta interpretación de los mensajes por parte de audiencias clave, alineándose con los objetivos operativos de la fuerza.

Esta capacidad opera directamente sobre la dimensión cognitiva del entorno de la información, influenciando percepciones, emociones y voluntades tanto en tropas propias como en poblaciones amigas, neutrales o enemigas. Su efectividad radica en la precisión comunicacional y en la capacidad de adaptar los mensajes a las características socioculturales del entorno, asegurando que refuercen la legitimidad y el éxito de las operaciones.

El COSACO no es un concepto estático; se nutre de la experiencia operativa y el adiestramiento constante de las Fuerzas Especiales (FFEE), las cuales son las principales ejecutoras de estas acciones. Estas unidades están preparadas para desplegar técnicas avanzadas y procedimientos comunicacionales en los escenarios más desafiantes, garantizando que el mensaje llegue con claridad y tenga el efecto deseado, ya sea para fortalecer la cohesión interna o para influir en las percepciones del enemigo.

En resumen, el COSACO es una herramienta poderosa que combina precisión, adaptabilidad y experiencia operativa, convirtiéndose en una capacidad indispensable para dominar la dimensión cognitiva en cualquier entorno de conflicto.

Este enfoque profesional y estratégico asegura que la COSACO no solo sea relevante, sino que se perciba como una capacidad crítica para el éxito en las operaciones modernas.

Especialistas adecuados para las actividades de cosaco

Especialista	**Dimensión del Entorno que Afecta**	**Oportunidad**
Operador en psicología social	Cognitiva	Permanente
Especialista en comunicación social	Cognitiva - Datos	Permanente
Especialista en periodismo	Cognitiva - Datos	Permanente
Especialista en informática (Hackers)	Datos	Permanente
Especialista en propaganda	Cognitiva	Permanente
Especialista en radiodifusión	Datos	Permanente
Intérpretes - Traductores	Cognitiva - Datos	Permanente
Especialista en antropología	Cognitiva	Permanente
Especialista en salud	Cognitiva	Permanente

Sacerdote/Pastor (cristiano)	Cognitiva	Permanente
Especialista en negociación	Cognitiva	Permanente

Explicación del Cuadro y Descripción de las Especialidades

El cuadro presentado detalla un conjunto de Especialistas fundamentales para las Operaciones de Información (OI), clasificando su impacto según las dimensiones del entorno que afectan (Cognitiva, Datos o ambas) y destacando su contribución como oportunidades permanentes dentro del entorno de la información. Estas capacidades son esenciales para dominar el espacio informativo y generar ventajas tácticas y estratégicas.

Especialistas y Descripción

1- Operador en Psicología Social (Dimensión Cognitiva):

Estos especialistas trabajan directamente en el ámbito emocional y psicológico, analizando y moldeando percepciones, actitudes y comportamientos tanto de las propias tropas como del enemigo o la población civil.

Ejemplo histórico: Durante la Segunda Guerra Mundial, las campañas psicológicas aliadas incentivaron la rendición de soldados alemanes mediante mensajes que apelaban a la desesperación y desmoralización en el frente.

2- Especialista en Comunicación Social (Dimensión Cognitiva-Datos):

Encargados de diseñar y ejecutar estrategias de comunicación dirigidas a influir en audiencias específicas, estos especialistas trabajan en la narrativa y el mensaje.

Ejemplo histórico: Las transmisiones de Radio Free Europe durante la Guerra Fría mantuvieron informadas a las poblaciones detrás del Telón de Acero, debilitando la narrativa comunista.

3- Especialista en Periodismo (Dimensión Cognitiva-Datos):

Utilizan los medios de comunicación para generar opinión pública favorable y desacreditar al adversario. Su labor es clave en la gestión de crisis y propaganda.

Ejemplo histórico: La cobertura de la guerra en Vietnam influyó significativamente en la opinión pública estadounidense, acelerando el retiro militar.

4- Especialista en Informática (Hackers) (Dimensión Datos):

Estos expertos se enfocan en ciberseguridad y ciberataques, asegurando la protección de datos propios y afectando sistemas enemigos.

Ejemplo histórico: Durante el conflicto entre Rusia y Georgia (2008), los ciberataques rusos paralizaron infraestructuras críticas georgianas antes de las operaciones militares.

5- Especialista en Propaganda (Dimensión Cognitiva):

Diseñan mensajes estratégicos para influir en percepciones y comportamientos. La propaganda puede ser dirigida al enemigo para desmoralizar o a la población propia para generar cohesión.

Ejemplo histórico: La propaganda nazi durante la Segunda Guerra Mundial consolidó el apoyo interno al régimen en sus primeras etapas.

6- Especialista en Radiodifusión (Dimensión Datos):

Gestionan sistemas de transmisión para garantizar la difusión de mensajes clave en entornos operativos.

Ejemplo histórico: Durante la Operación Overlord (1944), las transmisiones de radio se utilizaron para difundir desinformación sobre el desembarco aliado en Normandía.

7- Intérpretes y Traductores (Dimensión Cognitiva-Datos):

Facilitan la comunicación efectiva en operaciones multinacionales o en zonas con diversidad lingüística.

Ejemplo histórico: Durante la Guerra de Irak, los intérpretes locales jugaron un papel crucial al mediar entre las fuerzas estadounidenses y las comunidades iraquíes.

8- Especialista en Antropología (Dimensión Cognitiva):

Estudian las dinámicas culturales y sociales para diseñar estrategias que respeten y utilicen estas características en beneficio de las operaciones.

Ejemplo histórico: En Afganistán, la comprensión de las estructuras tribales locales ayudó a las fuerzas aliadas a generar alianzas estratégicas.

9- Especialista en Salud (Dimensión Cognitiva):

Promueven el bienestar psicológico y físico, contribuyendo a la cohesión de las tropas y mitigando los efectos del estrés en combate.

Ejemplo histórico: Durante la Primera Guerra Mundial, los equipos médicos trataron el "shock de las trincheras", ayudando a los soldados a regresar al frente.

10-Sacerdote/Pastor (cristiano) (Dimensión Cognitiva):

Proveen apoyo espiritual y moral, fortaleciendo la resiliencia y la cohesión interna.

Ejemplo histórico: En la Guerra de Malvinas, los capellanes militares ofrecieron consuelo espiritual a los soldados argentinos en condiciones adversas.

11-Especialista en Negociación (Dimensión Cognitiva):

Facilitan acuerdos y alianzas en entornos de alta presión, reduciendo conflictos y generando ventajas tácticas.

Ejemplo histórico: Las negociaciones durante la guerra en los Balcanes permitieron corredores humanitarios críticos para la población civil.

12-Especialista en Narrativa (Dimensión Cognitiva):

Diseñan historias y mensajes coherentes que alinean las operaciones con los objetivos estratégicos y refuerzan la legitimidad de las acciones.

Ejemplo histórico: La narrativa aliada en la Segunda Guerra Mundial se centró en la liberación de Europa del fascismo, consolidando el apoyo popular.

13-Especialista en Comunicación Institucional (Dimensión Cognitiva):

Gestionan la relación entre las fuerzas militares y la sociedad, garantizando una percepción positiva y transparente.

Ejemplo histórico: Durante la Guerra del Golfo, los informes de prensa cuidadosamente gestionados presentaron una imagen eficiente de las fuerzas aliadas.

Inteligencia: esta capacidad difiere de la inteligencia táctica que normalmente nos proporciona conocimientos sobre el enemigo y el ambiente geográfico, en primer lugar, analiza de manera integrada las tres dimensiones del entorno de la información con especialistas que recopilan datos informáticos, psicosociales y de estructuras físicas los cuales son analizados y difundidos. Es una capacidad vital que apoya a las OI, empleando herramientas y técnicas que permiten evaluar el entorno de la información e integrarse a otras capacidades relacionadas con la información por una finalidad particular. En la actualidad las fuerzas armadas no disponemos de un elemento que puntualmente este capacitado y adiestrado para el análisis de factores psicosociales de la población propia, del enemigo y de países neutrales, siendo esencial su empleo particularmente antes de cualquier tipo de conflicto con el fin de disponer de información básica relacionada con el entorno de la información y poder actualizarla y completar el proceso de apreciación de situación a efectos de obtener conclusiones provechosas para el comandante.

Si bien las normas legales establecen que no podrán llevarse a cabo lo que a continuación se detalla:

Realizar tareas represivas, poseer facultades compulsivas, cumplir por si, funciones policiales ni de investigación criminal, salvo ante requerimientos específicos realizado por

autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción, o que se encuentre, para ello autorizado por ley.

Obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, culturales o laborales, así como por la actividad licita que desarrollen en cualquier esfera de acción.

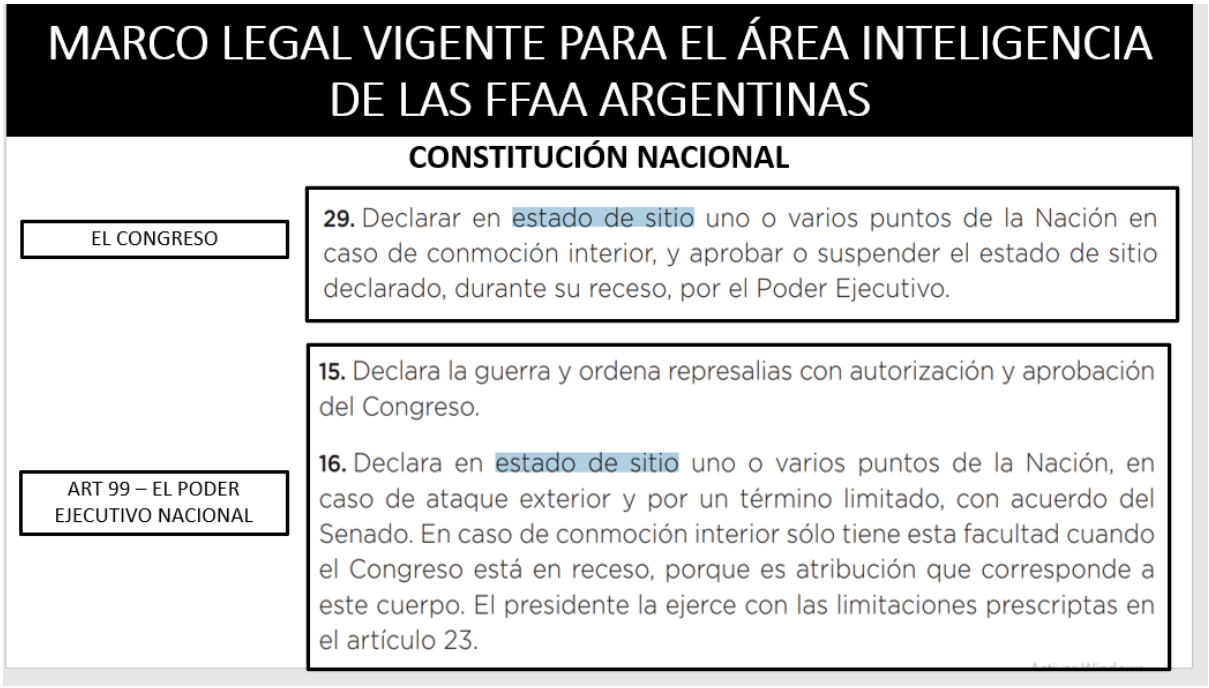
Influir de cualquier modo en la situación institucional, política, militar, policial, social y económica del país, en su política exterior, la vida interna de los partidos políticos legalmente constituidos, en la opinión pública, en personas, en medios de difusión o en asociaciones o agrupaciones legales de cualquier tipo.

En cuanto al artículo Nro 16; en función de lo estipulado en las leyes 23554 de defensa nacional, Nro 24059 de seguridad interior y Nro 25520 de inteligencia nacional; los organismos de inteligencia del estado mayor conjunto de las fuerzas armadas y los estados mayores generales del ejército, la armada y la fuerza aérea, no podrán realizar ninguna actividad de contrainteligencia, cualquiera fuera la denominación que la misma adopten y denominadas indistintamente también entre otras formas según la doctrina como actividades especiales de contrainteligencia, censura o medidas de seguridad de contrainteligencia prevista para el ámbito militar según dicha doctrina legal vigente.

En cuanto al artículo Nro 17; en función de lo estipulado en las leyes 23554 de defensa nacional, Nro 24059 de seguridad interior y Nro 25520 de inteligencia nacional; los organismos de inteligencia del estado mayor conjunto de las fuerzas armadas y los estados mayores generales del ejército, la armada y la fuerza aérea, no podrán realizar ningún tipo de actividad o de apoyo a la actividad conocida según la doctrina vigente como acción

psicológica o cualquiera otra de tales características, cualquiera fuera la denominación que reciban.

Comprendiendo que la Constitución Nacional en relación al estado de sitio en tiempos de guerra estable lo siguiente:



Debemos comprender que una vez se establezca un Teatro de Operaciones (TO) en un escenario de conflicto, se deben observar las normativas del Derecho Internacional Humanitario (DIH) y el Derecho Internacional de los Conflictos Armados (DICA), en conformidad con los convenios y protocolos de Ginebra, incluyendo sus protocolos adicionales. La creación de un TO implica la declaración de una situación legal excepcional, como el Estado de Sitio por ataque externo, conforme a lo estipulado en los Artículos 75 Inciso 27, y 99 Incisos 15 y 16 de la Constitución Nacional (CN). Esto implica la suspensión de ciertas garantías constitucionales y la no aplicación de las leyes y resoluciones mencionadas previamente. Adicionalmente, ninguna normativa, ya sea la Ley 25.520 de Inteligencia Nacional, ni las leyes de Seguridad Interior y Defensa Nacional, ni la Resolución Ministerial de Defensa 381, restringen la instrucción y desarrollo de procedimientos para capacitación o técnicas de análisis. Las restricciones solo se aplican a operaciones especiales con fines de inteligencia, acciones psicológicas, el mantenimiento de bases de datos de individuos por razones no reveladas aquí, la interferencia en la situación institucional o la ejecución de actividades represivas. Por otro lado, el Artículo 26 de la Ley 25.520 establece

la obligación de los miembros del sistema de inteligencia de instruirse en cuestiones específicas.

Medios de obtención más apropiados para las operaciones de información

Medio de obtención más adecuado	Dimensión del entorno que afecta	Oportunidad
Operador en psicología social	Cognitiva	Permanente
Especialista en comunicación social	Cognitiva- Datos	Permanente
Especialista en periodismo	Cognitivo-datos	Permanente
Especialista en informática - hackers	Datos	Permanente
Especialista en inteligencia humana	Cognitivo	Permanente
Especialista en escucha electromagnética	Datos	Permanente
Interpretes- traductores	Datos-cognitivo	Permanente

Medidas de seguridad de contra inteligencia: Las Medidas de Seguridad Contra la Inteligencia (MSCI) representan un conjunto de normativas y disposiciones cruciales que deben ser implementadas para salvaguardar a nuestras propias fuerzas militares contra las actividades de inteligencia enemiga y fortalecer la seguridad táctica en el contexto de operaciones de información. Estas medidas de seguridad tienen como objetivo principal proteger integralmente el entorno de la información, abarcando todas sus dimensiones. Los propósitos fundamentales de estas actividades son los siguientes:

Negar Información al Enemigo en la Dimensión Cognitiva: Esto implica preservar la integridad de la información que afecta tanto a nuestras propias tropas como a la población civil. Cualquier impacto en estas dimensiones puede tener un efecto directo en las decisiones tomadas por el comandante, por lo que es crucial salvaguardar esta información.

Proteger Toda Clase de Información: Esto incluye información documentada o almacenada en formatos digitales. Es esencial prevenir la propagación de información falsa, que, si bien puede no ser exclusivamente de naturaleza militar, puede tener un impacto significativo en la percepción pública y el estado de ánimo de la población. Para lograr esta capacidad, se requiere un alto nivel de capacitación y conciencia, especialmente antes del inicio de un conflicto. Es importante recordar que un enemigo inteligente se preparará durante años, estudiando y comprendiendo nuestro entorno de información antes de cualquier conflicto.

En resumen, las MSCI desempeñan un papel crucial en la protección y seguridad de nuestras fuerzas militares y la población civil, y su implementación adecuada es fundamental para garantizar el éxito en operaciones de información y en el ámbito militar en general.

Medios más apropiados para las MSCI en las operaciones de información

Medio/especialista	Dimensión del entorno que afecta	Oportunidad
Operador en psicología social	Cognitiva	Permanente
Especialista en comunicación social	Cognitiva-Datos	Permanente
Especialista en periodismo	Cognitivo-datos	Permanente

Especialista en protección informática - hakers	Datos	Permanente
Especialista en inteligencia humana	Cognitivo	Permanente
Especialista en escucha electromagnética	Datos	Permanente
Interpretes-traductores	Datos-cognitivo	Permanente
Especialista en ciberdefensa	Datos	Permanente
Especialista en contraespionaje	Datos-Cognitivo	Permanente

Destrucción Física: Esta capacidad se refiere a la desactivación o inutilización de los activos físicos del entorno de la información del enemigo. Esto incluye componentes como antenas, centros de comando, estaciones satelitales, redes informáticas que puedan transmitir o recibir datos relevantes para el comando y control del enemigo. Además, se puede considerar como objetivos estratégicos elementos como antenas satelitales, fuentes de suministro energético y otras instalaciones críticas del enemigo.

En el contexto de operaciones de información de naturaleza ofensiva, esta capacidad puede ser ejecutada por fuerzas de operaciones especiales. Cuando se trata de objetivos de

alta importancia estratégica, estas misiones suelen ser llevadas a cabo por comandos y fuerzas especiales altamente entrenadas.

En el caso de operaciones de información de carácter defensivo, se hace hincapié en la protección de los propios activos físicos mencionados anteriormente. Esto implica mantener en secreto la existencia y ubicación de estos activos frente al enemigo, así como asegurar su defensa adecuada en caso de un intento de ataque. Es especialmente crucial para la seguridad nacional proteger instalaciones estratégicas como las centrales nucleares, como es el caso de Atucha y Las Toninas en la República Argentina.

Medios de destrucción en operaciones de información de carácter ofensivo

Medio/especialista	Dimensión del entorno que afecta	Oportunidad
Comandos	Física	A orden
Fuerzas especiales	física	A orden

Medios de destrucción en operaciones de información de carácter defensivo

Medio/especialista	Dimensión del entorno que afecta	Oportunidad
cazadores	Física	A orden
Tropa regular	física	A orden

Guerra electrónica:

El campo de combate moderno nos presenta una creciente utilización de las radiaciones ópticas, electromagnéticas y acústicas, provocada por los avances tecnológicos y la necesidad de información, lo cual ha transformado sensiblemente el escenario de las operaciones.

La electrónica se ha introducido necesaria y decisivamente en todos los sistemas de armas y de comunicaciones, forzando cada vez más la dependencia de las operaciones al entorno electromagnético, al constituirse este en parte integral de todas las formas de guerra. Surge así una dimensión de vital importancia en el campo de Batalla EL ESPECTRO ELECTROMAGNÉTICO (EEM), cuya característica primaria es la de ser empleado con tanto por propia tropa, como por el enemigo; siendo su dominio un objetivo constante de toda fuerza armada.

En la actualidad el batallón de Operaciones electrónicas 601 constituye la única unidad táctica de Guerra Electrónica del Ejército Argentino, tiene como responsabilidad principal la de determinar el uso y explotación que hace el enemigo del espectro electromagnético, y utilizar la información obtenida para beneficio de propia tropa; luchando por el dominio de este, actuando en sistemas de comunicaciones.

En sí, esta unidad de GE realiza dos grandes actividades para cumplir con su misión. Una de carácter pasivo (MAE), mediante la búsqueda, interceptación, escucha, localización y registro de las transmisiones enemigas para obtener información del mismo (ubicación de PC, OBE, etc); y la otra de carácter activo (CME) que a partir de la información que se dispone, producto de emisiones enemigas interceptadas y analizadas, se está en capacidad de introducirse en la frecuencia enemiga y “trabajar” dentro de ella, ejecutando interferencia y/o

engaño, para obtener ventajas y de ser posible el dominio de porciones del espectro electromagnético (Garruba, 2015)

Guerra Electrónica en el Nivel Táctico: Según la doctrina del Ejército Argentino, la guerra electrónica en el nivel táctico implica la instalación, operación y mantenimiento del sistema táctico de guerra electrónica del componente terrestre del Teatro de Operaciones (TO). En esta fase inicial, se lleva a cabo la recopilación del orden de batalla electrónico a través de la inteligencia de emisiones. Luego, se planifican y ejecutan acciones de ataque electrónico destinadas a facilitar el propio sistema de comando y control (EA, 2015).

Guerra Electrónica en Operaciones de Información: Cuando se trata de Operaciones de Información, la guerra electrónica puede desarrollarse de manera defensiva en la protección de los medios considerados de Alto Valor (OAV). En este contexto, la seguridad electrónica desempeña un papel crucial para prevenir la interferencia en las señales, la distorsión de mensajes, el robo de información y el espionaje. Es importante destacar que, con el avance constante de la tecnología y la creciente conectividad, los riesgos asociados a estas amenazas se han vuelto más significativos. Por lo tanto, las medidas de seguridad a adoptar deben ser cada vez más sofisticadas y exhaustivas.

Especialistas y medios empleados en Guerra electrónica

Medio/especialista	Dimensión del entorno que afecta	Oportunidad
Personal especialista en guerra electrónica	Datos	A orden
Tropas de operaciones especiales	Datos	A orden

Ciber expertos	Datos	A orden
Especialistas en drones con capacidad para ejecutar ataques electrónicos	Datos	Permanente
Especialistas en desarrollo científico y en guerra electrónica	Datos	Permanente
Personal especialista en ciber inteligencia	Datos	Permanente
Analistas de inteligencia electrónica	Datos	Permanente

Conclusiones Parciales

El análisis realizado permite extraer conclusiones fundamentales sobre la necesidad de dominar el entorno de la información como una herramienta estratégica indispensable para respaldar los objetivos del comandante y garantizar la seguridad nacional. A continuación, se presentan las ideas principales, redactadas de manera más clara, atractiva y comprensible:

1. **Importancia de las Capacidades Relacionadas con la Información (CRI):**

Es imprescindible contar con un conjunto de capacidades relacionadas con la información que operen de manera cohesionada y flexible. Estas capacidades deben adaptarse tanto a los medios disponibles como a las necesidades específicas de cada dimensión del entorno informativo: cognitiva, física y de datos.

Sin embargo, se observa un déficit en equipamiento, doctrina y respaldo legal que limita su implementación efectiva, subrayando la urgencia de abordar estas carencias de manera prioritaria.

2. La Sinergia como Clave del Éxito:

La efectividad de las operaciones de información radica en la coordinación conjunta de todas las capacidades bajo un plan integral supervisado por niveles superiores.

Muchas de estas capacidades deben activarse incluso antes de un conflicto, permitiendo proteger las dimensiones del entorno informativo, disuadir posibles amenazas y garantizar una ventaja estratégica.

3. Relevancia Estratégica de las OI en el Escenario Actual:

Los recientes conflictos y ataques cibernéticos en el mundo —como el caso de Red October en 2007, el conflicto en Georgia en 2008 y las innovaciones de Estonia en tecnología blockchain— destacan la creciente importancia de las operaciones de información. Estos eventos subrayan cómo el dominio del entorno informativo puede influir decisivamente en el resultado de un conflicto.

4. Desafíos y Requisitos:

La expansión y consolidación de las capacidades de información dependerán del avance tecnológico y económico del país, apoyado por un marco legal sólido. Esto incluye el desarrollo de herramientas para prevenir la manipulación de percepciones públicas, proteger infraestructuras críticas como redes satelitales e Internet, y garantizar la seguridad de los sistemas de información.

5. La Necesidad de una Estrategia Proactiva:

El dominio del entorno informativo no solo se limita a responder a amenazas, sino que debe ser un esfuerzo continuo que contemple acciones preventivas y defensivas para

garantizar la integridad del espacio informativo nacional. Esto incluye el diseño de doctrinas que abarquen todas las dimensiones y prevengan sorpresas estratégicas.

6. Impacto en la Seguridad Nacional:

En un mundo cada vez más digitalizado, el entorno informativo se convierte en un frente prioritario de defensa. Dominarlo implica no solo proteger los intereses estratégicos del país, sino también garantizar la resiliencia frente a amenazas externas y salvaguardar la soberanía nacional

Las operaciones de información representan una herramienta crítica en el escenario contemporáneo. Su desarrollo requiere un enfoque integral que combine tecnología, coordinación operativa y respaldo legal. La lección aprendida de los eventos recientes deja claro que quien domine el entorno informativo tendrá una ventaja significativa en cualquier conflicto, reforzando así su posición estratégica y su seguridad nacional.

Capítulo III

Diseñar un órgano de operaciones de información, con el fin de asegurar una asesoría y asistencia efectiva al Comando de Tropas Terrestres y Operaciones (CTTO)."

Propósito del capitulo

El propósito de esta investigación hasta este punto ha sido abordar la cuestión de las operaciones de información en Argentina, centrándonos en el marco legal y las capacidades relacionadas con la información. En el primer capítulo, hemos destacado que las normas legales existentes en nuestro país, aunque pueden considerarse limitantes en ciertos aspectos, no prohíben expresamente la ejecución de operaciones de información. Además, hemos enfatizado la importancia del adiestramiento y la práctica de estas operaciones, lo cual no está prohibido por la ley.

En el segundo capítulo, hemos explorado las características del ambiente operacional de Argentina y analizado las dimensiones que conforman el entorno de la información. Esto nos ha permitido identificar las capacidades relacionadas con la información más adecuadas para nuestra doctrina, considerando las normas legales vigentes, especialmente la Constitución Nacional.

El objetivo central de este capítulo es proponer la creación de un Órgano de Operaciones de Información (OOI) que permita integrar, coordinar y potenciar las capacidades relacionadas con la información, asegurando su implementación efectiva en el Comando de Tropas Terrestres y Operaciones (CTTO). Este diseño busca adaptarse a las particularidades del entorno operacional argentino, respetando las normativas legales vigentes y alineándose con las lecciones aprendidas de doctrinas internacionales.

En capítulos anteriores, hemos identificado dos elementos clave:

La viabilidad legal de las operaciones de información en Argentina, basándonos en un marco normativo que no prohíbe su planificación, adiestramiento o ejecución.

La necesidad de capacidades relacionadas con la información (CRI), que abarcan dimensiones como la cognitiva, la física y la informativa, esenciales para proteger y dominar el entorno informativo en conflictos actuales y futuros.

A partir de esta base, en este capítulo se establece una propuesta concreta y práctica para el diseño de un OOI. Este órgano será un pilar esencial en la ejecución de las operaciones de información, proporcionando asesoría, planificación y supervisión en el CTTO.

Estructura del órgano de Operaciones de información

Matriz 1 COSACO

Especialistas	Auxiliares/Asesores	Misión General

Especialista en COSACO	Especialistas en propaganda	"Misión: Coordinar, sincronizar e integrar las tareas de COSACO con las actividades específicas de cada capacidad representada dentro del órgano de OI, tanto antes, durante como después del proceso de planeamiento y ejecución de las operaciones. Teniendo como objetivo principal contribuir al logro del efecto deseado por parte del comandante del CTTO."
	Operadores en psicología social	
	Sociólogos	
	Psicólogos	
	Asesor jurídico	
	Especialistas en salud	
	Especialista en comunicación social y prensa	

Matriz 2 Inteligencia

Especialistas	Auxiliares/Asesores	Misión General
Especialista en Inteligencia del entorno de la información	Especialista en espionaje y contraespionaje	"Misión: Coordinar, sincronizar e integrar las tareas de Inteligencia del entorno de la información con las actividades específicas de cada capacidad representada dentro del órgano de OI, tanto antes, durante como después del proceso de planeamiento y ejecución de las operaciones. Teniendo como objetivo principal contribuir al logro del efecto deseado por parte del comandante del CTTO."
	Especialista en análisis de datos	
	Especialista en inteligencia humana	
	Especialista en escucha electromagnética	
	Asesor jurídico	
	Especialista en informática	
	Intérpretes y traductores	

Matriz 3 Contrainteligencia

Especialistas	Auxiliares/Asesores	Misión General
Especialista en Contra Inteligencia del entorno de la información	Especialista en contraespionaje	"Misión: Coordinar, sincronizar e integrar actividades de Contra Inteligencia del entorno de la información con las actividades específicas de cada capacidad representada dentro del órgano de OI, tanto antes, durante como después del proceso de planeamiento y ejecución de las operaciones. Teniendo como objetivo principal contribuir al logro del efecto deseado por parte del comandante del CTTO."
	Especialista en análisis de datos	
	Especialista en inteligencia humana	
	Especialista en escucha electromagnética y guerra electrónica	
	Asesor jurídico	
	Especialista en informática	
	Intérpretes y traductores	

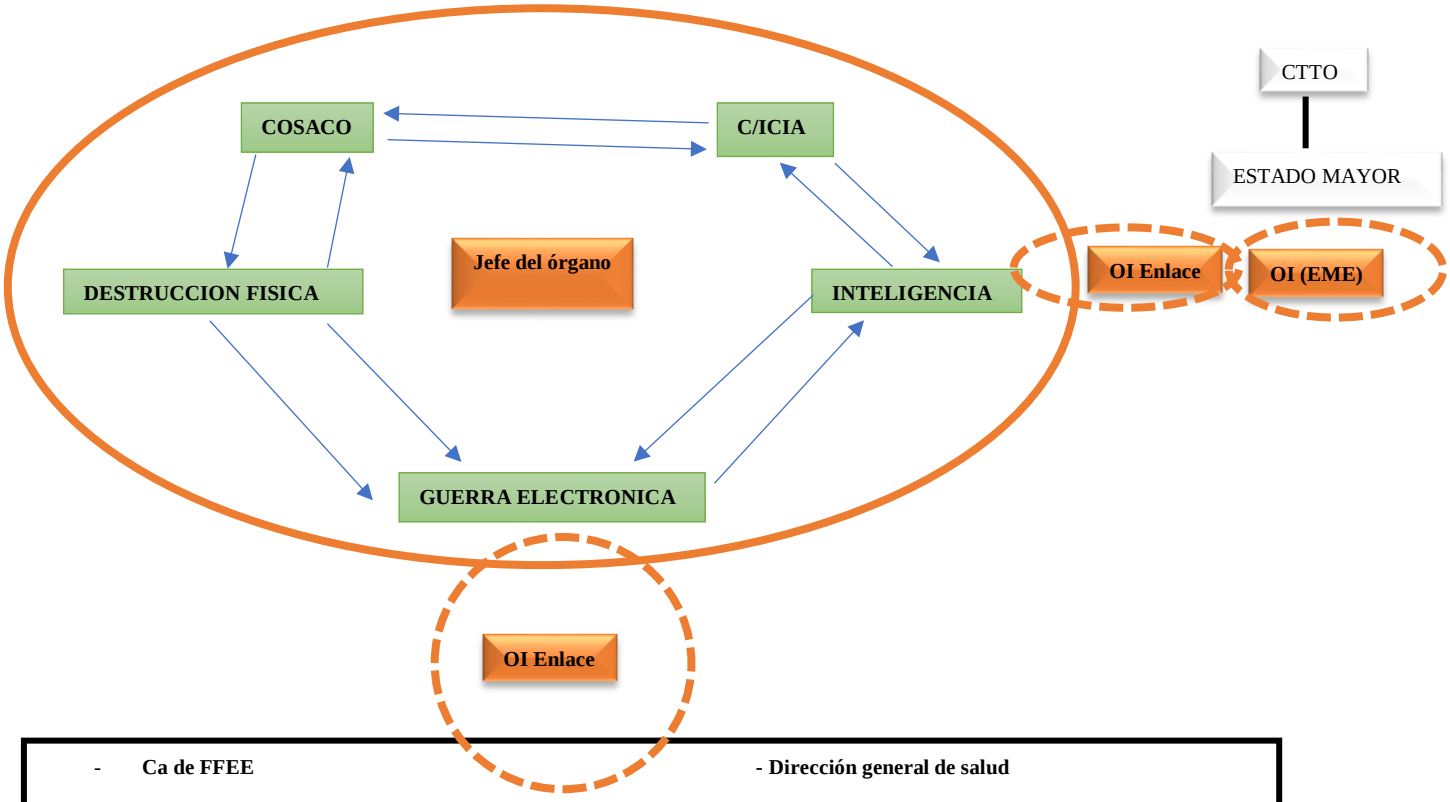
Matriz 4 destrucción física

Especialistas	Auxiliares/Asesores	Misión General
Comandos- FFEE y TOE(S) Cazadores Montaña, Monte y Patagónicos, hakers	Especialista en planeamiento de operaciones de comandos	"Misión: Coordinar, sincronizar e integrar las acciones de destrucción física que puedan afectar el entorno de la información con las actividades específicas de cada capacidad representada dentro del órgano de OI, tanto antes, durante como después del proceso de planeamiento y ejecución de las operaciones. Teniendo como objetivo principal contribuir al logro del efecto deseado por parte del comandante del CTTO."
	Especialistas en ejecución de operaciones de Comandos	
	Especialistas en inutilización de medios tecnológicos de alta complejidad	
	Asesores técnicos/ ingenieros especializados en equipos e instalaciones de alta complejidad tecnológica	
	Asesor jurídico	
	Especialista en informática	
	Especialistas en medios electromagnéticos e informáticos.	

Matriz 5 de Guerra electrónica

Especialistas	Auxiliares/Asesores	Misión General
Especialista en Guerra electrónica	Especialista en drones con capacidad para ejecutar ataques electrónicos	"Misión: Coordinar, sincronizar e integrar las acciones de Guerra electrónica del entorno de la información con las actividades específicas de cada capacidad representada dentro del órgano de OI, tanto antes, durante como después del proceso de planeamiento y ejecución de las operaciones. Teniendo como objetivo principal contribuir al logro del efecto deseado por parte del comandante del CTTO."
	Especialista en ciberdefensa y ciber ataques	
	Analista del sistema electromagnético y cibernético de probables amenazas.	
	Especialista en escucha electromagnética	
	Analistas de inteligencia electrónica	
	Especialista en informática	
	Especialistas en seguridad de Objetivos estratégicos nacionales (las Toninas)	

Estructura del órgano de Operaciones de información



- Ca de FFEE	- Dirección general de salud
- Ca(s) de Comandos	- Dirección General de investigación y desarrollo
- Ca (s)Caz Monte, patagónicos y Montaña	- Aviación de Ejercito
- Batallón de operaciones electrónicas y ciberdefensa	- Dirección General de Materiales
- B (s) ICIA	
- DIC	
- Comunicación institucional	
- Dirección general de salud	

Funcionamiento del órgano de operaciones de información

A lo largo de este trabajo, hemos explorado y analizado las leyes, doctrinas y las particularidades del ambiente operacional argentino con el propósito de identificar las capacidades relacionadas con la información más adecuadas para nuestra realidad. Basándonos en estas capacidades, proponemos la creación de un órgano de operaciones de información diseñado para coordinar, sincronizar e integrar actividades y tareas específicas. Este sistema busca lograr una sinergia única que permita anticiparnos a eventos adversos,

planificar y ejecutar operaciones de manera efectiva, y contribuir al éxito del comandante del Componente Terrestre del Teatro de Operaciones (CTTO).

El órgano de operaciones de información operará en el entorno informativo, abarcando las dimensiones cognitivas, física y de datos, con un enfoque permanente en influir, interrumpir, corromper o neutralizar la toma de decisiones del enemigo. Esta estructura es el resultado de un diseño centrado en las necesidades de la guerra moderna, adaptado a las capacidades y restricciones legales de nuestra nación.

Estructura del Órgano

1. Composición del Órgano

El órgano estará integrado por cinco oficiales especialistas, cada uno enfocado en una de las capacidades clave que hemos identificado como esenciales para operar en el entorno de la información:

- COSACO (Comunicación Social Aplicativa al Combate): Encargada de diseñar mensajes estratégicos y psicológicos para influir en las percepciones y comportamientos, tanto de tropas amigas como del adversario y la población civil.
- Inteligencia de Operaciones de Información: Responsable de la recopilación, análisis y aprovechamiento de datos relevantes para el planeamiento de las operaciones.
- Contrainteligencia: Su misión será proteger las operaciones propias, detectar vulnerabilidades y contrarrestar intentos de infiltración o manipulación adversaria.

- Destrucción Física: Orientada a neutralizar infraestructuras críticas del adversario mediante operaciones precisas y quirúrgicas, minimizando daños colaterales.
- Guerra Electrónica: Esta capacidad incluye ciberdefensa, ciberataque y operaciones electromagnéticas, como interferencia y explotación de señales adversarias.

Cada capacidad contará con el respaldo de especialistas y asesores técnicos, cuya labor será esencial para garantizar el éxito de las operaciones.

2. Oficial de Enlace Interno

Este oficial actúa como punto de contacto entre el órgano y los elementos de la fuerza que poseen capacidades específicas, como inteligencia, comunicaciones y asuntos civiles. Su función principal será garantizar la integración y sincronización de todos los esfuerzos.

3. Oficial de Enlace con el Estado Mayor del CTTO

Este enlace asegura una comunicación directa y constante entre el órgano y el Estado Mayor del CTTO. Además, colabora con el oficial de operaciones de información que forma parte del Estado Mayor Especial, orientado al planeamiento estratégico de las operaciones.

4. Coordinación del Órgano

El liderazgo estará a cargo de un jefe del órgano, quien supervisará y coordinará todas las actividades. Este líder no solo garantizará la alineación de las capacidades con los objetivos del comando superior, sino que también será responsable de evaluar constantemente los resultados y ajustar las estrategias según sea necesario.

Pilares del Funcionamiento

1. Planeamiento Integral y Continuo:

Las operaciones de información no se limitan a momentos de conflicto. El órgano debe operar de manera permanente, anticipándose a posibles amenazas, fortaleciendo el entorno informativo propio y disuadiendo acciones adversarias.

2. Flexibilidad y Adaptabilidad:

La guerra moderna demanda estructuras que puedan ajustarse rápidamente a los cambios del entorno. Este órgano está diseñado para operar tanto en escenarios convencionales como no convencionales, adaptándose a las necesidades específicas de cada situación.

3. Sinergia entre Capacidades:

La verdadera fortaleza de este órgano radica en su capacidad para coordinar diferentes disciplinas en un esfuerzo conjunto. Al integrar capacidades como COSACO, ciberdefensa y guerra electrónica, se asegura un impacto multidimensional en el entorno informativo.

4. Conformidad Legal y Doctrinaria:

Todas las operaciones se llevarán a cabo dentro del marco normativo vigente, respetando los principios establecidos por la Constitución Nacional y las leyes internacionales aplicables.

Impacto y Beneficios del Órgano

Anticipación y Prevención: Al operar continuamente, este órgano puede identificar y neutralizar amenazas antes de que se materialicen.

Respuesta Integral: La combinación de capacidades permite abordar el entorno informativo de manera holística, asegurando que ninguna dimensión quede desprotegida.

Fortalecimiento del CTTO: Al centralizar las operaciones de información bajo un órgano especializado, se optimizan los recursos y se proporciona un apoyo más efectivo al comandante.

Resiliencia Operativa: Este diseño dota a nuestras fuerzas de una capacidad robusta para operar en escenarios complejos y proteger los intereses estratégicos de la nación.

Conclusiones Parciales

Tras un análisis exhaustivo del entorno operacional, hemos identificado las capacidades relacionadas con la información que resultan indispensables para fortalecer la eficacia operativa del Componente Terrestre del Teatro de Operaciones (CTTO). Este estudio ha considerado factores legales, psicosociales, culturales, económicos y las condiciones actuales de nuestras fuerzas armadas, con el objetivo de proponer soluciones adaptadas a las necesidades reales y a las posibilidades del país.

El resultado es una estructura orgánica innovadora, diseñada para operar de manera cohesionada y resolver los desafíos que plantea la guerra moderna. Esta estructura está fundamentada en un enfoque sistémico, que prioriza la coordinación e integración de todas las capacidades en las diferentes dimensiones del entorno de la información: cognitiva, informativa/datos y física.

Aspectos Clave de las Conclusiones

1- Capacidades Identificadas y Su Relevancia

Las capacidades seleccionadas, como COSACO, Inteligencia de Operaciones de Información, Contrainteligencia, Guerra Electrónica y Destrucción Física, fueron elegidas no solo por su eficacia, sino también por su viabilidad dentro del marco normativo argentino. Estas capacidades han demostrado ser fundamentales en escenarios internacionales recientes, donde la información ha jugado un rol decisivo en los conflictos modernos.

Cada una de estas capacidades fue analizada en función de su impacto potencial en el entorno informativo nacional e internacional, adaptándose a nuestras limitaciones operativas y legales, pero maximizando su utilidad.

2- Estructura Organizativa Propuesta

El diseño incluye una plana mayor especial que asesora y asiste al Estado Mayor del CTTO, garantizando la alineación estratégica y táctica.

Además, se ha establecido un sistema de oficiales de enlace, que actúan como puntos de conexión entre el órgano y las diversas organizaciones que poseen capacidades específicas, asegurando una integración total de esfuerzos.

Este modelo organizativo refuerza la capacidad de sincronizar operaciones antes, durante y después de un conflicto, lo que permite una preparación constante y una respuesta ágil frente a amenazas emergentes.

3- Permanencia y Continuidad Operativa

Reconocemos que las operaciones de información no son herramientas exclusivas de un escenario bélico declarado, sino que deben ser empleadas de manera continua para proteger el entorno informativo, anticiparse a posibles amenazas y disuadir acciones adversarias.

Esta estructura no solo opera en el momento del conflicto, sino que funciona como un mecanismo permanente de defensa y proyección estratégica, generando efectos acumulativos que refuerzan la posición del país en un mundo interconectado.

4- Respaldo Legal y Doctrinario

La propuesta respeta plenamente las leyes nacionales y se alinea con los principios de la Constitución Nacional. Aunque algunas normativas actuales pueden presentar restricciones, el marco legal vigente permite la ejecución de las operaciones planteadas, siempre que se realicen dentro de los límites éticos y jurídicos establecidos.

La doctrina y la capacitación constante se identifican como pilares fundamentales para garantizar la efectividad del órgano, adaptándolo a los avances tecnológicos y las dinámicas del entorno global.

5- Innovación y Adaptación al Contexto Argentino

En un país con características únicas como vasto territorio, baja densidad poblacional y recursos estratégicos distribuidos, esta estructura responde a la necesidad de crear multiplicadores de fuerza que permitan compensar limitaciones materiales.

La flexibilidad de este modelo asegura su relevancia en diversos escenarios, desde conflictos de baja intensidad hasta operaciones multidominio.

El establecimiento de un órgano de operaciones de información representa un salto cualitativo en la capacidad de las Fuerzas Armadas para enfrentar los desafíos de la guerra moderna. Este diseño no solo aporta una herramienta estratégica clave, sino que también refuerza la soberanía nacional al garantizar que Argentina esté preparada para dominar el entorno informativo, proteger sus intereses y enfrentar amenazas con eficacia.

Con una estructura bien definida, capacidades ajustadas al entorno y un respaldo doctrinario y legal sólido, este órgano tiene el potencial de ser un modelo operativo adaptado a las necesidades del siglo XXI. Su implementación marcará un antes y un después en la forma en que nuestro país enfrenta los desafíos del presente y se prepara para las incertidumbres del futuro.

Conclusiones

Esta investigación se ha guiado por un objetivo general bien definido: concebir y establecer un órgano de Operaciones de Información con la finalidad de brindar orientación y respaldo al comandante del componente terrestre en el teatro de operaciones durante el proceso de toma de decisiones. Este órgano tiene como objetivo facilitar la integración efectiva de las diversas acciones que conforman las operaciones de información. Para alcanzar este objetivo, se establecieron tres objetivos particulares que, a lo largo del

desarrollo de la investigación, proporcionaron los fundamentos científicos, tácticos y técnicos necesarios para cumplir con el objetivo general.

En un primer lugar, se constató que en nuestra nación no existe una doctrina consolidada que enseñe las operaciones de información. En un mundo caracterizado por un ambiente operacional dinámico y cada vez más complejo debido a los avances tecnológicos, con diversos actores que van desde lo militar y político hasta empresas privadas, medios de comunicación, terrorismo y narcotráfico, muchos países han desarrollado doctrinas y cuentan con oficiales de información en sus estados mayores para asesorar y asistir en estas cuestiones. Sin embargo, es fundamental destacar que, si bien existen leyes de seguridad, defensa y de inteligencia nacional que limitan algunas actividades necesarias para el desarrollo de las operaciones de información, estas leyes no prohíben en ningún momento la realización de operaciones de información ni impiden la instrucción y capacitación de los elementos en estas áreas.

Otro aspecto relevante al que se llegó en esta investigación se basa en la jerarquía normativa, conocida como la pirámide de Kelsen. Esta jerarquía establece que el sistema jurídico tiene diferentes niveles jerárquicos, y en situaciones de conflicto armado, las normas constitucionales pueden derogar las leyes nacionales, reglamentos y tratados, permitiendo así la realización de actividades que, bajo las leyes actuales, están restringidas.

Tras un exhaustivo análisis de las bases legales y doctrinarias pertinentes, y teniendo en cuenta las lecciones extraídas de estas fuentes, se procedió a estudiar el entorno de la información y las dimensiones que lo componen: cognitiva, informativa-datos y física. Este análisis proporcionó los fundamentos necesarios para identificar aquellas capacidades de la fuerza que pueden incidir significativamente en el entorno de la información. Estas capacidades se denominan Capacidades Relacionadas con la Información (CRI). Para cada una de las CRI, se realizó un estudio detallado que identificó los elementos que las

componen, los especialistas y asesores involucrados y su misión general en el contexto de las operaciones de información.

Como resultado de este análisis, esta investigación identificó cinco CRI fundamentales: COSACO, Inteligencia, Contrainteligencia, Destrucción Física y Guerra Electrónica. Vale la pena destacar que la Guerra Electrónica engloba actividades relacionadas con la ciberdefensa y los ciberataques, lo que subraya su relevancia en un entorno operacional cada vez más digitalizado y conectado.

Es importante resaltar que las CRI operan de manera integrada y coordinada entre sí, y su ámbito de acción se limita al entorno de la información. Su propósito principal es dominar este entorno, contribuyendo así al éxito de las operaciones militares en general.

Después de un detenido análisis de la doctrina, las normas legales y la selección de los medios que proporcionan las Capacidades Relacionadas con la Información (CRI) más apropiadas para influir en el entorno de la información en apoyo de las operaciones militares, hemos emprendido la tarea de organizar una estructura que nos permita poner en funcionamiento estas capacidades. En este sentido, este órgano se encuentra bajo la dirección de un jefe, quien asume la responsabilidad de garantizar el funcionamiento sistémico y efectivo de esta entidad.

Es crucial destacar que cuando hablamos de operaciones de información, no nos referimos exclusivamente a actividades de inteligencia. Más bien, involucra la participación de diversas especialidades necesarias para operar este sistema complejo pero esencial. Por lo tanto, un oficial de operaciones de información se distingue de un oficial de inteligencia.

El órgano, en su operación, deberá asegurarse de que las tareas y actividades de las CRI se ejecuten de manera organizada, coordinada, integrada y sincronizada. Cada capacidad estará representada en el órgano por especialistas en la materia, con la cantidad de asesores necesarios para un desempeño óptimo. Por esta razón, el órgano debe contar al menos con un

oficial de información que funja como enlace con las diferentes unidades de las fuerzas que poseen las capacidades pertinentes.

Además, el órgano de operaciones de información mantendrá un oficial de enlace con el estado mayor del componente terrestre del teatro de operaciones. Esto se justifica debido a que el órgano incluirá un estado mayor especial como parte de su estructura, integrado en el estado mayor del componente terrestre del teatro de operaciones, participando activamente en el proceso de planeamiento. Esta investigación ha culminado con la concepción de una estructura operativa que permitirá el funcionamiento eficiente de las CRI en el entorno de la información. La coordinación y la integración adecuadas de estas capacidades son fundamentales para el éxito de las operaciones militares y garantizar la superioridad en el ámbito informativo.

Aporte profesional

El aporte profesional de esta investigación radica en la destacada relevancia que tiene en un contexto global caracterizado por conflictos internacionales y una creciente rivalidad entre naciones. La realidad actual ha demostrado que las guerras contemporáneas no solo se libran en el campo de batalla, sino que comienzan mucho antes, en el ámbito de la información y la desinformación.

Uno de los principales aportes de esta investigación es la comprensión de que las naciones y actores involucrados en conflictos emplean todos los recursos disponibles para influir en la percepción de la población, difundiendo propaganda y narrativas específicas. La conectividad global ha eliminado las fronteras físicas y ha permitido la difusión instantánea de mensajes, lo que significa que la instrucción y la propaganda pueden llegar a cualquier lugar del mundo.

Un aspecto crucial destacado en este estudio es que esta situación no solo persistirá, sino que se volverá aún más compleja debido al rápido avance tecnológico. Por lo tanto, es

fundamental reconocer la importancia de asegurar el entorno de la información en sus tres dimensiones: cognitiva (influencia en la percepción de la población), informativa (seguridad de los datos) y física (protección de objetivos estratégicos).

El aporte de esta investigación también se refleja en la necesidad imperante de que las fuerzas armadas comprendan la importancia de desarrollar una doctrina que abarque las Operaciones de Información. Esto implica formar y capacitar a oficiales de información especializados que puedan planificar y coordinar de manera efectiva con los estados mayores y otros elementos de las fuerzas armadas. Esta preparación es esencial para garantizar la seguridad y defensa de los intereses nacionales en un mundo cada vez más interconectado y expuesto a amenazas en el ciberespacio.

En resumen, esta investigación destaca la urgente necesidad de reconocer la importancia de las Operaciones de Información en el contexto actual y futurista de conflictos internacionales. Proporciona una base sólida para la formulación de políticas y estrategias que permitan a las naciones proteger sus intereses y su seguridad en un entorno global altamente dinámico y desafiante.

Referencias

Arquilla & Ronfeldt. (2003). Redes y Guerras en Red. Madrid: Alianza Editorial

EA. (2008). Inteligencia Tactica

EA. (2015). Manual de COSACO.

EA. (2015). Reglamento de tecnicas y procedimientos de fuerzas especiales.

EA. (2001). Manual de conduccion de fuerzas especiales.

ST Garruba. (2015). El batallon de operaciones Guerra electronica 601 en el desarrollo de ejercitaciones conjuntas.

Ejercito de Brasil. (2019) Manual de Operaciones de Información.

Ejército de EEUU. () Manual de Operaciones de Información.

Ejercito de España. (2006). Manual de operaciones de información.

Ejercito del Perú. (2013) Manual de técnicas de Operaciones psicológicas.

Bilibio, R. (2017). Operaciones de Información. Buenos Aires: Escuela Superior de Guerra Conjunta de las FFAA.

Mintzberg, H. (2005). La Estructuración de las Organizaciones. Barcelona: Editorial Ariel S.A.

OTAN. (2009). Doctrina Conjunta Aliada para Operaciones de Información. Departamento de Estandarización.

OTAN. (2017). Doctrina Conjunta Aliada. Departamento de Estandarización.

EA. (2001). Terminología castrense de uso en el Ejército Argentino. EA.

EA. (2015). Conducción para las Fuerzas Terrestres. EA.

EA. (2019). Demoliciones . EA.

PEN. (1988). Ley 23554. Ley de Defensa Nacional. .

PEN. (1991). Ley 24059. Ley de Seguridad Interior.

República Argentina. (1994). Constitución de la Nación Argentina.

República Argentina. (2001). Ley 25520 de Inteligencia Nacional.

República Argentina. (06/08). Resolución Ministerial 381 y 1280.

Galicia R. (2013). El sistema C3I2 en la era de la información

Matthew J. Sheiffer. (2018). Las operaciones de información y actividades ciber electromagnéticas del ejército de EUA.

Perceptions are reality. (2018). Fort Leavenworth: US Army University Press.

Sun Tzu. (2003). El Arte de la Guerra. Biblioteca Virtual Universal.