



TRABAJO FINAL INTEGRADOR

TEMA:

**DISEÑO DE PUESTOS COMANDO DE NIVEL OPERACIONAL PARA
CONDUCIR OPERACIONES MULTIDOMINIO**

TÍTULO:

**HACIA EL DISEÑO DE UN ÓRGANO DIRECTOR DE OPERACIONES
DE INFORMACIÓN PARA SU INCORPORACIÓN A UN ESTADO
MAYOR DE NIVEL OPERACIONAL**

AUTOR: MAYOR (EA) ELIO MAXIMILIANO ALVAREZ

TUTOR: TENIENTE CORONEL (RE) Mg GUILLERMO CAMPOS

Año 2023

Resumen

En el complejo panorama que presentan los ambientes operacionales actuales, donde los avances tecnológicos son cada vez más influyentes, las Operaciones de Información (OI) se han convertido en un elemento crucial para las Fuerzas Armadas de todo el mundo, siendo hasta consideradas un elemento más del poder nacional, llegando a tener inclusive un empleo que, por el alcance de sus efectos, trasciende el ámbito puramente militar.

Tradicionalmente, las OI se enfocaban en la adquisición y el procesamiento de información con fines estratégicos. Sin embargo, en la era digital actual, su alcance y complejidad han experimentado una expansión significativa. En el nivel operacional, las mismas no sólo se centran en la recopilación de datos, sino que se utilizan para influir en la percepción de la población, desestabilizar a los adversarios y contribuir al logro de los objetivos tácticos y estratégicos, permitiendo alcanzar los estados finales deseados correspondientes.

Los conflictos de este último tiempo se producen en entornos cada vez más complejos, donde las Nuevas Tecnologías de la Información y Comunicaciones (NTIC) juegan un rol clave, por las enormes posibilidades que brindan en el uso dirigido de los medios de comunicación social (MCS), logrando un marcado efecto en la opinión pública ante una situación de crisis, actuando directamente en el plano cognitivo del conductor adversario, para afectar así su capacidad de accionar coordinadamente y su espíritu de lucha, como también propiciando el apoyo o desaprobación de cualquier sociedad a una determinada causa, lo cual puede hacer fracasar una campaña entera.

Mientras que, tanto en el marco regional como internacional, muchos países ya contemplan a las OI en su doctrina y también en su estructura organizacional, esto no sucede así en el ámbito de las Fuerzas Armadas (FFAA) argentinas, significando para la realidad nacional, una clara desventaja ante cualquier eventual situación de conflicto.

Por ello, se buscará arribar a las características generales de una posible organización conjunta en el marco de las FFAA, estableciendo como premisa la relevancia que han cobrado las OI en los conflictos modernos, analizando tanto la doctrina de otros países que marchan a la vanguardia en esta temática, como así también la experiencia en conflictos de diversa índole, donde se pueda apreciar y extraer las enseñanzas sobre su empleo que permitan realizar una contribución en el sentido pretendido.

Palabras Clave

Guerra, Información, Organización, Integración, Capacidades

ÍNDICE

Introducción.....	1
Capítulo 1. Análisis doctrinal y del empleo de las OI en distintos escenarios.	10
1.1 Doctrina de OI en países de referencia.....	10
1.2 Empleo de las OI en distintos escenarios históricos	19
Capítulo 2. Aspectos generales sobre el diseño de un órgano director de Operaciones de Información de nivel operacional	23
2.1 Característica principales de las OI.....	23
2.2 Descripción de las características generales de un órgano director de OI	26
Conclusiones	32

Introducción

"Porque quien consigue controlar nuestra mente consigue el poder"

Pedro Baños.¹

Para comprender el protagonismo que han adquirido las acciones relacionadas con el ámbito de la información y su empleo direccionado o gestionado hacia distintos objetivos, mediante el uso de distintas capacidades, técnicas y procedimientos, podemos partir de la antigua premisa que sostiene que la esencia del arte militar radica en el uso del engaño como herramienta principal de los conflictos, por ello el más alto mérito en la estrategia militar es lograr la derrota del enemigo sin la necesidad de un enfrentamiento directo. En definitiva, aquellos conductores que simplemente ganan todas las batallas o han tenido éxito en diferentes contiendas no resultaría mérito suficiente para ser considerados exitosos en el arte de la guerra; sino más bien que, los más grandes expertos en ese arte son aquellos que logran la rendición de las fuerzas enemigas sin recurrir a la confrontación armada. (Sun Tzu, 2004, págs. 17-25).

En este sentido el concepto de OI como tal, ha tenido a lo largo del tiempo sus fundamentos en lograr afectar las percepciones de los actores de un determinado entorno para controlar la mente mediante diversas estratagemas², dirigiendo la información en forma intencionada, para afectar la interpretación que ante una situación pueda tener el adversario, y por ende su comportamiento que incide en su proceso de toma de decisiones, buscando quebrar la voluntad de lucha y finalmente hacerlo deponer su actitud obteniendo la victoria al alcanzar un Estado Final Deseado (EFD) de los niveles correspondientes, pero sin dejar de lado, la posibilidad de lograr esto sin llegar al empleo de los medios militares en forma directa, lo cual es la tendencia actual buscada por medio de este tipo de operaciones y que como mencionamos al principio proviene de una idea o concepción antigua.

Para lograr esto, la información ha sido primordial a la hora de afrontar con posibilidades de éxito una batalla o contienda armada, como forma de dirimir una disputa, siendo la misma un verdadero instrumento de la política, para su gestión a través de distintos

¹ Coronel del Ejército de Tierra de España y diplomado de Estado Mayor, actualmente en situación de reserva. Ha sido jefe de Contrainteligencia y Seguridad del Cuerpo de Ejército Europeo en Estrasburgo. Es magíster en Defensa y Seguridad por la Universidad Complutense de Madrid. Ha participado en misiones en Bosnia y Herzegovina (UNPROFOR, SFOR y EUFOR), y hoy es uno de los mayores especialistas en geopolítica, estrategia, defensa, seguridad, terrorismo, inteligencia y relaciones internacionales. Es autor de los libros *Así se domina el mundo*, *El dominio mundial* y *El dominio mental*.

² 1) Ardid de guerra. 2) Astucia, fingimiento y engaño artificioso. (RAE)

modos, o en otros términos, la continuación de la política por otros medios (Clausewitz, 2003, pág. 49).

Sin embargo, lo que ha cambiado radicalmente a lo largo de los años es la forma en que se libran y se ganan las batallas. La llegada de nuevas tecnologías, como el uso del espectro electromagnético, internet y las redes sociales que potencian la influencia del manejo intencionado de la información buscando un determinado resultado, las ha convertido en una parte cada vez más influyente de la guerra moderna.

Al respecto, podemos decir que es fácil encontrar en el devenir histórico, ciertas creaciones, inventos o medios, como las armas arrojadas, la pólvora y las armas de fuego, el telégrafo, las comunicaciones radiales y el uso del campo electromagnético, el sonar, el radar, la radio y la televisión, la ametralladora, el tanque, las armas químicas, el avión y el submarino, las armas de destrucción masiva, entre otros; los cuales resultaron ser en mayor o menor medida vehículos de importantes cambios, los que provocaron que el ambiente operacional del momento se volviera particularmente más complejo y dinámico.

Ahora bien, a nuestro entender la irrupción de la tecnología en la era contemporánea, especialmente la relacionada con la información, la cual evoluciona cada vez más rápidamente y en forma constante, a través de inventos tales como internet y las redes sociales, los medios masivos de comunicación, la inteligencia artificial, robótica y demás avances tecnológicos, hacen que las posibilidades que de ella se desprenden, en todo sentido y dirección, constituyan un cambio realmente disruptivo, mucho más significativo y profundo que todos los anteriores. Porque se trata de alteraciones profundas en los patrones humanos y en la forma en que se desarrolla la vida, en forma transversal, sin dejar ningún aspecto o área de la condición humana afuera de su alcance.

Estos enormes avances tecnológicos generan cambios profundos considerando las acciones en el ciberespacio, en el ámbito de la información y en el espacio aeroespacial, las operaciones integradas multidominio³, la digitalización del campo de batalla y el combate en red o *netwar*, *swarming*⁴, son claros ejemplos del impacto directo de estas inventos tecnológicos, que nos obligan a evaluar considerablemente y hacen necesaria la renovación de

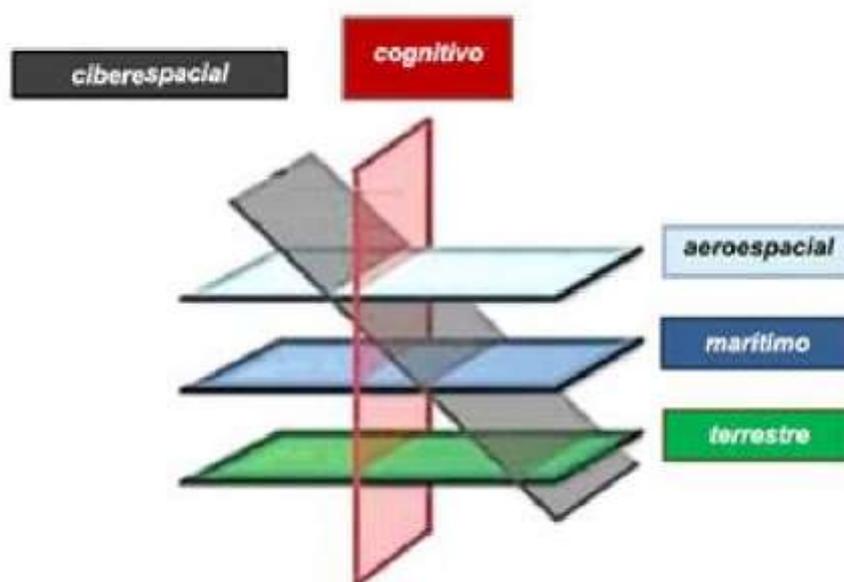
³ Se refiere a la integración buscando un empleo sinérgico de las operaciones en los ámbitos tradicionales físicos (aeroespacial, mar y tierra), a los que se suman los no físicos (el ciberespacio y cognitivo) (CESEDEN, 2020). Ver Figura 1

⁴ Es una manera aparentemente amorfa, coordinada y estratégica de golpear a un punto o a varios en particular desde todos los frentes, mediante un ritmo sostenido de fuego, tanto de cerca como desde posiciones alejadas. Esto ocurre cuando las unidades dispersas de una red de pequeñas fuerzas (y algunas grandes también) convergen sobre un blanco desde múltiples direcciones. Esta capacidad de acercamiento sigiloso sugiere que, en la guerra en red, los ataques tienen más probabilidades de realizarse en forma de *enjambres* que mediante el método tradicional de “frentes” y donde el papel de las NTIC juegan un rol fundamental. (Arquilla & Ronfeldt, 2003, pág. 42-43)

buena parte del equipamiento militar para este nuevo entorno operativo, sino también sus técnicas de empleo y tácticas asociadas, como así también revisar la doctrina constantemente y adaptar las estructuras organizacionales (Calderón, 2022).

Figura 1

Dominios del ambiente operacional moderno



Nota. Tomado de PDC-01 (A) Doctrina para el empleo de las Fuerzas Armadas españolas, Ministerio de Defensa, 2018, p. 81.

Los cambios abruptos y vertiginosos, la incertidumbre en los acontecimientos futuros, el aumento de la complejidad, lo que podríamos definir como entornos VUCA (volatilidad, incertidumbre, complejidad, ambigüedad), el número de actores en los escenarios de seguridad y la difícil imputación de la autoría de las agresiones, sobre todo en el ciberespacio y en el ámbito cognitivo, vienen a confirmar la necesaria interrelación entre la defensa y la adaptación oportuna a las tecnologías emergentes por parte de las Fuerzas Armadas (Calderón, 2022).

La naturaleza de la guerra está experimentando una transformación notable. En un futuro no muy lejano, los actores de un conflicto podrían emplear armas genéticas antes de embarcarse en acciones militares, resultando en la mutua destrucción de fuerzas humanas y el entorno donde habitan. Esto podría llevar a que una nación o país pierda su capacidad de luchar y sea conquistado sin necesidad de derramamiento de sangre (Otero, 2023).

Es así que, la irrupción de las NTIC⁵ ha significado un cambio sumamente profundo y transversal a todos los aspectos del desarrollo humano, del cual aún no se vislumbra un horizonte definido, lo que generará y de hecho ya está presentando, desafíos ético-morales y de diversas índoles, al cruzarse barreras que al menos plantean cierto recelo o reserva, como así ya han alertado sobre sus potenciales peligros para la humanidad, por ejemplo, algunos de los principales inventores de inteligencia artificial (AI) en una carta abierta firmada por los líderes de Open AI, Google, Google DeepMind y Anthropic, junto a otros 350 ejecutivos, investigadores, científicos e ingenieros expertos (País, 2023).

Es importante considerar que esa combinación entre la mente y el cerebro, abarcando tanto los aspectos abstractos como los físicos, constituye el centro de control del ser humano, donde se supervisan todos los aspectos de su existencia, tales como los pensamientos, sentimientos, conductas y decisiones. Por lo tanto, aquel que logra dominar este binomio vital de la persona, puede ejercer influencia sobre individuos y comunidades enteras (Baños, 2020).

De hecho, ya existen avances tecnológicos que buscan tener efectos sobre la mente humana, tales como artefactos de uso militar con capacidad de accionar sobre el área cognitiva en forma remota como son las armas silenciosas: sónicas, electromagnéticas, psicotrónicas, biológicas y robóticas ⁶ (Baños, 2020).

Todas ellas se usan contra la mente para inducir alucinaciones, enfermedades, mutaciones en las células humanas y hacer que el ser humano actúe como autómatas o peor aún, pudiendo en ocasiones hasta causar la muerte. Son herramientas que se han utilizado con el propósito de ejercer influencia sobre la parte cognitiva de las poblaciones y manipularlas de manera remota, logrando así los objetivos de aquellos que las emplean (Otero, 2023).

Además, algunas sociedades pasibles de ser influenciadas carecen en cierto modo, de los medios para verificar la veracidad de la información o en ocasiones simplemente no se toman la molestia o carecen de interés, lo que facilita la difusión de noticias falsas y operaciones mediáticas. Asimismo, las sociedades occidentales son altamente susceptibles a enfoques emocionales que hacen hincapié en el sufrimiento humano, por ejemplo, el impacto de ver compatriotas caídos en combate, como sucedió en la guerra de Vietnam luego de la

⁵ Según la Asociación Americana de las Tecnologías de la Información, NTIC se refiere al estudio, el diseño, el desarrollo, el fomento, el mantenimiento y la administración de la información por medio de sistemas informáticos, esto incluye todos los sistemas informáticos, Internet, telefonía celular, televisión, periódicos digitales, etc.

⁶ El *arma sónica*, es aquella que provoca una agresión electromagnética medida con radiofrecuencias que se basan en la emisión de infrasonidos de 0,1Hz a 20Hz, y de ultrasonidos a partir de 20Khz a 300Khz. Estas frecuencias son inaudibles, pero impactan en la fisiología del organismo humano.

Las *armas psicotrónicas*, son aquellas que utilizan ondas electromagnéticas para deformar la percepción humana y generar efectos psicosomáticos negativos.

ofensiva del Tet⁷, especialmente entre los segmentos más vulnerables de la sociedad, lo que provocaría una intolerancia a la violencia que se relaciona con la fuerte convicción de no tener bajas, incluso hasta rechazando las víctimas civiles y militares enemigas (Sánchez, 2019, pág. 10).

La información se ha convertido en una herramienta poderosa para influir en la opinión pública, tanto en el país propio como en el adversario. Esto es especialmente relevante en democracias, donde la misma desempeña un papel importante. La información, ya sea verídica o falsa, puede afectar la voluntad del adversario y manipular las emociones de la audiencia. Además, existe la posibilidad de negar la participación en la difusión de esta información ya que es difícil su imputación o autoría, lo que permite su uso incluso sin estar en un conflicto armado formal. (Sánchez, 2019).

Respecto de los antecedentes que pueden ser tenidos en cuenta para hacer una aproximación teórica conceptual sobre la guerra de la información (GI) u operaciones que se aplican en el ámbito informacional como parte de aquella, analizaremos diferentes conceptos y estudios realizados por varios autores que iremos citando.

Según conceptualiza Campos (2011), existen tres tipos de Guerra de la Información: el primer tipo consiste en manejar las percepciones del enemigo mediante operaciones y técnicas, a la vez que la propia organización busca protegerse de las acciones enemigas por manipular las percepciones amigas. El segundo tipo busca negar, destruir, degradar o distorsionar los flujos de información del enemigo mediante distintas acciones y medios con el objeto de desarticular sus organizaciones y que deje de actuar coordinadamente. Y por último de tercer tipo el cual busca reunir información a partir del empleo por parte del enemigo de sus sistemas de información, a la vez que se protegen los sistemas propios.

Por otro lado, podemos mencionar el concepto de uno de los autores más reconocidos en esta área, que define a la GI como un mecanismo integral para la conducción de operaciones militares, que identifica siete estrategias distintas para llevar a cabo la guerra que implica el uso de la información en diferentes formas, incluyendo la protección, manipulación, debilitamiento y negación de la misma. Estas estrategias abarcan: la guerra de mando y control, la guerra basada en la inteligencia, la guerra electrónica, la guerra psicológica, la guerra de

⁷ Consistió en una serie de ataques sorpresa llevados a cabo por el Ejército de Vietnam del Norte y el Viet Cong en 1968, durante la Guerra de Vietnam, que tomó por sorpresa a las fuerzas estadounidenses y survietnamitas. Aunque estas lograron repeler la ofensiva, la visibilización de imágenes de las bajas estadounidenses en los MCS tuvo un profundo impacto en la opinión pública, marcando un punto de inflexión en el desarrollo del conflicto, ya que cambió la percepción social sobre el mismo y contribuyó a generar una fuerte oposición a la guerra, lo que provocaría inexorablemente el fracaso de la campaña para los norteamericanos unos años después.

adquisición de información, la guerra económica de la información y la guerra cibernética (Libicki, 1995, pág. 7).

También resulta valioso hacer mención a otra concepción sobre esta particular forma de hacer la guerra moderna donde se establece que la GI es una modalidad de conflicto centrada en la gestión de la información, que puede preceder o complementar a las acciones militares en el contexto de una guerra tradicional, o bien puede ser una forma de hostilidad con fines políticos sin la ejecución de acciones armadas. Este término abarca tanto la agresión como la protección de la infraestructura física que sostiene la información (como redes de comunicación y computadoras, antenas, radares y satélites), así como los esfuerzos dirigidos a influir en las creencias y el conocimiento de los adversarios humanos (Tovar, 2011, pág. 1-2).

A lo largo de la historia, las OI se han utilizado primordialmente en tiempos de guerra y conflicto para difundir propaganda, desinformación y manipulación en el plano cognitivo. Durante la Primera y Segunda Guerra Mundial, los gobiernos emplearon técnicas de propaganda para moldear la opinión pública y mantener el apoyo a la guerra. La radio, el cine y los periódicos eran utilizados como herramientas para difundir mensajes y manipular la información.

Asimismo, en la década de 1950 el ejército de Estados Unidos desarrolla el concepto de operaciones psicológicas (PSYOP) para influir en el comportamiento de las fuerzas enemigas y los civiles. En los años 70', la Unión Soviética desarrolla el concepto de medidas activas para llevar a cabo OI encubiertas contra sus enemigos.

Durante la década de 1990, el ejército de Estados Unidos comienza a integrar las operaciones de información en su doctrina y planificación. A partir del 2000, internet y las redes sociales se convierten en herramientas cada vez más importantes para las operaciones de información.

Una década más tarde, las OI fueron utilizadas por una variedad de actores, incluyendo gobiernos, fuerzas militares, grupos terroristas y corporaciones. De acuerdo a las experiencias obtenidas por parte de USA, desde la guerra de Vietnam y con la OTAN en su participación en los conflictos de los últimos 25 años, el avance tecnológico y los cambios en las características de los conflictos, determinan que el espectro de la Información es transversal y afecta a todos los dominios. (Rosenkranz Romero, 2020)

Referido al estado actual, los cambios en el entorno de la información han sido uno de los más relevantes y profundos que ha experimentado la historia de la humanidad, producto del desarrollo de la ciencia tecnológica contemporánea, la cual ha revolucionado la velocidad del intercambio y capacidad de gestión y procesamiento de la información, teniendo un efecto

transversal a toda la sociedad por el cual se ven modificados la forma de vida, los procesos de trabajo, los sistemas transaccionales económicos y el entendimiento de ciertos fenómenos (Galizia, 2014, pág. 113).

La GI representa uno de los tipos de cambios fundamentales respecto de los actores, causas y formas en que se desarrolla la guerra, introduciendo nuevos conceptos, tácticas y procedimientos, y cambios estructurales en las organizaciones, junto con la precisión extrema, ataques remotos, el mejorado comando y control y la no letalidad. Cambios todos ellos profundos y transformadores de las ciencias militares, que propiciados por los avances tecnológicos disruptivos alcanzados en esta era, constituyen una verdadera revolución de asuntos militares⁸ (Neilson, 1997).

Con el desarrollo de las NTICs, las operaciones de información se han vuelto aún más sofisticadas. La llegada de Internet y las redes sociales ha ampliado el alcance y la velocidad de la difusión de información, lo que ha permitido una mayor influencia y manipulación de la opinión pública con la consecuente presión que ella puede ejercer sobre una determinada campaña o situación de conflicto. Los actores estatales y no estatales han utilizado estas plataformas para difundir propaganda, desinformación y narrativas falsas en tiempo real, lo que plantea nuevos desafíos y riesgos.

Los términos "guerra de información" u "operaciones de información" incluyen operaciones militares de apoyo de información realizadas por operadores especiales. A veces todavía se les llama "operaciones psicológicas", los especialistas involucrados utilizan diversos medios para afectar las percepciones y la opinión de las poblaciones locales o líderes con el fin de apoyar a los comandantes dependientes en lograr ciertos resultados en el campo de batalla (Magnuson, 2022).

También está surgiendo una nueva generación de revolucionarios y militantes radicales, con nuevas doctrinas, estrategias y tecnologías que respaldan su dependencia de las formas de organización en red y este puede ser el modo dominante de conflicto en la sociedad en el siglo XXI.

El surgimiento de la *netwar*⁹ plantea la necesidad de repensar la estrategia y la doctrina para llevar a cabo la lucha contra la misma. Las concepciones tradicionales de la guerra y los

⁸ RMA por sus siglas en inglés, es una teoría que se centra en el cambio fundamental en la forma en que las FFAA se organizan, equipan y conducen la guerra, debido a avances tecnológicos, doctrinas militares y cambios en la estrategia. Implica un cambio significativo en la manera en que se llevan a cabo las operaciones militares.

⁹ Netwar se refiere a conflictos y estrategias en los que actores no estatales, como grupos insurgentes o terroristas, utilizan redes y tecnología de la información para llevar a cabo operaciones y luchar contra estados u otros actores (Arquilla & Ronfeldt, 2001).

conflictos de baja intensidad como un proceso secuencial basado en la concentración de fuerzas, el movimiento y el combate, probablemente resultarán inadecuadas para enfrentar los conflictos de la era de la información, que son no lineales, se asemejan a enjambres y están estrechamente entrelazados con elementos militares y sociales.

En definitiva, vemos que las OI han evolucionado a lo largo del tiempo adquiriendo una nueva dimensión con las posibilidades casi ilimitadas que otorgan el auge de la era digital, el empleo de las redes sociales y medios de comunicación social (MCS). Estas operaciones se han utilizado históricamente para influir en la opinión pública y la percepción durante los conflictos, pero su alcance y efectividad han aumentado significativamente de la mano de las NTIC.

Como sostiene Zarza (2016), resulta vital para el país realizar el cambio organizacional necesario para convertir sus FFAA de tipo mecanizadas a unas informatizadas, ya que las mismas no son ajenas a estas realidades modernas donde el binomio información-NTIC juegan un papel preponderante, sino que simplemente las tienen que asimilar e implementar, de allí proviene la relevancia y fundamentación de la propuesta de este trabajo.

Para abarcar mediante un enfoque integral los desafíos que presenta una temática específica en el campo militar, como amerita la Guerra de la Información y sus operaciones; es necesario considerar tres ejes fundamentales: la doctrina, la organización y el equipamiento. Por ello, en cuanto a los alcances y limitaciones de este trabajo, el mismo se circunscribirá a los aspectos referidos con los cambios organizacionales necesarios con el objetivo de proponer la conformación de una organización particular que atienda la problemática de las OI en el nivel conjunto, y si bien como base de análisis se sustentará en el análisis doctrinario y experiencias de otros países de referencia, resultará propio de otros estudios e investigaciones la elaboración y publicación de la doctrina respectiva, como así también la consideración de las mejoras y adquisiciones de equipamiento adecuado.

En cuanto a los aportes teórico y/o prácticos al campo disciplinar, la GI ha contribuido a establecer el concepto de la *información* como un dominio transversal de la guerra, un elemento más del poder nacional, una nueva función de combate o una herramienta significativa a la hora de influir en un conflicto, según de que autor o doctrina se trate como veremos a lo largo de este trabajo.

Es así como cada vez más, las FFAA de distintos países van incorporado a su cuerpo doctrinario y en sus estructuras organizacionales a las OI, reflejando la trascendencia que la cuestión de la información ha adquirido en la guerra potenciada por el uso tecnológico. Estas doctrinas enfatizan la necesidad de proteger los sistemas de información, negar la misma al

enemigo y utilizarla para alcanzar objetivos políticos y militares, pudiendo ser aplicadas también a otros fines del quehacer nacional.

Para desarrollar este trabajo se partirá del siguiente interrogante: ¿Cuál es el diseño organizacional más adecuado de un elemento que dirija las Operaciones de Información en el nivel operacional? Y en su desarrollo se procuró dar los fundamentos básicos sobre la marcada injerencia que las OI tienen cada vez más en situaciones de conflicto y la ventaja de contar con un órgano que las conciba, dirija y asesore al respecto, analizando la doctrina y experiencia de otros países que han incorporado esta temática, para analizar las características de su estructura organizacional acorde a la realidad propia.

En función de dar respuesta al interrogante inicial se determinó un objetivo general que se orientó a analizar las características más adecuadas de una organización para dirigir en forma eficiente las OI en un estado mayor de nivel operacional. Así, empleando el método deductivo y con la finalidad de dar cumplimiento a ese objetivo general, se trazaron dos objetivos específicos, uno relacionado con el análisis de la doctrina existente en distintos marcos de referencia sobre los conceptos generales y las organizaciones respectivas de OI, y el empleo que este tipo de acciones tuvieron en diversos escenarios históricos, para comprender mejor la naturaleza compleja de estas operaciones buscando delimitar su ámbito de empleo. En segundo término, referido al análisis de los órganos y estructuras de OI en distintos países, para intentar realizar una aproximación a la descripción ideal de las características generales de un órgano de OI en el nivel operacional.

El presente estudio tiene un diseño descriptivo y se utilizó como técnica de validación el análisis bibliográfico, documental y lógico. Solo fueron utilizados documentos legales en vigencia y declaraciones oficiales provenientes de fuentes abiertas y reservadas, debido a que ello conforma el marco legal y determina la circunscripción de referencia para el accionar de las FFAA en territorio nacional ante la conformación de un eventual TO.

Capítulo 1. Análisis doctrinal y del empleo de las OI en distintos escenarios.

“Para el cambiante carácter de la guerra en la era de la información, se requerirán fuerzas militares que reconozcan que apoderarse o controlar el terreno es secundario... y que capturar percepciones es el nuevo "terreno llave" en los conflictos actuales, ya que lo moral es tres veces más importante que lo material.”

General J. M. Mattis (7 July 2009).¹⁰

En este capítulo, se analizará la doctrina de varios países que se encuentran a la vanguardia en materia de OI para cotejar sus definiciones al respecto y consideraciones en cuanto a su empleo, tanto en el marco global y regional, así como el estado sobre la doctrina de las Fuerzas Armadas Argentinas (FFAA) al respecto. Además, se considerarán los casos históricos recientes donde aparecen este tipo de operaciones y sus resultados o efectos.

La necesidad de comprender las OI y crear conciencia respecto de su relevancia en todos los niveles, radica en su capacidad para influir en el resultado de una confrontación o puja de intereses, haya llegado a su estadio armado o no necesariamente, y en su capacidad para moldear la percepción de la realidad en medio de la confusión y el caos de la guerra. Para abordar adecuadamente este tema, es esencial analizar tanto la doctrina y las teorías que sustentan estas operaciones como los casos históricos que ejemplifican su alto impacto e influencia en las campañas.

En resumen, este capítulo establece las bases para una comprensión profunda de las OI en los conflictos armados, abordando tanto la doctrina que las respalda como los casos históricos que las ilustran. A través del análisis de la teoría y la práctica, buscaremos hacer las consideraciones correspondientes sobre cómo la información y su aplicación intencionada, se ha convertido en un arma poderosa en el escenario de la guerra contemporánea.

1.1 Doctrina de Operaciones de Información en países de referencia

ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE

El reglamento de Doctrina Conjunta Aliada para Operaciones de Información AJP 3-10 (2009), define a las OI como aquellas acciones planificadas para influir en la percepción, el juicio, el comportamiento y la comprensión de individuos, grupos, organizaciones o sistemas,

¹⁰ Comandante Aliado Supremo de Transformación (SACT) de la OTAN. El SACT es responsable ante el Comité Militar, de la transformación y el desarrollo de la OTAN para garantizar que sea capaz de enfrentarse a los desafíos presentes y del futuro.

en beneficio propio o de la Alianza, mientras se protege la propia información y las operaciones. Estas acciones buscan crear, reforzar, proteger o explotar la información o negar, degradar y/o destruir la del adversario, y pueden emplear la fuerza y otras formas de poder en apoyo de los objetivos (OTAN, 2009, pág. 1-3).

A su vez, incluye como capacidades, herramientas o técnicas constitutivas de las OI a las Operaciones Psicológicas (PSYOPS), la Disuasión, mediante la presencia, el despliegue o actitud de una fuerza, Operaciones de Seguridad, incluye seguridad de la información, Acciones de Engaño, Guerra Electrónica, Destrucción Física, Identificación de principales actores y sus interrelaciones, Operaciones en Redes Informáticas, Cooperación Cívico-Militar, y Asuntos Públicos. Si bien esta última no es una capacidad de las OI, pero es necesario coordinar el mensaje correcto a distribuir a las audiencias y todas ellas se tratan en la Junta de Coordinación de OI que está integrada por representantes de distintas agencias (OTAN, 2009, pág. 1-8).

Es importante destacar que, relacionado con el enfoque sobre OI, las naciones pertenecientes a la OTAN, han incorporado a la "Información" como una función de combate en el ámbito del accionar militar conjunto, resultando primordial para la toma de decisiones y la forma en que se informa e influye a las audiencias. La función de información contribuye con los comandantes y el personal que aplica o utiliza la información a comprender el impacto de las tecnologías emergentes y disruptivas, junto con otras funciones, para informar e influir en las percepciones, comportamientos y toma de decisiones de las audiencias relevantes (OTAN, 2023, pág. 14).

Recientemente se ha realizado la publicación de una actualización del reglamento Doctrina Conjunta Aliada para Operaciones de Información AJP 10.1 (2023) que define a las OI como una función de asesoramiento encargada de analizar, planificar, evaluar e integrar actividades de información para crear efectos deseados en la voluntad, comprensión y capacidad de adversarios, posibles adversarios y audiencias en apoyo de los objetivos de la misión (OTAN, 2023, pág. 25).

El entorno de información se segmenta en tres dimensiones: cognitiva, física y virtual, donde la cognitiva es la dimensión decisiva porque es donde se crean los efectos en el pensamiento de las personas, lo que a su vez impulsa sus comportamientos y decisiones. Todas las acciones en las demás dimensiones afectan en última instancia a la dimensión cognitiva (OTAN, 2023, pág. 105).

Define las capacidades relacionadas con las OI dividiéndolas en: capacidades de comunicación, que incluye PSYOPS y asuntos públicos, como responsable de promover los

objetivos militares de la OTAN siendo parte de las comunicaciones estratégicas, e incluye como capacidades o técnicas adicionales a las operaciones en el ciberespacio, guerra electrónica, cooperación e interacción cívico-militar, destrucción física, operaciones de seguridad y engaño, seguridad de la información, empleo de tecnologías emergentes y disruptivas¹¹ (OTAN, 2023, pág. 30-37).

Además en la misma publicación se introducen cambios sobre el enfoque referido a la comunicación estratégica, con la creación del Directorio de Comunicación Estratégica (StratCom) que se constituye como el área J10 StratCom del el Estado Mayor de nivel operacional y establece cómo se efectúa la integración vertical de StratCom, en conjunto con la necesaria integración horizontal de OI en el órgano de asesoramiento de ese nivel, a través de la orientación de los documentos respectivos que le dan marco doctrinario, la guía de implementación y el plan de comunicaciones integradas o anexo StratCom (Anexo SS) al Plan de Campaña correspondiente. También, amplía y agrega los cuatro pasos del proceso de planeamiento de las OI: analizar, planificar, integrar y evaluar (OTAN, 2023, pág. 13).

Respecto de la capacitación específica para el personal que integra los elementos de OI en el ámbito de la Defensa, el Grupo Conjunto de Actividades de Información (JIAG) dicta los siguientes cursos: Curso de Operaciones de Información Conjuntas, Curso de Operaciones Psicológicas Militares, Curso de Análisis de Audiencias, Curso Básico de Operaciones de Información y el Curso de Comunicadores de la Defensa (OTAN, 2023, pág. 42).

ESTADOS UNIDOS DE AMÉRICA

Ante la evidente trascendencia que ofrece el manejo intencionado de la información en distintos conflictos, propiciado por esta era tecnológica e hiperconectada actual que evoluciona y se desarrolla continuamente, el Departamento de Defensa (DoD) de los Estados Unidos (EEUU), considera a la información como un recurso tan poderoso, que bien se la podría considerar como un elemento más del poder nacional y por lo tanto, el DoD debe estar preparado para orientar el esfuerzo en tal sentido, buscando sincronizar medios y acciones como parte de un esfuerzo conjunto de todo el gobierno” (US Department of Defense, 2016).

De acuerdo con el Manual de Operaciones de Información Conjunto, las OI constituyen la utilización combinada de guerra electrónica, operaciones de redes informáticas, operaciones

¹¹ Según BIT revista profesional sobre tecnología y transformación digital, abarcan la Inteligencia Artificial, la computación cuántica, la gestión de la información, los sistemas aeroespaciales, el armamento de energía dirigida, la nube de combate, la integración operativa de vehículos tripulados y no tripulados, las armas cibernéticas, los macro datos, la robótica, la generación y almacenamiento de energía, los meta materiales y técnicas de fabricación avanzada, las capacidades no letales, etc.

psicológicas, estrategias de engaño militar y operaciones de seguridad, que se coordinan de manera conjunta para influir, interrumpir, corromper o tomar el control de la toma de decisiones de adversarios humanos e inteligentes, al mismo tiempo que se brinda protección a las propias fuerzas y civiles (Kuehl, 2014, pág. 8).

Otro concepto elaborado por el EMCFFAA de EEUU establece que las OI se centran en la utilización coordinada de una variedad de capacidades relacionadas con la información (CRI) para lograr efectos específicos. Su objetivo es influir en la toma de decisiones de audiencias específicas, ya sea perturbando, corrompiendo o usurpando la misma. Las OI no se basan en el uso individual de estas capacidades, sino en su integración de todas ellas para amplificar su impacto. Esto incluye una amplia gama de capacidades militares, como comunicación estratégica, coordinación interagencial, asuntos civiles, cibernética, operaciones psicológicas, seguridad de la información, inteligencia, engaño militar, seguridad, operaciones técnicas especiales y otras, de acuerdo a la situación en cuestión (EMCFFAA EEUU, 2014).

Estas operaciones de amplio espectro se consideran constantes, ya que requieren una preparación anticipada, especialmente de naturaleza analítica. Preparar el terreno para las OI involucra actividades como la recopilación de inteligencia, el reconocimiento y la vigilancia, así como la planificación en el espectro electromagnético, con el fin de lograr efectos rápidos al inicio del conflicto (EMCFFAA USA, 2014).

En cuanto a las organizaciones relacionadas con OI, existe la célula J-39 dentro del estado mayor conjunto que es asistido por el Centro Conjunto de Operaciones de Información (Kirschbaum, 2021), la cual se compone de diversos agentes, representantes y especialistas de todas las áreas, medios y capacidades que la componen.

Como última consideración de las OI, en relación con los medios de comunicación, el país desarrolla una intervención gubernamental previa que establece el orden de determinadas frecuencias de operación, con una significación política en la cesión de licencias de uso. Este control si bien puede resultar menor a los efectuados en países de oriente, resulta de todos modos lo suficientemente efectivo para salvaguardar de manera preventiva los intereses nacionales y coordinar la narrativa y la comunicación estratégica vitales para las OI.

REINO UNIDO DE GRAN BRETAÑA

En cuanto a la contribución del Ministerio de Defensa del Reino Unido a la *Campaña de Información*¹², esta incluye todas o algunas capacidades militares, en cualquier nivel, para

¹² Se refiere a un conjunto de acciones planificadas y coordinadas que buscan influir en la percepción, la toma de decisiones y el comportamiento de audiencias específicas en apoyo de los objetivos estratégicos y

influenciar audiencias y prevenir que ellas puedan imponer su voluntad. Consta de dos partes: Operaciones de Información y Operaciones con medios de comunicación, las cuales deben apoyarse mutuamente, las cuales a su vez pueden ser complementadas con otras acciones militares, tales como diplomacia defensiva, despliegue de fuerzas o directamente el empleo efectivo de las mismas en el lugar necesario (UK JDCC, 2002).

Las campañas de información, por lo tanto, son aplicables a todo el espectro de tensión y en todo tipo de operación, desde la prevención de un conflicto hasta la lucha armada. Tiene cuatro objetivos principales:

- Durante la etapa previa a un conflicto puede buscar, como parte de la estrategia interagencial de gobierno, predisponer y persuadir determinadas audiencias de los beneficios de un curso de acción particular, capaz de prevenir una situación que podría devenir en una crisis.
- Durante una situación de crisis, su objetivo es persuadir audiencias sobre las ventajas de un curso de acción, mientras se las convence de no adoptar otro distinto, el cual podría conducir a un conflicto.
- Mientras sucede el conflicto, el objetivo principal puede ser presionar a los adversarios de adoptar un curso de acción deseado, aislarlos y debilitar su voluntad de continuar con la agresión. Además, asegurar o persuadir a los aliados y actores neutrales sobre las ventajas de un determinado curso de acción.
- En una situación post conflicto la campaña de información persigue el objetivo de asegurar la población y el liderazgo, reestableciendo la confianza en los procesos políticos y fomentar la estabilidad como parte de una actividad interagencial gubernamental de reconstrucción.

De acuerdo a la doctrina británica, las OI se definen como las acciones coordinadas ejecutadas para influenciar un adversario real o potencial en apoyo a los objetivos políticos y militares afectando su voluntad, cohesión y proceso de toma de decisiones, a través de la intervención de sus sistemas de información y sus procesos relacionados, mientras que se protegen a los decisores propios y los procesos de toma de decisiones (JDCC, 2002).

Las OI consisten básicamente en dos actividades principales:

- Actividad de Influencia, por la cual se busca afectar la voluntad, incluyendo Operaciones Psicológicas, Presencia y actitud militar adoptada buscando un efecto

políticos del Reino Unido. Estas campañas tienen como objetivo utilizar la información como una herramienta estratégica para lograr resultados deseados en el ámbito militar y político (JWP 3-80).

disuasivo, Operaciones de Seguridad, Engaño militar, Guerra Electrónica, Destrucción Física, Operaciones cibernéticas; Operaciones en los MCS y la cooperación cívico-militares (CIMIC).

- Actividad contra el Comando, que tiene como objetivo el comando y control enemigo, que empleará normalmente las herramientas de destrucción física sobre un objetivo específico, el uso de tecnologías emergentes¹³, acciones ofensivas de Guerra Electrónica y Operaciones cibernéticas (JDCC, 2002, pág. 2-6).

La célula de OI es apoyada por el Grupo de Planeamiento de OI, el cual está encabezado por el oficial de OI e integrado por representantes de las capacidades correspondientes a las Actividades de Influencia y Contra Comando, así como de los demás componentes de las fuerzas. Normalmente incluirá al C-1, C-2, C-3, C-4, C-5, Operaciones con MCS, CIMIC, PSYOPS, GE, asesor político y legal (JDCC, 2002, pág 4-2).

CHINA

Resulta adecuado remarcar la diferencia conceptual entre occidente y oriente, en la que muchos analistas chinos entienden a la GI como un fin en sí mismo, mientras que para los expertos militares norteamericanos es una forma más de combatir o es un medio de contribuir al logro de los objetivos y estados deseados. Según Wang Pufeng “la guerra de información se refiere a un tipo de guerra y a un tipo de patrón de la guerra, mientras que el concepto de GI para los norteamericanos se refiere a ciertas operaciones y un patrón operacional.” (Troxler, 2022)

Según ciertos autores chinos de referencia definen a las OI como el uso de diferentes tipos de técnicas, medios y capacidades, para lograr la desinformación o la destrucción de los sistemas de información del enemigo, particularmente los de comando y control, afectando la toma de decisiones del enemigo y al mismo tiempo el uso de todos los medios posibles para asegurar que los propios sistemas de información no sean dañados. (Thomas, 2004, pág. 14).

Actualmente en China, el concepto de GI sigue evolucionando hacia lo que se conoce como la *Guerra Cognitiva*, producto del desarrollo de la Inteligencia Artificial (IA), la neurociencia y las aplicaciones digitales como las redes sociales. Afirman que, en el futuro, será posible influir en el cerebro del enemigo para afectar directamente a la cognición humana. De este modo, se crea la posibilidad de someter al enemigo sin luchar, ya sea por medios

¹³ Armas de energía dirigida: radio frecuencia, laser, acústica y otras armas no letales, como alternativa al uso directo de la fuerza con la posibilidad de reducir el daño colateral y por ende mayor aceptabilidad pública.

técnicos o informativos. Al igual que los países de occidente distinguen a la GI en tres ámbitos: el físico, el informativo y el cognitivo, siendo el dominio cognitivo el eje de la guerra en un futuro (Troxler, 2022).

El presidente chino expuso la teoría de la "inteligentización" o guerra inteligente¹⁴, como evolución de la guerra informacional, en su informe al 19º Congreso del Partido, en octubre de 2017, donde instó al área de Defensa a acelerar el desarrollo de la inteligentización militar y mejorar las capacidades de operación conjunta en todos los dominios basadas en sistemas de información en red (Mallick, 2021, pág. 5).

Por su parte, Qi Jianguo, ex subdirector del Estado Mayor del Ejército Popular de Liberación (EPL), ha sostenido que aquellos que lideren en el desarrollo de tecnologías de IA de última generación tendrán el control sobre el centro de la defensa nacional: la cognición humana. Además, argumentan que la intervención directa en el cerebro del enemigo o su control inconsciente pueden causarle daño mental, confusión y alucinaciones, forzándolo a abandonar las armas y rendirse. (Takagi, 2022).

RUSIA

A diferencia de otros actores internacionales, declara el uso de la guerra de la información como estrategia militar definida mediante la última Doctrina Militar de la Federación de Rusia. El hecho de que desde 2014 la GI forme parte de la Doctrina Militar, refleja que el Kremlin considera que Rusia está involucrada en una guerra de la información a gran escala. (Milosevich-Juaristi, 2017)

Para Rusia, la GI es un concepto amplio e integrado que conforma un conjunto de sistemas, métodos y tareas para influir en la percepción y el comportamiento del enemigo, la población y la comunidad internacional en todos los niveles, a través de una amplia gama de actividades, capacidades o herramientas más o menos similares a los países de la OTAN.

Un concepto sobre las OI las define como “una batalla entre estados que involucra el uso de armas exclusivas de información en la esfera de los modelos de información. El objetivo final del efecto de un arma de información es el conocimiento de un sistema de información específico y el uso intencionado de ese conocimiento para distorsionar el modelo del mundo de la víctima” (Thomas, 2005, pág. 78).

¹⁴ La “guerra inteligente” se centra en el uso de la inteligencia artificial (IA) y se caracteriza por cuatro rasgos clave: mayor capacidad de procesamiento de la información, toma de decisiones rápida, uso de *swarming* y guerra cognitiva (Mallick, 2021).

De acuerdo con el objetivo deseado, la guerra de la información puede ser de dos formas: Psicológica, para afectar al ámbito militar y a la población, desarrollado en forma permanente y Tecnológica, para afectar sistemas técnicos que reciben, reúnen, procesan y transmiten información, que se lleva a cabo durante los conflictos armados en tiempos de guerra. (Kvachkov, 2004)

Cabe mencionar sin dudas, los conceptos referidos a la GI de Gerasimov¹⁵ (2016), quien sostiene la idea de reducir el empleo militar convencional, potenciando otras capacidades no cinéticas, dándole gran preponderancia al uso de la red mundial de Internet para lograr un impacto masivo en la conciencia de la población objetivo. Y reconoce que las capacidades relacionadas con la información se han convertido en uno de los tipos de armas más eficaces, pudiendo hasta desestabilizar la situación general de un país desde adentro en muy poco tiempo. De esta manera, las técnicas indirectas y asimétricas propias de las guerras híbridas permiten afectar la soberanía efectiva de un país sin necesidad de tomar su territorio.

Y agrega, que de acuerdo a la experiencia (Georgia y Siria) son evidentes las ventajas de lograr los objetivos con el mínimo empleo posible del instrumento militar sobre el adversario, disminuyendo su capacidad militar y económica, a través de acciones que tengan efectos psicológicos por medio de la información, generando una oposición interna, por medio de la insurgencia y métodos subversivos (Gerasimov, Based on the experience of Syria, 2016), conceptos que en el conflicto reciente con Ucrania no han resultado tan efectivos o al menos han sido puestos bajo consideración.

MARCO REGIONAL (BRASIL – CHILE)

En el marco regional las Fuerzas Armadas de Brasil, definen a las OI como la coordinación integrada de Capacidades Relacionadas con la Información (CRI) que se integran con otras operaciones, ya sea como apoyo o como parte central del esfuerzo, con el propósito de informar e influir en individuos o grupos que pueden afectar de manera positiva o negativa la consecución de objetivos políticos y militares. Además, se busca comprometer el proceso de toma de decisiones de adversarios o posibles adversarios, todo ello sin comprometer la integridad de nuestro propio proceso (MD30-M-01, Ministério de Defesa, 2020)

Respecto de Chile su actual doctrina conjunta de OI está representada por el DNC 3-7 “Operaciones de Información Conjunta” de 2014 y que no ha sido aprobada, es decir, que aún

¹⁵ Jefe del Estado Mayor de las FFAA rusas y Primer viceministro de Defensa. Es conocido por su contribución a lo que se conoce como la "Doctrina Gerasimov" o "Guerra Híbrida", que se refiere a la combinación de tácticas militares convencionales y no convencionales, incluyendo la desinformación y la guerra de información, para lograr los objetivos políticos y estratégicos de Rusia (Gerasimov, 2013).

es un proyecto. Está basado en la doctrina OTAN AJP -3.10 del año 2009. Lo anterior se declara en la introducción de la doctrina nacional conjunta, de la cual se hizo simplemente una traducción con los cambios necesarios para su mejor comprensión y no una adaptación. (Ministerio de Defensa, 2014, pág. 13).

ARGENTINA

La doctrina local, sólo menciona brevemente en el reglamento sobre el Empleo de Terminología para la Acción Militar Conjunta, donde define a la GI como:

Uso y manejo de la información con el objetivo de conseguir una ventaja competitiva sobre un oponente, pudiendo consistir en la recolección de información táctica, en la confirmación de la veracidad de la información propia, en la distribución de propaganda o desinformación a efectos de desmoralizar al enemigo, socavar la calidad de la información de la fuerza enemiga y negarle las oportunidades de recolección de información, pudiendo adquirir diversas formas (EMCFFAA, 2019, pág. 95).

Además, es importante destacar que como primer paso hacia la implementación de los cambios organizacionales requeridos para abordar las OI y desarrollar la doctrina correspondiente, conforme al planeamiento estratégico militar definido a partir de la DPDN 2021, el Estado Mayor Conjunto de las Fuerzas Armadas (EMCFFAA) ha comenzado a trabajar en el último proyecto del reglamento PC 20-01 "Planeamiento para la Acción Militar Conjunta Nivel Operacional" 2023. En este proyecto ya se introducen conceptos como la concepción estratégica de "restricción de área" mediante un diseño multicapa, con operaciones multidominio, que incluyen a las OI como parte integral de las acciones a llevar a cabo en esa concepción.

Así también, se ha comenzado a contemplar, aunque de manera incipiente la posibilidad de establecer estructuras organizativas interdisciplinarias y de carácter transversal a varias áreas y en coordinación con distintas agencias en el Estado Mayor de un Teatro de Operaciones, especialmente en situaciones particulares o que requieran una especificidad mayor debido a una complejidad determinada, entre ellas el uso de las OI. Estas estructuras tienen el propósito de respaldar la ejecución de operaciones de este tipo y, al mismo tiempo, servir de base para la formulación de la doctrina correspondiente (EMCFFAA, 2023).

Haciendo un somero análisis de aspectos legales dentro de las consideraciones doctrinarias, actualmente las OI no están comprendidas en el Derecho Internacional, lo que significa que no se consideran acciones bélicas. A diferencia de otros aspectos de un conflicto armado, el Derecho Internacional no hace referencia a las OI como parte de sus regulaciones.

Un ejemplo de esto es el Artículo 41 de la Carta de la ONU, que no categoriza el uso de las mismas como un acto de guerra, dado que interrumpir las comunicaciones del enemigo no implica el uso de fuerza armada.

En el marco del Derecho Internacional de los Conflictos Armados (DICA), que establece criterios para el uso de la fuerza durante la guerra, se aplican principios como la necesidad, la proporcionalidad, la discriminación y la humanidad. Los Convenios de Ginebra y de La Haya demarcan las condiciones para el DICA, pero no establecen restricciones específicas sobre las OI.

Por el contrario, estas operaciones pueden ser compatibles con principios éticos y legales. Por ejemplo, cumplen con el principio de proporcionalidad al cuantificar el valor de un objetivo militar frente a las vidas y daños causados ya que son mínimos o nulos. También respetan el principio de discriminación, ya que se dirigen a objetivos con valor militar en lugar de objetivos exclusivamente civiles. Además, las OI pueden contribuir a reducir el sufrimiento humano durante la guerra buscando lograr los objetivos reduciendo o evitando el empleo de la fuerza, lo que concuerda con el principio de "humanidad" del DICA. En resumen, las OI no se consideran actos de guerra y pueden ayudar a cumplir con principios éticos y legales en el contexto del conflicto armado (Clark, 2010, pág. 9)

1.2 Empleo de las OI en distintos escenarios históricos

Irak 2003 (Iraqi Freedom)

Durante la guerra en Iraq, las OI se llevaron a cabo no solo a niveles estratégicos y operacionales, sino también en Brigadas y Unidades Tácticas. Los comandantes tácticos se dieron cuenta de la necesidad de adaptar las OI a las circunstancias locales y coordinarlas con el plan de Operaciones de Información a nivel operacional. Las unidades que tenían un grupo coordinador de OI en el Estado Mayor demostraron un mayor éxito. En el nivel de subunidad, el Jefe de Sección Apoyo se encargó de coordinar las OI para respaldar la maniobra de la unidad. Esto resalta la demanda de la coordinación efectiva de las OI en todos los niveles para lograr el éxito en las operaciones militares. (Saul, 2005, pág. 7).

Además, se implementó una eficiente gestión de la prensa que compartía intereses militares y apoyaba objetivos políticos para contrarrestar la propaganda iraquí. Este enfoque demostró una nueva dimensión del periodismo y cómo la organización de la información pública puede controlar el flujo de información en un conflicto armado que generó rechazo en la opinión pública mundial. Los reporteros estaban incrustados en las columnas de marcha y

transmitían en tiempo real lo que ocurría en primera línea, destacando la injerencia de la gestión mediática en los conflictos contemporáneos. (Ceballos, pág. 6)

Georgia (2008)

La estrategia militar rusa se basó en una rápida superioridad de medios en tierra, aire y mar, respaldada por operaciones cibernéticas, guerra electrónica y operaciones de información. Este enfoque reflejó la doctrina militar soviética y demostró la capacidad de Rusia para influir en su periferia mediante una fuerza militar significativa, a pesar de las deficiencias y problemas encontrados durante la operación.

El conflicto con Georgia impulsó una revisión y transformación de los esfuerzos de guerra de información en Rusia, incluyendo la intensificación de la explotación de Internet como medio de control de la información. Surgió el debate sobre la creación de Tropas de Información que abarcarían hackers, periodistas, especialistas en comunicaciones estratégicas y operaciones psicológicas, así como lingüistas para abordar las deficiencias percibidas en la capacidad de Rusia en este ámbito.

En resumen, el conflicto de 2008 marcó un punto de inflexión en la estrategia de guerra de información de Rusia, que incluyó la coordinación de ataques cibernéticos con operaciones militares y llevó a la consideración de la formación de Tropas de Información para fortalecer sus capacidades en este campo. (Pallin y Westerlund, 2009).

Crimea 2014

La invasión rusa de Crimea en 2014 proporciona un estudio de caso histórico de actividades de guerra híbrida que involucran operaciones terrestres y de OI. Las acciones rusas involucraron la difusión de noticias falsas a través de agencias de noticias rusas y canales de televisión. También utilizaron bots en línea para crear cámaras de eco y difundir información errónea en un esfuerzo por influir en la percepción pública. Estos métodos innovadores resaltan la capacidad de Rusia para adaptarse en el campo de batalla de la información. Es importante destacar que es probable que no hayan revelado todas sus estrategias, lo que debe ser una preocupación para los analistas occidentales. (Vergara, 2021)

Los analistas occidentales emplearon métodos socio-informáticos para identificar las fuentes de información que abastecían a conjuntos de cuentas de bots (conocidas como "sembradoras de información") y analizar las estrategias de comunicación y coordinación utilizadas. Durante este evento, las botnets utilizadas para difundir propaganda experimentaron

una evolución, volviéndose más sofisticadas y coordinadas. Su objetivo era influenciar directamente a audiencias rusas específicas y, al mismo tiempo, confundir y demorar las decisiones de los líderes políticos occidentales. (Woolley, 2017).

Israel – Palestina 2021

El conflicto de mayo de 2021 en la franja de Gaza ha sido catalogado por Israel como la "primera guerra de inteligencia artificial", aunque su característica más destacada fue la desinformación. A pesar de las capacidades avanzadas de Hamas, su objetivo principal no era una victoria militar sobre Israel, sino político e informativo. Utilizaron tácticas como escudos humanos y campañas de desinformación para reforzar su posición entre los palestinos y deslegitimar a Israel.

Israel se centró en objetivos operacionales y no respondió eficazmente en el ámbito de la información, permitiendo que la desinformación proliferara en su contra en las redes sociales. Como resultado, ambas partes consideran que han ganado, lo que perpetúa el conflicto.

Israel empleó tecnologías innovadoras, como la inteligencia artificial para identificar blancos, sistemas de comando y control y armas de precisión para aumentar la transparencia en la información compartida y obtenida. Sin embargo, el conflicto en Gaza, que involucra a grupos terroristas en un espacio reducido, contrasta con la preparación de Estados Unidos para batallas multidominio contra grandes potencias.

La competencia global no se limita a grandes operaciones militares, ya que actores estatales utilizan fuerzas no convencionales, como milicias respaldadas por Irán, "hombres verdes" rusos, contratistas militares privados y flotas pesqueras chinas.

Este conflicto puso de manifiesto la vulnerabilidad de Israel al ceder el control de la información a su adversario. Hamas logró desacreditar a Israel mediante la desinformación, explotando la susceptibilidad de las democracias a la opinión pública. La guerra en Gaza destaca la relevancia de la competencia informativa en los conflictos modernos y la necesidad de desarrollar estrategias efectivas de información y desinformación en el campo de batalla. (Wald, 2021)

Rusia – Ucrania 2022

La simple observación del conflicto en Ucrania, nos muestra un combate de narrativas entre los contendientes, que se juega en la mente de las opiniones públicas propias y ajenas.

Comprobamos empíricamente cómo toda noticia relativa a la guerra, procedente de fuentes cercanas a los contendientes, forma parte de una estrategia de comunicación bien diseñada y dirigida para influir sobre las decisiones de los líderes políticos occidentales, a través de las emociones de sus opiniones públicas (Pérez, 2022).

Ucrania está llevando a cabo una campaña de acusaciones de violaciones del derecho internacional de los conflictos armados, generando presión en Occidente para obtener apoyo mediático, económico y de armamento. La narrativa ucraniana ha logrado eliminar la perspectiva rusa a través de la censura y el rechazo social de explicaciones alternativas (García Servert, 2022).

Este enfoque está produciendo resultados significativos en la percepción global del conflicto lo que ha equilibrado la enorme disparidad de poderío militar entre ambos países, más allá del apoyo militar recibido por Ucrania. De esta manera vemos como las operaciones de información, más efectivas y poderosas de occidente apoyando a Ucrania, han sido un factor multiplicador del poder de combate logrando que esa amplia desventaja inicial de las fuerzas ucranianas frente una de las potencias militares y económicas más grandes del mundo, no se vea reflejada en lo real haciendo que al menos, por el momento, el conflicto perdure en el tiempo.

Capítulo 2. Aspectos generales sobre el diseño de un órgano director de Operaciones de Información de nivel operacional

"La guerra de la información es una guerra por el control de la percepción."

John Arquilla.¹⁶

2.1 Características principales de las Operaciones de Información

Luego de haber analizado la doctrina de los principales países respecto de las OI estamos en condiciones de reconocer algunos rasgos distintivos de este tipo de operaciones:

- **Multidimensionalidad:** Las OI abarcan diversos dominios, como el ciberespacio, el espacio electromagnético, el dominio cognitivo, los medios de comunicación, entre otros.
- **Uso de la información:** Las OI se centran en la gestión y el uso de la información para influir en las percepciones, actitudes y comportamientos de las audiencias objetivo. Esto puede incluir la difusión de información, desinformación, propaganda y operaciones psicológicas.
- **Apoyo a objetivos estratégicos:** dado los posibles efectos provocados por este tipo de acciones en el ámbito de la información, se utilizan para respaldar los objetivos estratégicos de un país o una organización militar. Pueden incluir la promoción de la legitimidad propia y la deslegitimación del adversario, contribuyendo significativamente a la definición de un conflicto, pudiendo ser en particulares circunstancias decisivas.
- **Coordinación:** Las OI requieren una coordinación efectiva entre diversos elementos, como la inteligencia, las operaciones cibernéticas, la guerra electrónica, la propaganda y las operaciones psicológicas. Esto asegura un enfoque integral necesario para el logro de los efectos deseados.
- **Adaptabilidad:** Las OI son altamente adaptables dadas las diversas capacidades que las conforman y pueden cambiar rápidamente para aprovechar las oportunidades emergentes o para contrarrestar las amenazas. Esto requiere una concepción flexible por parte de quienes las llevan a cabo.

¹⁶ John Arquilla es profesor y director de la cátedra Análisis de Defensa, en la Escuela de Postgrados de la Armada de los Estados Unidos de América y analista de RAND Corporation. Su investigación se centra en la interpretación de las implicancias de la revolución de la información para la organización militar, la doctrina y la estrategia, siendo ampliamente conocido por desarrollar los conceptos de ciberguerra, *netwar* (guerra en red) y *swarming* (tácticas de enjambre). (Naval Postgraduate School, <https://nps.edu/web/bix/speakers#arquilla>)

- Aplicación en todos los niveles: Las OI pueden llevarse a cabo en todos los niveles de la conducción, desde el estratégico hasta el táctico. Se adaptan a las necesidades y objetivos específicos de cada nivel.
- Uso de tecnología avanzada: Con el avance de la tecnología, las OI han evolucionado para incluir el uso de ciberataques, desinformación en línea y otras tácticas modernas. Se apoyan en sistemas de información y comunicación avanzados.
- Evaluación continua: Las OI requieren una evaluación continua de su efectividad y un ajuste constante de la estrategia en función de los resultados. El monitoreo y la adaptación son esenciales.
- Impacto en la percepción: En última instancia, las OI buscan influir en la percepción de las audiencias objetivo, lo que puede tener un impacto significativo en el curso de un conflicto o en la consecución de objetivos estratégicos.

El Entorno de la Información

El entorno de información es el conjunto de individuos, organizaciones y sistemas que recopilan, procesan, difunden o actúan sobre la información. Este entorno consta de tres dimensiones interrelacionadas que interactúan continuamente con individuos, organizaciones y sistemas. Estas dimensiones son la física, la informativa y la cognitiva.

La dimensión física está compuesta por sistemas de comando y control (C²), decisores clave y la infraestructura de apoyo que permite generar efectos. Es la dimensión donde residen las plataformas físicas y las redes de comunicación que las conectan. La dimensión física no se limita únicamente a sistemas y procesos militares; es una red difusa conectada a través de fronteras nacionales, económicas y geográficas.

La dimensión informativa abarca el lugar y la forma en que se recolecta, procesa, almacena, difunde y protege la información. Es el ámbito donde se ejerce el C² de las fuerzas militares y donde se comunica la intención del comandante. Las acciones en esta dimensión tienen un impacto en el contenido y flujo de la información.

La dimensión cognitiva engloba la mente de aquellos que transmiten, reciben y responden o actúan en función de la información. Se refiere al procesamiento de la información, la percepción, el juicio y la toma de decisiones de individuos o grupos. Estos elementos están influenciados por muchos factores, que incluyen creencias individuales y culturales, normas, vulnerabilidades, motivaciones, emociones, experiencias, valores, educación, salud mental, identidades e ideologías. Definir estos factores influyentes en un

entorno dado es fundamental para comprender cómo influir de la mejor manera en la mente del decisor adversario y crear los efectos deseados. Como tal, esta dimensión constituye el componente más importante del entorno de la información (EMCFFAA USA, 2014).

Las OI como elementos del diseño operacional

Las Operación de Información deben apoyar múltiples líneas de operación (LO) y en ocasiones puede ser la LO que tiene la prioridad del apoyo de otras LO para alcanzar el cumplimiento de un determinado punto decisivo (PD). Las OI también puede respaldar numerosas líneas de esfuerzo (LE) cuando la posición relativa de un enemigo o adversario tienen poca significación, como ser las operaciones contrainsurgencia u operaciones de estabilización. Las OI integran las capacidades relacionadas con la información (medios) con otras LO y LE (modos) para crear un efecto deseado en un adversario o posible adversario y lograr un objetivo (fines) (EMCFFAA USA, 2014).

Capacidades relacionadas con la OI

Las capacidades, herramientas y técnicas que se podrían considerar como base de las OI, en función de la doctrina analizada en el Capítulo I, adaptada a la realidad de nuestro instrumento militar terrestre (IMT) podemos enumerarlas en las siguientes:

- Guerra Electrónica
- Ciberdefensa
- Operaciones de Seguridad / Seguridad de la Información
- Comunicación Social Aplicativa al Combate (COSACO)
- Velo y Engaño
- Destrucción Física/operaciones de combate clásicas
- Comunicación Institucional
- Asuntos Civiles
- Asuntos Jurídicos
- Inteligencia

Las acciones coordinadas en estas operaciones se centran en la influencia directa sobre la voluntad de las personas, impactando en su conocimiento y en las habilidades que están estrechamente relacionadas con la voluntad. Estas operaciones son aplicables en una amplia

gama de situaciones militares y al hablar de voluntad, nos referimos a aspectos como la motivación, objetivos, actitudes, creencias y valores (Bilibio, 2017, pág. 11-12).

2.2 Descripción de las características generales de un órgano director de Operaciones de Información

En relación a la posibilidad de establecer un órgano de dirección para Operaciones de Información (OI), la Ley 23.554 de Defensa Nacional, en su Artículo 8, concede la autoridad para adoptar medidas relacionadas con la organización y disposición de recursos disponibles en caso de que se configuren teatros de operaciones de acuerdo con el actual ciclo de planificación estratégica, lo que definirá el contexto operativo que influirá en las operaciones futuras. Además, el Artículo 44 de la misma ley prevé la utilización de instalaciones y recursos para las actividades de comunicación social durante estas operaciones.

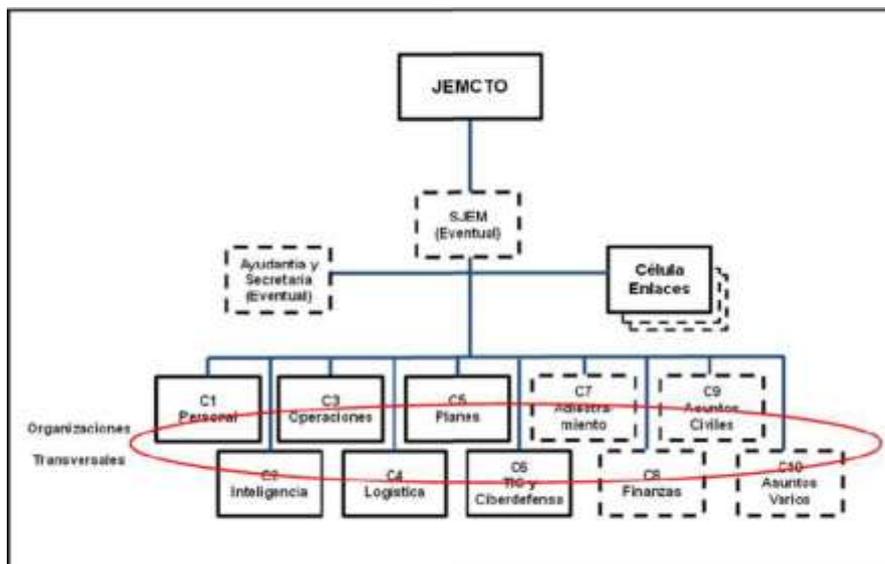
El nuevo proyecto de reglamento PC 20-01 Planeamiento para la AMC (2023), en su Anexo 2 menciona la cooperación transversal, como la acción de sincronizar, coordinar e intercambiar información entre las diferentes jefaturas de un Estado Mayor de nivel Conjunto y esto se logra mediante la creación de una estructura organizacional que combine la gestión administrativa y funcional de las Jefaturas con el cumplimiento de las funciones a través de Organizaciones Transversales orientadas a objetivos específicos y conformadas por personal capacitado proveniente de las distintas Jefaturas, direcciones, comandos conjuntos y otras agencias necesarias.

Las Organizaciones Transversales son elementos “ad-hoc” creados por el JEM para cumplir una tarea específica que requiera un elevado nivel de coordinaciones entre diferentes Jefaturas, Departamentos o Divisiones del EM y demás agencias y medios necesarios.

Estas organizaciones transversales podrán ser: Centros, grupos de planeamiento, células, panel, grupo de trabajo y equipo de planeamiento operacional. Dentro de las Células, se encuentra contemplada la Célula de Operaciones de Información, a la cual le asigna la responsabilidad de coordinar las acciones de COSACO, Velo y Engaño, Ciberdefensa, Guerra Electrónica y Relaciones Públicas (EMCFFAA, 2023, pág. 281).

Figura 2

Organizaciones transversales dentro de un Estado Mayor de nivel conjunto



Nota. Adaptada del reglamento PC 20-01 “Planeamiento para la AMC”, 2023, pág. 275.

Ahora bien entre las capacidades relacionadas con OI que creemos convenientes en base a la doctrina analizada y a la realidad local, mencionadas anteriormente y las contempladas en la doctrina nueva existe similitud, debiendo completarse algunas agencias o acciones que son parte de las OI como las operaciones de seguridad, inteligencia, asuntos civiles y comunicación institucional entre otros, teniendo en cuenta que no será una organización fija sino variable que se podrá integrar con los representantes de las capacidades y agencias que así lo requiera la situación y los objetivos a lograr dentro de la campaña en función de un determinado Teatro de Operaciones.

A nuestro entender esta Célula o Dirección de OI no debería encontrarse bajo la órbita de ninguna área o jefatura específica, debido a su injerencia en las operaciones como nueva herramienta para incidir en el resultado de las operaciones y la transversalidad de las capacidades que la componen, debiendo incorporar representantes y especialistas de todas las áreas del Estado Mayor y de los medios que integran las OI como así de otras agencias estatales y no estatales que puedan requerirse.

De esa manera el responsable del órgano de OI tendría la suficiente libertad de acción que le permita tener una visión integral para lograr la sincronización y coordinación de todas las capacidades y medios a disposición en busca del efecto deseado con este tipo de operaciones, que como queda demostrado a lo largo de esta investigación tienden a ser cada vez mas influyentes a la hora de dirimir un conflicto contribuyendo a logro de la decisión de manera concreta.

Relación de Comando

- Jefe del Estado Mayor Conjunto (JEMCO): El JEMCO tendría autoridad directa sobre el órgano de operaciones de información conjunto
- Comandantes de Componentes de las Fuerzas Armadas: Los comandantes de cada una de las FFAA también tendrían influencia y autoridad en las operaciones de información conjuntas, con su respectiva integración a este elemento a nivel conjunto, para lograr una correcta recurrencia de las OI entre niveles de comando, ya que como se ha mencionado se conciben al más alto nivel, se conducen a nivel operacional y se traducen en objetivos concretos para el nivel táctico que ejecuta este tipo de operaciones.

Relaciones Funcionales:

- Director de Operaciones de Información Conjuntas: Este sería el oficial designado para liderar el órgano de operaciones de información conjunto y coordinar todas las actividades relacionadas con la información. Sería responsable de la planificación, ejecución y evaluación de operaciones de información conjuntas.
- Directores de Operaciones de Información de Componentes: Cada una de las fuerzas armadas componentes podría tener su propio director de operaciones de información, que reportaría al director de Operaciones de Información Conjuntas. Estos directores se encargarían de las operaciones de información específicas de sus respectivas fuerzas.
- Oficiales de Inteligencia: Los oficiales de inteligencia de cada fuerza armada, estarían subordinados funcionalmente al órgano de operaciones de información conjunto.
- Unidades de Operaciones de Información: Estas unidades operativas, tanto a nivel conjunto como de componentes, estarían bajo la dirección y coordinación funcional del órgano de operaciones de información conjunto.
- Otros elementos de Apoyo: Los órganos de apoyo logístico, de los demás campos de la conducción, de comunicaciones y de ciberdefensa, operaciones especiales, comunicación institucional, asesoría jurídica, asuntos civiles, y otros, proporcionarían el respaldo necesario a las operaciones de información conjuntas y trabajarían en coordinación con el órgano de operaciones de información.

A nivel estratégico, las OI se centran en establecer y alcanzar los objetivos nacionales. Se utilizan para disuadir, degradar o derrotar a los adversarios, proteger los intereses nacionales

y promover la paz y la estabilidad, pudiendo influir en los líderes para terminar un conflicto. En el nivel operacional, se desarrolla la conducción de operaciones para alcanzar los objetivos estratégicos militares y transforman en objetivos para el menor nivel. Aquí se establecen los objetivos operacionales que deben lograrse a través de la acción militar conjunta. Este nivel actúa como un enlace entre los esfuerzos de las OI, orienta al nivel táctico y asesora al nivel estratégico. Se planifican las actividades de Operaciones de Información, se definen los objetivos y efectos deseados, y se coordinan con otras capacidades, herramientas y técnicas. En el nivel táctico, las OI se centran en apoyar las operaciones militares a nivel de unidad. Se utilizan para engañar, confundir o debilitar al adversario, proteger las propias fuerzas y promover la moral y la cohesión (EMCFFAA USA, 2014).

Las OI no dependen tanto del tipo de operación, sino más bien en los efectos que se deben lograr vía entorno de información para respaldar operaciones conjuntas o porque no pensar en que podrían llegar a definir una situación.

El responsable de OI juega un rol directivo para desarrollar las OI, las que deben estar integradas adecuadamente al proceso de planificación conjunto y a la intención del comandante con respecto a la operación a ejecutar. Elaborará el Plan de Operaciones de Información del respectivo Plan de Campaña y propone al Comandante todos los aspectos relativos al empleo de las capacidades relacionadas con la Información. Para tal efecto, planifica, coordina, sincroniza y evalúa el esfuerzo integral de las OI, prioriza y compatibiliza determinadas actividades de las mismas para generar el efecto deseado.

El personal especialista de OI, como staff permanente de apoyo al órgano de OI, será personal especialmente capacitado en operaciones de este tipo y con conocimientos generales de cada una de sus capacidades componentes como complemento de los especialistas de cada capacidad, para facilitar la integración efectiva de todas las partes, en apoyo del plan de campaña concebido.

Diseño de la estructura organizacional

La organización de OI conformará un sistema, como conjunto de partes relacionadas entre sí cuya funcionalidad produce emergentes sistémicos, como la sinergia, la cual es aquella propiedad que supone que el todo es distinto a las partes, es decir que la suma de las mismas no es igual al todo, sino que tiene un efecto superador al conjunto (Bertalanffy, 1986).

Este elemento multidisciplinario y multiagencial, sería un sistema complejo de tipo adhocracia, la cual debe disponer de expertos con su respectiva valoración. En este tipo de

estructura los especialistas deben aunar sus esfuerzos, unir fuerzas junto a otros equipos multidisciplinarios, cada uno con una capacidad específica pero que en su integración generen efectos sinérgicos para el logro de los objetivos. (Mintzberg, 1991, pág. 211)

Su principal propiedad sería la fractalidad. Un fractal es un objeto geométrico cuya estructura básica, se repite a diferentes escalas. Las organizaciones fractales son sistemas complejos y flexibles que se autoorganizan y tienen éxito gracias a los objetivos compartidos y a la cohesión de los esfuerzos del grupo por alcanzarlos. Esta propiedad le permitiría replicarse en los distintos niveles desde el nivel estratégico al táctico. Además, teniendo en cuenta el ambiente operacional presente y futuro, podemos decir que el órgano de OI deberá estar en condiciones de desempeñarse eficientemente en un entorno VUCA, sobre todo en el nivel operacional (Alvarez, 2022).

Es fundamental asegurar un funcionamiento fluido, flexible e interrelacionado entre capacidades tan disímiles, donde se comparta la información necesaria, pudiendo aplicarse la forma celular de la teoría del swarming, con pequeñas organizaciones complejas interconectadas entre sí por la tecnología que comparten la información, y operan en forma sincronizada e integrada (Arquilla & Ronfeldt, 2003).

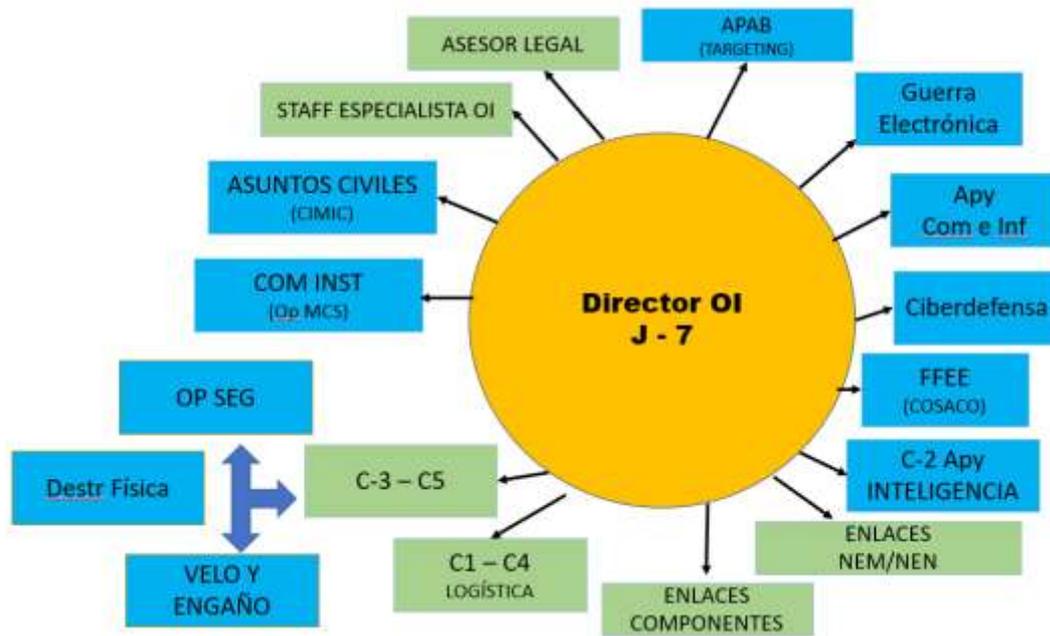
Para ello resulta necesario diseñar una estructura del tipo celular, donde cada parte integrante a su vez deberá ser conjunta internamente, por ejemplo el área de Ciberdefensa del órgano de OI deberá estar integrada por representantes de las tres fuerzas, y así con todas las agencias, procurando lograr un eficiente funcionamiento, teniendo en cuenta las hipótesis de congruencia, donde los parámetros de diseño están en relación con los factores de contingencia, es decir hay una relación entre los fines y los medios, la estructura orgánica se ajusta a la misión que cumple; y de configuración, donde existe un equilibrio organizacional entre las funciones.

El sistema de flujo empleado sería el de constelación de trabajo, ideal para operaciones simultáneas, teniendo bien definida su razón de empleo y la autoridad del Director del órgano de Operaciones de Información de nivel conjunto, quien lidera la misma teniendo una especial capacidad de asesoramiento al decisor respectivo (Mintzberg, 1991).

En cuanto el mecanismo de coordinación y control de la organización se emplearía el de estandarización de resultados, donde la coordinación de las funciones integrantes la efectúa el director de OI quien especificará a cada capacidad el efecto o resultado a lograr, dejando el cómo a criterio de los especialistas de cada capacidad relacionada, pero la integración y sinergia obtenida entre todos ellos permitirá el cumplimiento más eficiente de los objetivos previstos (Mintzberg, 2005).

Figura 3

Estructura de un órgano de Dirección de las OI



Nota. Elaboración propia

Conclusiones

Para dar respuesta a la pregunta de investigación y por ende al objetivo general fijado para este trabajo, el de analizar las características de diseño de una organización de OI de nivel conjunto para planificar, dirigir, evaluar y asesorar en forma integrada las múltiples acciones que conforman las operaciones de información, se trazaron dos objetivos particulares siguiendo una lógica secuencial para su desarrollo, primeramente, sobre el análisis de la doctrina existente en distintos marcos de referencia sobre los conceptos generales y las organizaciones respectivas de OI, y el empleo que este tipo de acciones tuvieron en diversos escenarios históricos, para comprender mejor la naturaleza compleja de estas operaciones buscando definir su concepto de empleo. En segundo término, referido al análisis de los órganos y estructuras de OI en distintos países, para intentar realizar una aproximación a la descripción aproximada de las características generales de un órgano de OI en el nivel operacional.

En el primer Capítulo se realizó un análisis de la doctrina en países destacados a nivel mundial y en la región para comprender las Operaciones de Información (OI). Se concluyó que las OI son actividades realizadas por múltiples agencias, incluyendo diferentes ramas militares, inteligencia, asuntos civiles y comunicación institucional, además de coordinación con entidades no militares. Estas operaciones abarcan varios dominios, como lo físico, lo informacional y lo cognitivo, y deben ejecutarse de manera integrada y coordinada para lograr un efecto sinérgico.

En resumen, este análisis conceptualiza las OI como actividades multiagenciales y transversales que requieren planificación y coordinación en varios niveles, y que tienen un impacto significativo en el logro de objetivos políticos y militares.

Se proporcionaron ejemplos de cómo las OI se han utilizado en conflictos recientes para demostrar su influencia en el resultado de las operaciones militares. Estas operaciones se consideran una herramienta valiosa para resolver conflictos o crisis sin recurrir necesariamente a la fuerza o para reducir su uso. Se enfatiza la necesidad de llevar a cabo las OI de manera integrada y coordinada, ya que involucran acciones en el ámbito de la información que son realizadas por diversos elementos con capacidades específicas. La conclusión principal es que la combinación de diferentes acciones en el ámbito informacional, cuando se ejecutan de manera coherente hacia un objetivo común, puede tener un impacto decisivo en el curso de una campaña. Esto se aplica tanto a nivel nacional como en los niveles subsiguientes de mando, reconociendo que las OI son transversales y deben ser conducidas de manera integral en todos los niveles.

Otro aporte del análisis de la doctrina de OI y los conflictos armados donde estas se emplearon permite concluir que las OI son un componente esencial de la guerra moderna y que resultaría una gran desventaja omitirlas o dejarlas de lado. Las OI pueden utilizarse para lograr una amplia gama de objetivos, desde la disuasión del adversario hasta una clara contribución a obtener la victoria en el campo de batalla.

A modo de resumen del análisis doctrinal resulta más claro comprender los conceptos de OI en el contexto de Estados Unidos y la OTAN debido a la disponibilidad de publicaciones y manuales conjuntos que abordan estas operaciones. En contraste, Rusia y China no han hecho pública la doctrina respectiva no siendo accesible en fuentes abiertas, por ende, los investigadores dependen en gran medida de opiniones académicas, discursos y artículos publicados de sus principales pensadores y referentes, para comprender estos conceptos, ya que los mismos dejan una clara tendencia que debería ser necesariamente recogida en sus manuales y reglamentos.

Finalmente, habiendo hecho el análisis necesario de la doctrina, su viabilidad y su aplicación práctica, en el Capítulo 2, se consideraron las características básicas de las OI para aproximarnos conceptualmente a la descripción de la estructura de la organización que mejor se adapte a la propia realidad política, económica y social, con sus características esenciales, cuáles elementos o acciones deberían conformarla de acuerdo a las propias posibilidades para su funcionamiento sinérgico, arribando a una propuesta lógica de concretar, debiendo ser doctrinariamente más parecida a las adoptadas por países de occidente y en el marco regional, en consonancia con una estrategia nacional defensiva cooperante.

Las OI, en su esencia, implican el uso de la información como un medio para lograr efectos que derivan en la obtención de objetivos estratégicos. Combinando elementos de propaganda, guerra psicológica, operaciones cibernéticas y desinformación, entre otras capacidades, estas operaciones se han convertido en un componente fundamental de la estrategia militar contemporánea, buscando disminuir al máximo posible, los elevados costos humanos y materiales de una contienda armada. Su impacto no se limita al campo de batalla físico, donde se desarrollan las acciones cinéticas, sino que se extiende a la psicología de las poblaciones, la percepción pública y la toma de decisiones en los niveles políticos más altos.

Por su naturaleza sinérgica, las OI no se conciben aplicando las capacidades que las componen en forma aislada. La integración sincronizada y coordinada de las múltiples agencias que las conforman les dan el rasgo distintivo a estas operaciones y permiten todas ellas lograr el efecto deseado en forma sinérgica, generando el componente de ofensiva no cinético en los

ámbitos no físicos, que podría eventualmente disuadir el conflicto armado o disminuirlo sustancialmente en cuanto a la necesidad de un empleo del instrumento militar.

Existen motivos sólidos como hemos desarrollado a lo largo de este trabajo, por los cuales resulta vital considerar la implementación de OI, que surgen y se coordinan desde los niveles superiores de la conducción política y militar del país, debiéndose previamente comprender y asimilar este concepto de empleo novedoso acabadamente, ya que el entorno de la información es cada vez más complejo y disputado por diversos actores para la concreción de sus fines, además que estas operaciones pueden utilizarse para lograr objetivos variados y permiten también complementar las operaciones militares tradicionales siendo un multiplicador de efectos.

En conclusión, las OI son un arma poderosa que puede utilizarse para influir en el comportamiento de los adversarios, los aliados y los socios. Las OI son cada vez más importantes en los conflictos armados, y los militares deben estar preparados para utilizarlas de manera efectiva en un futuro cercano, siendo evidente la necesidad de desarrollar nuevas capacidades relacionadas a la información para hacer frente a las amenazas emergentes.

Por ello, la creación de un órgano de naturaleza conjunta de Operaciones de Información significaría un valioso aporte al campo de la doctrina y organizaciones militares, permitiendo incrementar la efectividad de este tipo de operaciones y garantizar que las mismas se empleen de una manera holística, en estrecha sintonía con los objetivos fijados por la estrategia militar y nacional, ya que cada vez son más notorios los resultados que se pueden lograr con su aplicación y del mismo modo en los últimos años son más los países que las contemplan y utilizan para alcanzar sus objetivos, en forma exclusiva o al menos contribuyente.

Este elemento específico para librar la batalla “informativa” permitiría abordar los desafíos complejos del ambiente operacional moderno y convertir esas características en una ventaja o fortaleza, donde diversas formas de comunicación y tecnología desempeñan un papel importante en las crisis actuales. Esta organización particular buscaría abonar a la necesaria sinergia multidominio, mediante el empleo de distintas capacidades y medios que conforman las OI, aprovechando el impacto de este tipo de operaciones cada vez más presentes en la nueva era de la guerra, para contribuir al logro de los objetivos de nivel estratégico y operacional.

El proceso de crear conciencia y asimilar el concepto de esta nueva forma de hacer la guerra puede ser un camino largo y arduo, debiendo sortear innumerables obstáculos y sesgos cognitivos, para lograr en definitiva entender su concepción como idea superadora que aglutina medios y capacidades que deben ser empleadas en forma sinérgica, en búsqueda del logro de

los efectos tales que contribuyan a alcanzar la concreción de los Estados Finales Deseados con el menor empleo del instrumento militar posible.

Teniendo en cuenta que la presente contribución está orientada particularmente hacia generar los cambios organizacionales a nivel operacional relacionados con las OI, para la adopción de esta nueva forma de hacer la guerra en los tiempos actuales y futuros, caracterizados por una marcada influencia de los avances tecnológicos; el resto de los aspectos a considerar respecto del abordaje integral sobre las OI, deberán ser tema de estudio en sendas investigaciones, para elaborar la doctrina adecuada sobre OI y determinar cuál es el equipamiento más adecuado a fin de lograr el empleo eficiente de estas operaciones en un ambiente operacional cada vez más digitalizado y atravesado por la tecnología.

Consideramos además que el presente trabajo servirá de aporte para hacer una aproximación conceptual más concreta sobre las OI, de manera tal que en futuras líneas investigativas, pueda servir de base a la elaboración de doctrina derivada, para orientar la concepción y empleo de estas operaciones particulares como parte de las acciones multidominio que la estrategia militar ha definido, permitiendo tomar real dimensión de las posibilidades y ventajas de su aplicación en el marco de un conflicto.

Otro aspecto importante a tener en cuenta y que amerita su tratamiento, es la capacitación del personal perteneciente al ámbito de las OI, para que posean una formación específica, creándose una nueva tropa técnica, con sus respectivos ciclos de formación y de perfeccionamiento, creándose la aptitud especial correspondiente, en relación a la trascendencia que este tipo de operaciones tiene, más aún en la era de la información en la que nos movemos y hacia donde vamos.

Resultaría adecuado además tener en cuenta para futuros abordajes, la evolución organizacional de este órgano transversal director de OI, hacia la creación de un Comando Conjunto de Operaciones de Información, como ya sucede en otros países, que absorba y ponga bajo su paraguas a los comandos conjuntos relacionados con las capacidades que las conforman, para darle la preponderancia suficiente a esta modalidad de la guerra. Pero ello sería solo posible habiendo alcanzado la madurez organizacional y doctrinal suficiente, que los condicionantes de la cultura organizacional permitan alcanzar con mayor o menor celeridad.

Bibliografía

- Alvarez, E. M. (2022). *La estructura de un órgano de dirección de OI a nivel CTTO*. Buenos Aires: ESG.
- Argentina, C. G. (1994). *Constitución de la Nación Argentina*. Santa Fe: Boletín Oficial de la República Argentina.
- Arquilla & Ronfeldt. (2003). *Redes y Guerras en Red*. Madrid: Alianza Editorial.
- Baños, P. (2020). *El Dominio Mental: la geopolítica de la mente*. Barcelona: Editorial Ariel.
- Bertalanffy, L. v. (1986). *Teoría General de los Sistemas*. México DF: Fondo de Cultura Económica.
- Bilibio, R. (2017). *La importancia de la aplicación de la Operaciones de Información en un ambiente operacional*. Buenos Aires: ESGCFFAA.
- Bogdanov, T. (1991). Center of Operational and Strategic Studies.
- Brander Palacios, J. M. (2009). *El dominio de la información*. Revismar.
- Brangetto and Veenendaal. (2016). *Influence Cyber Operations*. N. Pissanidis.
- Calderón, T. L. (2022). El futuro entorno operativo y las tecnologías emergentes y disruptivas necesarias para abordarlo. *Bit*.
- Campos, G. (2011). *Transformación del carácter de la Guerra en el siglo XXI. Hacia un modelo integral*. Buenos Aires: Escuela Superior de Guerra.
- Cansdale, M. (2021). *British Army's Approach to Robotics and Autonomous Systems*. Andover: UK MOD.
- Ceballos, A. (s.f.). *Más allá de la Operacion Iraqi freedom*.
- CESEDEN. (2020). *Nota conceptual "Operaciones Multi dominio"*. Madrid: Estado Mayor de la Defensa.
- Clark, B. (2010). *Las OI como elemento disuasivo para el conflicto armado*. Military Review
- Clausewitz, K. v. (2003). *De la guerra*. Buenos Aires: Distal.
- Defense, U. D. (2016). *Strategy for operations in the information environment*.
- DoD, U. (2017). *Joint Publication 3-0 "Joint Operations"*. Washington: Departamento de Defensa.
- Ejército de Tierra. (2006). *Operaciones de Información*. Granada: Mando de Adiestramiento y Doctrina.
- El País. (30 de mayo de 2023). *Los principales creadores de la IA alertan sobre el "peligro de extinción" que supone esta tecnología para la humanidad*. Obtenido de Tecnología: <https://elpais.com/tecnologia/2023-05-30/los-principales-creadores-de-la-ia-alertan->

sobre-el-peligro-de-extincion-que-supone-esta-tecnologia-para-la-humanidad.html#?prm=copy_link

- EMCFFAA. (2019). *Glosario de términos para la AMC*. Buenos Aires.
- EMCFFAA. (2023). *PC 20-01 Planeamiento para la AMC - proyecto*. Buenos Aires: Departamento de Doctrina Conjunta.
- EMCFFAA USA. (2014). *JP 3-13 Information Operations*. Washington: Joint Chiefs of Staff.
- Franz, G. (1996). *Information-The Fifth Element of Combat Power*. Kansas: Escuela de Estudios Militares Avanzados de la Escuela de Comando y Estado Mayor del Ejército de USA.
- Galizia, R. (sep de 2014). *El sistema C3I2 en la era de la información*. Revista de la ESG Nro 588, pág. 187.
- García Servert, T. (23 de mayo de 2022). *Las nuevas Operaciones Multidominio de la OTAN*. Obtenido de <https://www.defensa.com/opinion/nuevas-operaciones-multidominio-otan>
- Gerasimov, V. (2013). *La Ciencia Militar en el Siglo XXI*. Voenno-Promyshlenny Kuryer.
- Gerasimov, V. (9 de marzo de 2016). *Based on the experience of Syria*. Obtenido de Voenno-promyshlenny kuryer: http://vpk-news.ru/sites/default/files/pdf/VPK_09_624.pdf
- CIDH (1969). *Pacto de San José de Costa Rica*. San José: Publicación Oficial de la Organización de los Estados Americanos, No. 36.
- Infodefensa. (23 de julio de 2019). *El Regimiento de Operaciones de Información del Ejército echa a andar*. Madrid: Infodefensa.
- JDCC. (2002). *JWP 3-80 Information Operations*. Swindon: Centro de Doctrina Conjunta.
- JIOC. (2000). *History and Evolution of Information Operations*. Texas.
- Kirschbaum, J. (2021). *Entorno de la Información*. Washington: GAO.
- Kuehl, D. (2014). *Manual de Operaciones de Información Conjunto*. Washington: Universidad de Defensa Nacional de los EEUU.
- Kvachkov, V. (2004). *Russia's Special Purpose Forces*. Voennoy Literatura.
- Libicki, M. (1995). *Qué es la guerra de la información*. Washington D.C: Universidad de Defensa Nacional de los Estados Unidos de América.
- Magnuson, S. (2022). *U.S still playing catch up in Information Operations*. Obtenido de National Defense Magazine: <https://www.nationaldefensemagazine.org/articles/2022/2/11/still-playing-catch-up-in-information-operations>
- Mallick, P. (2021). *Defining China's Intelligentized Warfare and Role of Artificial Intelligence*. New Delhi: Vivekananda International Foundation.

- Milosevich-Juaristi, M. (2017). *La "combinación", instrumento de la guerra de la información de Rusia en Cataluña*. Real Instituto Elcano, 7.
- Ministerio de Defensa. (2014). *DNC 3-7 Operaciones de Información Conjunta*. Santiago: Ministerio de Defensa, EMCO.
- Mintzberg, H. (1991). *Diseño de Organizaciones Eficientes*. Buenos Aires: El Ateneo.
- Mintzberg, H. (2005). *La Estructuración de las Organizaciones*. Barcelona: Editorial Ariel S.A
- Neilson, R. (1997). *Sun Tzu y la guerra de la información*. Washington: US National Defense University.
- OTAN. (2009). *Doctrina Conjunta Aliada para Operaciones de Información*. Bruselas: Departamento de Estandarización.
- OTAN. (2023). *Allied Joint Doctrine for Information Operations*. Brussels: NATO STANDARDIZATION OFFICE (NSO).
- Otero, L. E. (2023). *Nuevas amenazas silenciosas. En la amenaza biológica. Cuadernos de Estrategia*. Madrid: IEEE. Ministerio de Defensa.
- Pallin y Westerlund. (24 de Julio de 2009). *Russia's war in Georgia: lessons and consequences*. Small Wars and Insurgencies, pág. 400/424.
- Pérez, C. (22 de agosto de 2022). *Information Warfare in Russia's War in Ukraine*. Obtenido de FP Analytics: <https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/>
- Ronfeldt, A. &. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. . Santa Mónica, California: Rand corporation.
- Ronfeldt, A. y. (1996). *The advent of netwar*. RAND's National Defense Research Institute.
- Rosenkranz Romero, J. (Feb-Mar de 2020). *¿Es relevante la función conjunta "Información" para la guerra en el mar?*. Revista de Marina, vol 137, nro 979.
- Sánchez, C. J. (2019). *Información y guerra*. Documento de Opinión 44/2019 del Instituto Español de Estudios Estratégicos, 10.
- Sierra, F. (2000). *Guerra informativa y sociedad telegigilada*. Universidad de Sevilla.
- Sun Tzu. (2004). *El Arte de la Guerra*. Buenos Aires: Bureau Editor S.A.
- Takagi, K. (22 de Julio de 2022). *The Future of China's Cognitive Warfare*. Obtenido de Hudson Institute: <https://www.hudson.org/research/17991-the-future-of-china-s-cognitive-warfare-lessons-from-the-war-in-ukraine>
- Tovar, H. (2011). *Guerra de Información ¿el arma es el mensaje?*. Caracas: UCV.

- Troxler, K. Y. (05 de julio de 2022). *Chinese Definitions of Information Warfare*. Obtenido de Swiss Institute for Global Affairs: <https://www.globalaffairs.ch/2022/06/08/chinese-definitions-of-information-warfare/>
- Vergara, T. d. (2021). *El uso de las Operaciones de Información en la dirección e implementación de las operaciones militares*. Buenos Aires: Escuela Superior de Guerra.
- Wald, C. (12 de noviembre de 2021). *America's Lesson From Gaza: Prepare for Desinformation War*. *Global, Land Warfare*, págs. 1-8.
- Woolley, S. (2017). *Computational Propaganda in Russia: The Origins of Digital Misinformation*. *Post-soviet affairs*.
- Zarza, L. (2016). *Estrategia militar y su transformación en la era de la información*. *Visión Conjunta*, 14.