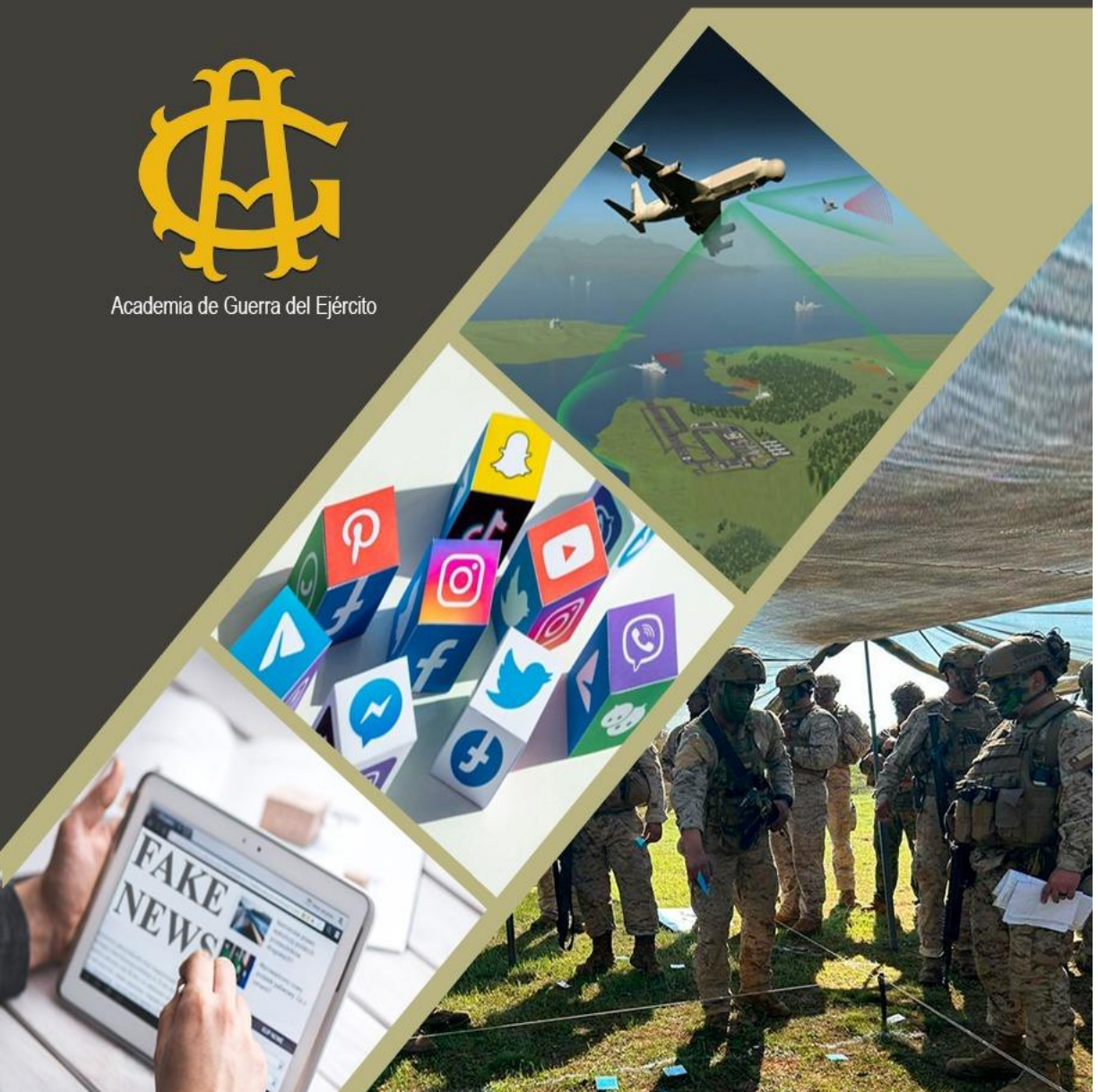
INFOOPS:
Operaciones de Información

Academia de Guerra del Ejército



CEEAG
CENTRO DE ESTUDIOS ESTRATÉGICOS DE LA ACADEMIA DE GUERRA
EJÉRCITO DE CHILE

"LAS OPERACIONES DE INFORMACIÓN (INFOOPS) EN EL CONTEXTO DE LAS OPERACIONES MILITARES"

Centro de Estudios Estratégicos CEEAG

Diciembre 2024

ISBN 978-956-7734-20-7
Inscripción Registro de Propiedad Intelectual Nº 2025-A-2448

Diseño de portada
Francisco Lizama Delgado

Las Operaciones de Información (INFOOPS) en el contexto de las Operaciones Militares

CENTRO DE ESTUDIOS ESTRATÉGICOS DE LA ACADEMIA DE GUERRA
EJÉRCITO DE CHILE

COMITÉ ACADÉMICO

COMITÉ EDITORIAL

Dedicado a los profesores y alumnos del Curso Regular de Estado Mayor de la Academia de Guerra.

Índice

Prólogo

En la actualidad la importancia de la información en el contexto militar, ha pasado a ser un elemento decisivo para el logro de los objetivos de cualquier operación. En ese contexto, el comandante tiene un amplio listado de actividades por las cuales ocuparse durante el empleo de sus medios en la guerra, y como sabemos, estas parten antes de esa fase, con la preparación, planificación, alistamiento, etc. No obstante, además de las actividades esenciales propias las operaciones militares y que se relacionan con su conducción principalmente, hoy con los incrementos en tecnologías, eficiencia de estas y esferas en las que tienen influencia, las actividades de las Operaciones de Información (INFOOPS) constituyen un factor primordial que se suma a las actividades mencionadas en forma general y que por sus eventuales consecuencias debe ser un asunto por el cual también ocuparse.

A tal efecto, y con el fin de contar con antecedentes e información actualizada y veraz del tema, se ha asumido el desafío de efectuar un trabajo de investigación y posterior publicación del Tema de Investigación Central de la Academia de Guerra (TICA) 2024, titulado ***Las Operaciones de Información (INFOOPS) en el contexto de las Operaciones Militares.*** Este trabajo ha sido desarrollado por un grupo de profesores de la Academia de Guerra y otros externos especialistas en el tema y que regularmente apoya al Instituto en el desarrollo de diferentes actividades académicas y, en esta ocasión, con el especial el aporte de una alumna extranjera del CREM, perteneciente al Ejército de Tierra de España, quien además de ser especialista en el área, ha servido en unidades que desarrollan INFOOPS. Este desafío, como es regular, ha sido asumido y coordinado por el Centro de Estudios Estratégicos (CEEAG), con el fin de mantener el debate académico en las líneas de investigación

que son del ámbito de nuestra Academia de Guerra, a través de nuestras publicaciones y aprovechar la oportunidad de presentar una temática contingente que estimule la discusión en un ámbito de crucial importancia, dado el escenario de conflictos que actualmente se observa en el mundo.

En ese contexto, en la guerra Israel – Hamás, Hezbolá (Eje de la Resistencia) es posible distinguir una variada gama de INFOOPS, por parte de ambos lados, como por ejemplo utilizando las redes sociales para transmitir sus narrativas y movilizar el apoyo en su favor. En ese sentido, Hamás ha utilizado plataformas como "X" (ex Twitter) y Facebook para difundir videos y mensajes que muestran su resistencia y logros durante el conflicto, buscando captar la atención de la comunidad internacional y ganar apoyo popular. Por su parte, Israel ha utilizado INFOOPS para resaltar los ataques de Hamás y su derecho a la defensa, intentando obtener apoyo internacional y justificar sus acciones militares. Como este tipo de ejemplos, existen diversos, en diferentes ámbitos y modalidades, con lo cual se puede demostrar cómo las Operaciones de Información son utilizadas estratégicamente en conflictos contemporáneos para influir en la percepción pública y en la narrativa global.

Asimismo, en la guerra Rusia – Ucrania, las Operaciones de Información han desempeñado un papel crucial, siendo utilizadas por ambas partes para influir en la percepción pública y obtener ventajas estratégicas, convirtiéndose en una herramienta esencial en el conflicto. En ese sentido, dos ejemplos de ello: al inicio del conflicto se destaca el uso de *Desinformación y Propaganda***,** llevando a cabo campañas de desinformación para justificar su invasión y desestabilizar a Ucrania. Muestra de ello fue la difusión de narrativas falsas sobre la existencia de un "genocidio" en el Donbás y la necesidad de "desnazificar" Ucrania, sin pruebas que respaldaran estas afirmaciones. Posteriormente, durante el desarrollo de las

acciones, destaca la realización de *Operaciones de Falsa Bandera,* donde Rusia ha creado incidentes simulados para culpar a Ucrania y justificar acciones militares. Un ejemplo es la acusación de que Ucrania planeaba ataques en la región separatista de Transnistria, en Moldavia, sin evidencia que lo sustente.

En el presente, las Operaciones de Información contemplan una amplia gama de áreas interrelacionadas, las que son determinantes en el desarrollo, planificación y ejecución de cualquier operación militar y tienen implicancias serias en la de seguridad. Entre las que desde el punto de vista general han adquirido relevancia y de las cuales podemos tener evidencia pública, se encuentra el uso de técnicas de hacking y ciberataques para interrumpir, desestabilizar o manipular sistemas de información, la utilización de plataformas como "X", Facebook e Instagram para propagar mensajes que influyan en la opinión pública y a la vez permitan contrarrestar la desinformación, también se encuentran las metodologías para crear y difundir información falsa o engañosa para confundir al enemigo y afectar la moral, por otra parte está la pericia en el uso de técnicas psicológicas y de comunicación para influir en la opinión pública y en la toma de decisiones del adversario, y así una variada y cada vez más novedosas formas de realizarlas, lo que refleja la naturaleza multidimensional y dinámica de estas en el contexto actual.

Considerando lo señalado, el comandante producto del análisis del ambiente operacional, se verá obligado a buscar formas de contrarrestar esas acciones, con una variada gama de medidas, entre las que se deducen de dichas acciones, están la de evitar o contrarrestar la propagación de información errónea que pueda socavar las operaciones militares y afectar la moral de las tropas y la población civil, particular preocupación tendrá la protección de las redes de información y comunicaciones para evitar ataques cibernéticos que podrían afectarla debido a la evolución constante

de las tecnologías de la información, por lo que resulta muy importante que los comandantes se mantengan actualizados y adaptativos ante los avances de la tecnología y métodos de uso. Por otra parte, está el uso de la INFOOPS en beneficio propio, con el objeto de que cooperen o formen parte de los elementos que en la concepción y posterior diseño de la maniobra.

Se inicia el presente libro con el capítulo 1, titulado *Las Operaciones de Información en la historia militar*, del Teniente Coronel Mauricio Oyanader Arntz, buscará ejemplificar mediante el análisis de dos operaciones militares relacionadas con las INFOOPS, cómo una adecuada aplicación de acciones destinadas a una audiencia objetivo permite afectar el ciclo de toma de decisiones. De igual manera, identifica bajo este contexto histórico, si las INFOOPS obedecen a un enfoque moderno ligado a ciertos avances tecnológicos o si son de una naturaleza más conceptual y ligada más directamente a las teorías de la comunicación humana.

Seguidamente en el capítulo 2, *¿Ambiente o Dimensión de la Información?*, del Teniente Coronel Martín Muñoz Lepe, en el que profundiza sobre la creciente importancia de la información en el ámbito militar contemporáneo, desplazando su rol de instrumento secundario a convertirse en un factor decisivo para el éxito, junto a ello analiza el concepto del ambiente de la información, para luego interconectarlo con el ambiente operacional y concluye con la relación entre dominios y dimensiones, ahondando en la dimensión de la información y sus respectivos entornos y capas.

A continuación, en el capítulo 3, el Coronel Ricardo Kaiser Onetto desarrolla el tema *Evolución doctrinaria de las operaciones de información y los desafíos para un empleo integral*, en el que analiza las INFOOPS desde una mirada evolutiva doctrinaria, examinando como estas han incrementado la relevancia de la información en la guerra moderna, a través del auge de las tecnologías relacionadas

con la información (el medio), el poder de la narrativa (el mensaje) y la importancia de los medios de comunicación. Finalmente, desarrolla el tema relacionado con la hipótesis de que las INFOOPS están en constante evolución doctrinaria por las tecnologías emergentes, la necesidad de revisar la narrativa y la influencia de las capacidades esenciales con la información para ganar la iniciativa en este ambiente.

Posteriormente está el capítulo 4, con el tema *Las Operaciones de Información en el conflicto actual*, el Teniente Coronel Cristián Retamal Valenzuela explica las razones del éxito y la preponderancia que tiene el desarrollo de operaciones de información en el conflicto actual, tomando como ejemplos aplicados a Rusia y China, países que han sido referentes en el uso de este modo de emplear medios militares y no militares en un esfuerzo sincronizado desde el más alto nivel de la conducción.

Luego, en el capítulo 5, titulado *La dimensión humana en el contexto de las operaciones de información: Un enfoque psicológico basado en la comunicación, la influencia y la persuasión*, el Psicólogo (Mg.) Francisco Javier Urra Riveros, explora cómo integrar principios psicológicos en las INFOOPS para mejorar su efectividad, considerando aspectos como la defensa cognitiva, la manipulación de la información, y el rol crucial de la influencia, basada en la persuasión y cognición social. Además, se abordan los dilemas éticos asociados al uso de estas técnicas y se ofrecen recomendaciones para su aplicación ética y efectiva en el contexto militar.

A continuación, en el capítulo 6, la Comandante (Ejército de Tierra de España) Consuelo Delage Gª de Angulo, desarrolla el tema *Ejecución de INFOOPS en el Nivel Táctico: El Caso del Ejército de Tierra español.* En este capítulo ofrece una visión sobre la aproximación a operaciones de Información (INFOOPS) en el Ejército de Tierra de España (ET), con un enfoque particular en el

Nivel Táctico, precisando que la información contenida en este capítulo se extrae tanto de los avances en doctrina y publicaciones relacionadas en el entorno de las Fuerzas Armadas (FAs) españolas y de la OTAN, así como de la experiencia de la oficial autora de este capítulo en diferentes puestos relacionados con Comunicación Estratégica (STRATCOM) y Operaciones de Información (INFOOPS).

Finalmente, el capítulo 7, con el análisis del tema *Contrarrestando las Operaciones de Información de la Amenaza,* del Teniente Coronel Nicolás Kaiser Onetto, describe cómo las capacidades relacionadas a las funciones operacionales contribuyen a contrarrestar los efectos de las Operaciones de Información (INFOOPS) de una amenaza. Para ello, se estableció tres premisas claves.

Al concluir este prólogo, es de toda justicia agradecer el trabajo realizado por los investigadores y el CEEAG, por poner a disposición de la comunidad académica en general y de alumnos y profesores de la ACAGUE en particular, una publicación novedosa que aportará a la construcción y entendimiento, aprovechando la oportunidad de identificar estos contenidos en los actuales conflictos en desarrollo y su aplicación práctica en el desarrollo de los módulos y ejercicios del CREM, particularmente en el análisis del ambiente operacional.

Coronel Manuel Provis Baker
Director de la Academia de Guerra del Ejército de Chile

Las Operaciones de Información (INFOOPS) en el contexto de las Operaciones Militares

CAPÍTULO 1

Las Operaciones de Información en la historia militar

Teniente Coronel Mauricio Oyanader Arntz[1]

> *Toda guerra se basa en el engaño. Por lo tanto, cuando podemos atacar, debemos parecer incapaces; cuando utilizamos nuestras fuerzas, debemos parecer inactivos; cuando estemos cerca, debemos hacer creer al enemigo que estamos lejos; cuando estamos lejos, debemos hacerle creer que estamos cerca.*
>
> Sun Tzu

Introducción

¿Es la historia militar una disciplina que sólo se enfoca en narrar acerca de gestas, héroes o estrategias, entre otros elementos? Según lo expresa Roberto Arancibia, corresponde al estudio del hombre militar en el tiempo, donde la guerra, viene a ser la extensión del objeto de estudio. Al cruzar esto con la mirada trinitaria de la guerra de Clausewitz, la historia militar podría estudiar diferentes episodios bélicos desde la mirada de las decisiones razonadas de los "gobiernos", las acciones de los "ejércitos" en el campo de batalla o del rol del "pueblo" en la voluntad de lucha de un Estado, entre otras perspectivas. Sin embargo, para este caso, cobra interés revisar de qué forma los componentes de la

[1] Teniente Coronel del Ejército de Chile. Oficial de Estado Mayor del Ejército de Chile. Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica, Academia de Guerra del Ejército de Chile. Actualmente, es profesor de la ACAGUE. ✉ mauricio.oyanader@acague.cl.

trinidad de Clausewitz pueden comportarse cuando son audiencias objetivo de las operaciones de información (INFOOPS).

Así, mediante el análisis histórico de dos operaciones militares desde la perspectiva de las INFOOPS, este capítulo busca ejemplificar de qué forma un adecuado empleo de acciones sobre una audiencia-objetivo determinada, pueden afectar los ciclos de toma de decisiones y los resultados en la guerra. Adicionalmente, se invita al lector a preguntarse si las INFOOPS corresponden a un enfoque moderno ligado a ciertos avances tecnológicos o si en realidad han acompañado a los conflictos desde que nacen con el hombre.

Ver para creer: antes, ahora y siempre

Las INFOOPS se definen como el conjunto de acciones coordinadas que se realizan para influir en la toma de decisiones de un adversario en apoyo de la consecución de los objetivos propios, influyendo en su capacidad para explotar y proteger la información, en los sistemas de mando y control que la soportan y en los sistemas de telecomunicaciones e información que la procesan, mientras se resguardan los propios. Las INFOOPS constituyen actividades operativas que se realizan en el teatro de operaciones, sin depender de los detalles de las operaciones en curso, pero que tienen una influencia decisiva en ellas por lo que deben ser coordinadas y controladas por el comandante del teatro (Estado Mayor Conjunto, 2022, p. 73).

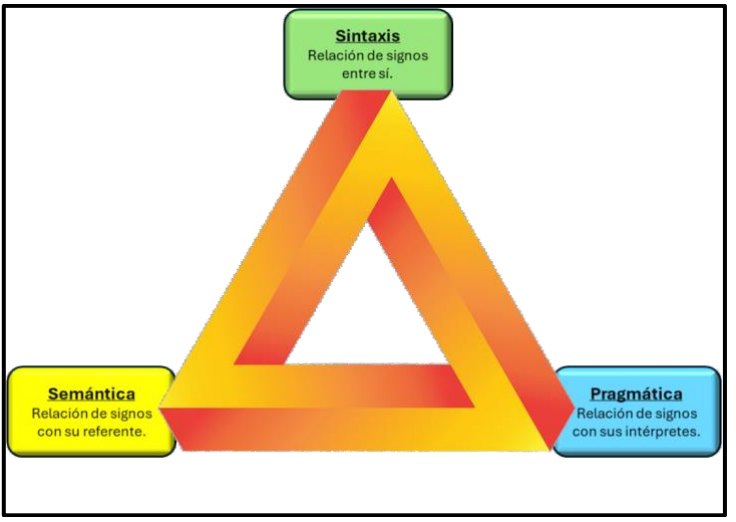
Si nos enfocamos en las audiencias objetivo de las INFOOPS, entre

otras, se conforman por la población civil y los tomadores de decisiones – de distintos niveles de la conducción militar – presentes en múltiples escenarios de guerra. Respecto de ellos, por ejemplo, en el nivel táctico se podría buscar influir sobre un comandante respecto de decisiones acerca de la posición y/o maniobras de sus unidades en terreno, mientras que en el nivel estratégico la influencia podría buscar la justificación y validez de una determinada campaña u operación. Independiente de quien sea la audiencia a la que se quiera afectar, queda de manifiesto que, conforme a la naturaleza humana, ella confiará y/o creerá en aquellos elementos que pueda identificar, percibir o decodificar; y, por lo tanto, en aquello que se le presente o le sea presentado.

Desde lo antes expuesto cobra relevancia la teoría de la semiótica del filósofo estadounidense Charles Williams Morris, para comprender en parte la naturaleza de la comunicación humana aplicada a las INFOOPS. La semiótica define los signos como cualquier cosa que pueda ser interpretada y que genere la representación de algo para una persona. Enfoca su estudio no solo a los signos o símbolos, sino también a sus propiedades, usos, y los efectos que tienen sobre los individuos. Desde esta perspectiva, un signo incluye palabras, imágenes, sonidos, gestos, y prácticamente cualquier fenómeno que pueda transmitir información de un ente a otro. Morris estaba especialmente interesado en cómo los signos afectan el comportamiento humano y cómo su comprensión puede ser utilizada para manipular la comunicación y la interacción social; lo que queda reflejado en su triángulo semiótico, compuesto por la sintaxis, la semántica y la pragmática.

Figura 1

Triángulo semiótico de Morris



Nota: Elaboración propia basada en "Foundation of Theory of Signs" (1938)

En el ámbito de las INFOOPS, la "sintaxis" se relacionaría con la estructura y forma de los mensajes dirigidos a una audiencia, dónde la organización de los signos contenidos en el mensaje puede afectar significativamente su claridad y eficacia. Por ejemplo, en la elaboración de narrativas consideradas dentro de operaciones de apoyo a la información militar (MISO), la estructura sintáctica debe diseñarse de tal manera que maximice la comprensión mientras se minimiza la posibilidad de interpretaciones erróneas.

Respecto de la "semántica" en INFOOPS se centraría en la acepción de los signos y cómo éstos son interpretados por las audiencias, especialmente por los tomadores de decisiones. Es crucial que los mensajes transmitidos reflejen con precisión la intención detrás de ellos,

especialmente en operaciones para influir en la percepción pública o en los ciclos de tomas de decisiones. La claridad y la precisión semántica son esenciales para evitar malentendidos que podrían comprometer la narrativa que se desea implantar en la audiencia objetivo.

La "pragmática" se relaciona con los efectos que los signos tienen sobre las personas que los reciben. En INFOOPS, esto significaría diseñar mensajes que no solo informen o engañen, sino que también motiven o influyan en el comportamiento del receptor. La pragmática puede ser crucial en acciones MISO, donde el objetivo es influir en percepciones y apreciaciones del ambiente.

Se podría pensar que la semiótica de Morris corresponde a una teoría de corte "moderno", sin embargo, ésta fue planteada en el año 1938, teniendo que transcurrir más de 50 años para que se incorporara conceptualmente en el cuerpo doctrinario de lo que hoy denominamos INFOOPS.

Con esto, a mediados de la década de los 90', el Departamento de Defensa de los EE.UU. (DoD) comenzó a desarrollar la doctrina de la guerra de mando y control (C2W), centrada en afectar el ciclo de toma de decisiones del adversario, su aptitud para conducir las operaciones y a su vez, proteger estos mismos aspectos propios. Se basaba en una capacidad robusta de plataformas de fuegos letales y no letales, que permitieran afectar el mando y control adversario. Un ejemplo de esto se evidencia en la destrucción física de la estructura de comunicaciones y mando y control iraquí, ejecutada durante la operación "Instant Thunder"

en la Guerra Golfo Pérsico del año 1991 (ver figura 2), la cual generó una parálisis estratégica en la toma de decisiones iraquí. Es en este mismo conflicto en las operaciones de seguridad (OPSEC), operaciones de decepción (MILDEC), operaciones psicológicas (PSYOPS), la guerra electrónica (EW) y la destrucción física son integradas a una campaña para potenciar los efectos buscados en el teatro de operaciones.

Figura 2

Primer día de operaciones aéreas en la Guerra del Golfo

Nota: R. Atkinson. *Crusade: The Untold Story of the Persian Gulf War*

Posteriormente, hacia 1996 el DoD difunde la Directiva Secreta S-3600.1, donde se desarrolló el concepto inicial de INFOOPS y que entregó tareas específicas a las ramas de las Fuerzas Armadas norteamericanas para desarrollar sus propias doctrinas, procesos de entrenamiento y equipamiento para ejecutar las INFOOPS.

Al revisar escuetamente lo planteado en los párrafos precedentes, se puede identificar que una teoría de comunicaciones (Morris) – entre tantas otras – tiene correlación con los conceptos de C2W e INFOOPS, desarrollados en para conflictos armados contemporáneos. No obstante, las INFOOPS, como concepto atemporal y genérico, buscan influenciar a un individuo o a un grupo de ellos, quienes por su naturaleza misma son susceptibles a diversas acciones que se generen en su ambiente de la información, y empujarán a creer en lo que "ven", o en lo que crean que están viendo.

Operación Bodyguard: Guardaespaldas de la verdad ¿o de la mentira?

> *En tiempo de guerra, la verdad es tan preciosa que siempre deberá ser resguardada por un guardaespaldas de mentiras.*
>
> *Winston Churchill*

En 1944 la Segunda Guerra Mundial se encontraba en una etapa crítica, con los Aliados preparándose para una invasión masiva hacia Europa Occidental, con el fin de liberar los territorios ocupados por el Eje, mediante las operaciones Neptuno y Overlord, las cuales por su

complejidad y relevancia se basaban en poder evitar las “superficies” y aprovechar los “vacíos” para la inserción de las fuerzas expedicionarias, buscando aminorar el derramamiento de sangre propia.

Los Aliados estaban plenamente conscientes de que, si los alemanes descubrían sus intenciones, el desembarco sería extremadamente difícil, sino imposible, principalmente por la preparación defensiva fortificada alemana del “Muro del Atlántico”. Por tanto, la operación Bodyguard se concibió para crear confusión y desinformación sobre las verdaderas intenciones aliadas, y se presenta como uno de los ejemplos más claros de la aplicación de INFOOPS diseñadas para afectar a los tomadores de decisiones alemanes y asegurar el éxito de Neptuno y Overlord, relacionadas con el desembarco de fuerzas aliadas en el frente de Europa occidental. Bajo una mirada doctrinaria actual, en esta extensa operación estratégica, se emplearon diversas capacidades relativas a la información (IRCs), las cuales lograron influir en la percepción y en las decisiones alemanas, significando una piedra angular para los Aliados, ya que les permitió potenciar su propia planificación y posteriormente alcanzar el éxito en esta empresa bélica.

La Operación Bodyguard, junto con sus 35 operaciones subsidiarias, agrupó a lo menos 5 objetivos de nivel estratégico, los cuales buscaban prevenir la concentración de fuerzas del Eje que pudieran concurrir a reforzar la estructura defensiva, específicamente en la zona general de Normandía, lugar donde se efectuaría el desembarco del 6 de junio de 1944.

Figura 3

Ubicación de las operaciones subsidiarias de Bodyguard

Nota: Weapon and Warfare (2017)

Los objetivos antes señalados se relacionaban con las siguientes operaciones subsidiarias principales:

Operación Pointblank: contribuyó a las INFOOPS buscando destruir la capacidad de bombardeo pesado alemán, a fin de proteger a las fuerzas aliadas que se concentrarían en Inglaterra y que serían empleadas en Neptuno y Overlord. Además de las fuerzas, se buscaba

proteger la capacidad de sostenimiento que se reunirían para poder apoyar le desembarco y las primeras fases de las operaciones. Lo anterior se ejecutó a través de un cambio de actitud en las operaciones aéreas, las cuales buscarían afectar infraestructura crítica para la capacidad aérea alemana y de esta forma disminuir los bombardeas sobre Inglaterra.

Operación Fortitude Norte: fue diseñada para generar la percepción de que se planificaba una invasión aliada a través de Noruega, con el propósito de evitar la concurrencia de fuerzas alemanas hacia Normandía. Consideró simular la activación del cuartel general del 4to Ejército Británico en la zona de Edimburgo y acciones de operaciones especiales, a modo de "configuración" previa a la invasión. Además de simular unidades terrestres, se aumentó el volumen de comunicaciones cifradas y en claro, para potenciar la narrativa aliada, mediante evidencias que recogía la inteligencia alemana.

Operación Fortitude Sur: su propósito era hacer creer que la invasión se ejecutaría a través del paso de Calais, buscando una mayor concentración de fuerzas alemanas hacia dicho sector, por sobre las playas de Normandía. Adicionalmente, buscaba implantar la idea de que la invasión por Normandía constituiría una operación de decepción y que el esfuerzo principal aliado iría por Calais. Dentro de este esfuerzo estaba considerada la operación Quicksilver I, con la creación del 1er Grupo del Ejército de los Estados Unidos (FUSAG) – o Ejército ficticio – concentrado al sur de Inglaterra y al mando del general George Patton, el cual simulaba la concentración de fuerzas que reforzaba la narrativa de Quicksilver I.

Figura 4

Señuelos de lanchas de desembarco en el sur de Inglaterra

Nota: War History (2024)

Operación Zeppelin: como una forma de continuar saturando de información a los cuarteles generales del Eje, se inicia la ejecución de esta operación a principios de 1944, la cual simularía una invasión anfibia hacia los Balcanes, empleando al 12vo Ejército Británico. Se simuló un cuartel general y la concentración de una fuerza expedicionaria ubicada en El Cairo, lo cual buscaba específicamente mantener la presencia de fuerzas alemanas al Este del Mediterráneo, evitando su concurrencia hacia Normandía.

Operación Bagration (Frente Oriental): mediante la acción diplomática se buscó que Rusia aplazará las operaciones ofensivas hasta

no antes del mes de Julio de 1944. Es de esta forma que se planifica la Operación Bagration por parte de Rusia, la cual consideraba una ofensiva en todo el frente oriental. Los indicativos de una inminente invasión desde el Este, aumentó la incertidumbre estratégica para los tomadores de decisión alemanes.

La historia misma refleja que los efectos buscados por las distintas operaciones subsidiarias de Bodyguard tuvieron resultados favorables en apoyo a la maniobra estratégica principal, la cual desembarcar a una fuerza expedicionaria en las costas de Normandía y reconquistar Europa occidental. La simultaneidad de efectos y estímulos generados sobre el alto mando alemán habría impedido una adecuada estimación de dónde sería el lugar específico del desembarco de las tropas aliadas. Cabe mencionar que, para poder lograr los efectos buscados, se empleó una combinación de lo que, en lenguaje moderno se denomina como capacidades relativas a información (IRCs), como una forma de potenciar las iniciativas destinadas a tratar de influir en la toma de decisiones del enemigo.

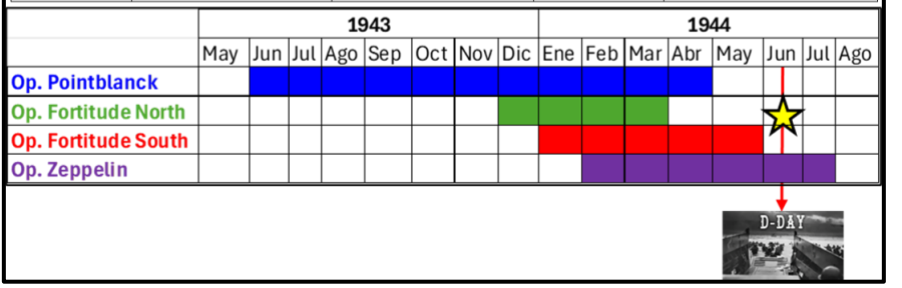
La Figura 5 que se presenta a continuación expone algunos de los efectos alcanzados y la temporalidad utilizada para las principales de las 35 operaciones subsidiarias que abarcó Bodyguard. Cabe resaltar la relación existente entre las fuerzas dispuestas para las operaciones de información y las fuerzas sobre las cuales se generó el efecto. Esto permite comprender que, pese a no haber existido acciones de enfrentamiento directo de alta intensidad, en la mayoría de las ocasiones, fuerzas de menor magnitud amplificadas con IRCs lograron afectar el

ciclo de toma de decisiones adversario, generando la acción o inacción buscada sobre fuerzas de mucho mayor magnitud.

Figura 5

Temporalidad de las principales operaciones subsidiaras y sus efectos.

Operación	Objetivo	Fuerzas asignadas	IRCs	Efecto logrado
Pointblank	Degradar capacidad de bombardeo pesado alemán y proteger concentración de medios.	Comando de Bombarderos de la Royal Air Force 8va Fuerza Aérea EE.UU	Destrucción física OPSEC	Alemania desvió desviar medios y principalmente pilotos, para contrarrestar los bombardeos sobre infraestructura crítica.
Fortitude Norte	Amarrar fuerzas en el frente noruego y evitar la concurrencia a Normandía.	Cuartel General del	MILDEC MISO EW Destrucción física	13 divisiones alemanas se mantuvieron en Noruega hasta el término de la primavera de 1944.
Fortitude Sur (Quicksilver)	Amarrar fuerzas en Pas-de-Calais y hacer creer que Normandía sería una operación de engaño.	23er Cuartel General de Ejército de EE.UU	MILDEC MISO EW	Pese a que Rommel solicita la asignación de medios de la reserva (03 divisiones panzer y 01 brigada de artillería de cohetes), su petición es desestimada por que su escalón superior consideraba el esfuerzo principal se mantendría en Calais.
Zeppelin	Amarrar fuerzas en el frente Este y evitar concurrencia al sector de desembarco.	Cuartel General Fuerza "A" del Ejército Británico	MILDEC MISO EW	Cerca de 300.000 tropas alemanas mantuvieron la ocupación de la zona para contener un posible desembarco aliado.
Frente Oriental (Bagration)	Complementar efecto de Operación Zeppelin.	Empleo de coordinaciones nivel político	MISO	Las fuerzas se mantienen en contacto con la ofensiva rusa la cual estaban planificada para mantener a Alemania con 02 (dos) contraofensivas simultáneas.



Nota: Elaboración propia

Luego de analizar diferentes aspectos de Bodyguard – planificada y conducida principalmente desde Gran Bretaña – es de gran utilidad observarla bajo los actuales principios de operaciones de información incluidos en el AJP 10.1 "Doctrina Aliada Conjunta para Operaciones de Información" ed. 2013, como a continuación se presenta.

Comprensión situacional: el entendimiento del ambiente operacional junto a sus audiencias, sumado a la comprensión de los objetivos e intención del escalón superior, habría permitido el adecuado diseño de todas las operaciones incluidas en Bodyguard. Existieron problemas militares específicos tales como proteger la concentración de fuerzas en Gran Bretaña, evitar chocar con las fuerzas principales del "Muro del Atlántico" o la posible concurrencia de fuerzas acorazadas hacia los sitios de desembarco. Esto y otros aspectos no podían ser afectados directamente por las fuerzas aliadas, por lo que se buscó afectarlas de manera indirecta a través de operaciones de información.

Guiado por una narrativa: existió una coherencia en la entrega del mensaje, diseñado desde el nivel político hasta ser ejecutado en acciones por el nivel táctico, generado una narrativa creíble. La gran cantidad de operaciones subsidiarias estaban "iluminadas" por una sola narrativa tendiente a provocar efectos que generaran las mejores condiciones posibles para un desembarco con las playas de Normandía.

Enfocado en efectos: a la par con los objetivos planteados, están los efectos buscados sobre el adversario. Es decir, el objetivo general de Bodyguard era el de "limpiar" las playas de Normandía de amenazas alemanas, lo cual se debería generar con el movimiento de diferentes fuerzas del Eje lejos de la zona o con, al menos, la neutralización de ellas. Para lograrlo, se diseñaron diferentes operaciones subsidiarias que sumaron efectos menores que se alienaban y coincidían con el esfuerzo superior.

Integración: los resultados y efectos diseñados deben estar integrados a un objetivo común, evitando generar esfuerzos cuyos resultados, y consumo de recursos, no tributen al objetivo principal. En esta empresa de INFOOPS confluyeron 35 objetivos secundarios que integraron a diferentes tipos de IRCs para generar los efectos deseados. Así, por ejemplo, Fortiude Sur integró el uso de fuerzas que simulaban preparativos para desembarcar en el paso de Calais (MILDEC) con la interceptación y decodificación de mensajes (EW) y el empleo de dobles agentes para entregar información falsa (MISO), logrando el efecto de dejar amarradas a las reservas acorazadas alemanas en ese sector.

Agilidad: la evaluación de la campaña o de las operaciones cobra un alto valor en las operaciones de información, debido a que permite ir ajustando las acciones que busquen generar los efectos deseado. En este aspecto destaca el aporte que entrega la función inteligencia para poder monitorear los efectos que se logren con las INFOOPS y evaluar la eficiencia de éstas. Este tipo de operaciones demanda de preparación y flexibilidad de los estados mayores para evaluar, ajustar, coordinar y dirigir a las IRCs empleadas para lograr afectar al adversario o, incluso, evitar que la propia fuerza se vea afectada por acciones mal planificadas.

Planificación centralizada y ejecución descentralizada: la desvinculación geográfica, necesidad del saber y mantención del secreto para este tipo de operaciones, exigen una alta capacidad por parte de los distintos comandantes y sus estados mayores para lograr alinear la intención del escalón superior. En este caso, la planificación de Bodyguard – como un todo – deriva de la intención principal de los

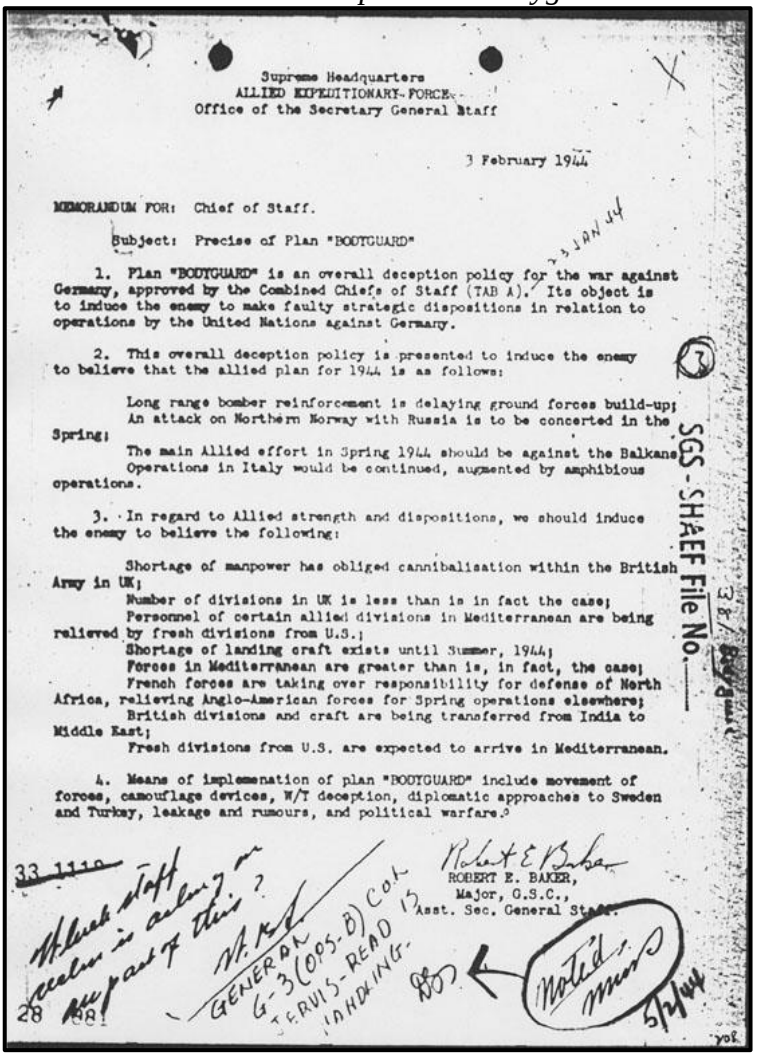
líderes políticos, quedando el detalle centralizado de ella en manos del nivel estratégico de la conducción aliada, sin embargo, en la ejecución se aprecia la descentralización en múltiples unidades de nivel inferior, como lo ejemplifica la tabla de la figura 5, precedente.

Evaluación constante: una parte fundamental de las operaciones de información es la evaluación a corto y largo plazo de los efectos buscados. Se debe poner atención en los indicadores que demuestren el comportamiento deseado de la audiencia objetivo y los resultados en sus decisiones. Para Bodyguard, la extensión geográfica que cubría – desde la Costa Atlántica de Europa y hasta la frontera con Rusia – significó un desafío para monitorear y finalmente evaluar si las fuerzas alemanas se comportaban de la forma deseada previo al día "D".

Últimamente, la historia pareciera indicarnos que este guardaespaldas logró proteger la verdadera intención y la planificación aliada, mientras la reemplazaba con una "realidad ficticia" que los tomadores de decisiones alemanes aceptaron y que repercutió en el posicionamiento y la maniobra proyectada de sus fuerzas. El éxito de la operación conjunto combinadas más grande de la historia – como lo fue la Operación Overlord – dependió en gran medida de este tipo de operaciones complementarias, como lo fue Bodyguard, que permitió, en definitiva, equilibrar los factores operacionales de fuerza, tiempo y espacio en favor de los Aliados.

Figura 6

Memorándum con detalles de la Operación Bodyguard



Supreme Headquarters
ALLIED EXPEDITIONARY FORCE
Office of the Secretary General Staff

3 February 1944

MEMORANDUM FOR: Chief of Staff.

Subject: Precise of Plan "BODYGUARD"

1. Plan "BODYGUARD" is an overall deception policy for the war against Germany, approved by the Combined Chiefs of Staff (TAB A). Its object is to induce the enemy to make faulty strategic dispositions in relation to operations by the United Nations against Germany.

2. This overall deception policy is presented to induce the enemy to believe that the allied plan for 1944 is as follows:

Long range bomber reinforcement is delaying ground forces build-up;
An attack on Northern Norway with Russia is to be concerted in the Spring;
The main Allied effort in Spring 1944 should be against the Balkans
Operations in Italy would be continued, augmented by amphibious operations.

3. In regard to Allied strength and dispositions, we should induce the enemy to believe the following:

Shortage of manpower has obliged cannibalisation within the British Army in UK;
Number of divisions in UK is less than is in fact the case;
Personnel of certain allied divisions in Mediterranean are being relieved by fresh divisions from U.S.;
Shortage of landing craft exists until Summer, 1944;
Forces in Mediterranean are greater than is, in fact, the case;
French forces are taking over responsibility for defense of North Africa, relieving Anglo-American forces for Spring operations elsewhere;
British divisions and craft are being transferred from India to Middle East;
Fresh divisions from U.S. are expected to arrive in Mediterranean.

4. Means of implemenation of plan "BODYGUARD" include movement of forces, camouflage devices, W/T deception, diplomatic approaches to Sweden and Turkey, leakage and rumours, and political warfare.

SGS - SHAEF File No.

ROBERT E. BAKER,
Major, G.S.C.,
Asst. Sec. General Staff.

Nota: *Hesketh. 2000, p. 12*

Los efectos que generaron las operaciones de información ejecutadas en el contexto de Bodyguard lograron como pocas veces en las operaciones militares, alcanzar los objetivos levantados durante la planificación mediante: *movimientos de fuerzas, medidas de camuflaje y*

decepción, aproximaciones diplomáticas con Suecia y Turquía, filtraciones y rumores, además de "guerra política".

Operación Badr y Granito: la información demasiado creíble es a su vez, poco creíble

> *Deja que tus planes sean oscuros e impenetrables como la noche y cuando inicies los movimientos, golpea como el rayo.*
>
> *Sun Tzu*

La guerra del Yom Kipur – o guerra de octubre – fue un hecho bélico enmarcado dentro del conflicto árabe - israelí donde los beligerantes estaban representados por la alianza egipcio - siria en contra Israel y desarrolló sus operaciones principales entre el 6 y el 25 de octubre de 1973.

Es en este contexto que Egipto planifica y ejecuta la denominada Operación Badr, la cual consistía en el cruce sorpresivo del Canal de Suez para invadir a Israel. Ésta, además de lograr un gran éxito militar inicial basado en la sorpresa y simultaneidad de sus efectos, se ha destacado por ser un caso ejemplar en el empleo de INFOOPS para desorientar a los tomadores de decisiones israelíes, mediante diferentes acciones de engaño (MILDEC) y la manipulación de la información. Con esto, Egipto logró tomar por desprevenido al sistema defensivo de israelí, lo que se considera como uno de los factores clave que permitieron potenciar la maniobra egipcia en el cruce del canal. Las operaciones de INFOOPS Granito I, II y III – diseñadas como parte de un complejo plan de decepción o MILDEC – jugaron un papel crucial para configurar el

éxito de las fases iniciales de Badr.

Las previsiones en la planificación de Badr contemplaban un ataque coordinado sobre Israel desde Egipto y Siria, con el fin de recuperar los terrenos perdidos durante la Guerra de los Seis Días de 1967, instancia en la que Israel anexa a sus territorios los Altos del Golán, Cisjordania, la Franja de Gaza y la totalidad de la península del Sinaí.

Para configurar Badr – y en directa relación con el tema de interés de este capítulo – Egipto se enfocó en tres pilares claves relacionados directamente con las INFOOPS: engaño estratégico o decepción (MILDEC), protección de la información y de las operaciones (OPSEC) y operaciones psicológicas (MISO). Esto fue faseado a través de las operaciones subsidiarias conocidas como *Granito I, II y III*, las cuales tenían como objetivo principal desorientar a los tomadores de decisiones israelíes y ocultar las verdaderas intenciones de la ofensiva egipcia.

Las operaciones *Granito* se ejecutaron en un contexto de tensiones acumuladas entre Egipto e Israel. Tras su derrota en la Guerra de los Seis Días (1967) Egipto adoptó una postura militar defensiva, complementada por discursos diplomáticos que sentaron la percepción de que no se estaba en condiciones de lanzar una guerra a gran escala, ni existía la intención de recuperar los territorios perdidos. El presidente Egipcio Anwar el-Sadat comprendió la importancia de elevar la preparación militar, sin cambiar esta percepción ni alertar al enemigo, siendo *Granito* el medio clave para lograr este objetivo.

Figura 7

Terrenos controlados por Israel luego de la Guerra de los Seis Días

Nota: Naciones Unidas, citada por Swissinfo

Las operaciones *Granito I, II y III* fueron las fases progresivas de un plan de engaño destinado a ocultar la preparación para la ofensiva egipcia en el Sinaí y a generar un entorno de falsa normalidad en el Canal de Suez. Estas fases, ejecutadas de manera escalonada, involucraron movimientos de tropas, simulaciones de maniobras y la manipulación de la información en diversos frentes:

Granito I fue la primera fase del plan de engaño, ejecutada varios

meses antes del inicio de la ofensiva. Durante esta etapa, Egipto comenzó a llevar a cabo maniobras militares a gran escala a lo largo del Canal de Suez. Estas maniobras se hicieron rutinarias y fueron diseñadas para familiarizar al enemigo con grandes movimientos de tropas sin generar alarma. El objetivo de *Granito I* era hacer que el despliegue masivo de tropas egipcias en las cercanías del canal pareciera una práctica habitual.

A través de la repetición de estas maniobras, Israel comenzó a asumir que los movimientos militares egipcios no representaban una amenaza inminente, sino que eran ejercicios defensivos o tácticas de entrenamiento. Esta desensibilización fue un éxito temprano en la campaña de información, ya que Egipto logró que las fuerzas israelíes redujeran sus niveles de alerta (Shazly, 1980). Así, la primera fase de *Granito* sembró la base para las siguientes etapas del engaño.

Granito II fue una ampliación de los efectos logrados en la primera fase con la "desensibilización" generada en el sistema de inteligencia israelí sobre la presencia de fuerzas egipcias en el Canal de Suez. Durante los meses previos a la ofensiva, Egipto intensificó sus maniobras militares, pero incluyó elementos adicionales para potenciar la MILDEC que buscaba generar. A diferencia de *Granito I*, esta fase se centró en crear señales contradictorias para las fuerzas israelíes. Se llevaron a cabo simulacros de cruce del Canal de Suez, que imitaban de manera casi exacta las tácticas que se emplearían durante la ofensiva real. No obstante, estos ejercicios se presentaron como simulaciones defensivas, lo que llevó a los israelíes a interpretarlos como ejercicios rutinarios.

Un elemento clave en *Granito II* fue la creación de patrones de movilización que parecían inofensivos o inconexos. A través de la inteligencia militar y con el apoyo de acciones MISO, Egipto manipuló la percepción israelí para que creyera que las fuerzas egipcias no estaban preparadas para un cruce real del canal. Esto incluyó la deliberada dispersión de desinformación a través de agentes de inteligencia y medios de comunicación, y la presentación de fallos logísticos o técnicos como razones para no temer un ataque (Herzog, 1975).

Durante *Granito II*, las fuerzas egipcias también comenzaron a recibir equipamiento adicional de la Unión Soviética. Sin embargo, estos envíos se disimularon dentro de la narrativa de ejercicios militares regulares, y Egipto aseguró que cualquier actividad que pudiera ser interpretada como preparación para la guerra fuera presentada bajo el pretexto de ejercicios prolongados (El Gamasy, 1993).

Granito III fue la etapa final del plan de engaño, ejecutada en los días y semanas previos a la ofensiva del 6 de octubre de 1973. En esta fase, Egipto aumentó su presencia militar en las cercanías del canal, pero se aseguraron de que esta actividad se mantuviera dentro de los parámetros establecidos por las fases anteriores. Las maniobras se hicieron más frecuentes e intensas, pero aún parecían una continuación de los ejercicios rutinarios.

Uno de los elementos más importantes de *Granito III* fue el manejo de la diplomacia internacional. Sadat y otros altos funcionarios egipcios realizaron declaraciones públicas que enfatizaban la necesidad de

resolver el conflicto a través de negociaciones pacíficas. Estas declaraciones fueron acompañadas de esfuerzos diplomáticos para restar importancia a cualquier actividad militar en el Sinaí, lo que reforzó la percepción de que Egipto no estaba buscando un conflicto inmediato (Kissinger, 1982)

Durante *Granito III*, las tropas egipcias fueron colocadas en sus posiciones finales sin alertar al enemigo. Los movimientos de última hora, como el posicionamiento de unidades de artillería y sistemas de defensa aérea, fueron cuidadosamente ocultados a través de la desinformación y la minimización de las comunicaciones entre los altos mandos. Egipto también restringió las transmisiones de radio y utilizó mensajeros para garantizar que los preparativos finales no fueran detectados por la inteligencia israelí (Shazly, 1980).

Desde la perspectiva de las operaciones de información, las *Operaciones Granito* fueron un éxito rotundo en cuanto a su objetivo principal: lograr la sorpresa táctica y permitir que Egipto lanzara su ofensiva con la mínima interferencia de Israel en las primeras horas. Al desensibilizar a las fuerzas israelíes, Egipto logró que su cruce del Canal de Suez fuera un éxito inicial. Para cuando Israel se dio cuenta de la magnitud del ataque, las fuerzas egipcias ya habían asegurado importantes cabezas de puente en el lado oriental del canal.

La sorpresa estratégica alcanzada por las *Operaciones Granito* permitió a Egipto penetrar las defensas israelíes en la Línea Bar-Lev, algo que no hubiera sido posible sin la efectividad del engaño y la

desinformación llevados a cabo en las tres fases. La capacidad de Egipto para ocultar sus verdaderas intenciones mediante maniobras de distracción y declaraciones diplomáticas redujo significativamente la capacidad de Israel para responder a tiempo (Herzog, 1975).

Figura 8

Fuerzas egipcias cruzando el Canal de Suez

Nota: Lt. Col. Nathan A. Jennings, PhD, U.S. Army (2023)

Las operaciones *Granito I, II y III* representan un caso excepcional en el uso de operaciones de información para alcanzar la sorpresa estratégica en un conflicto bélico. El engaño táctico y la desinformación ejecutados por Egipto lograron tomar a Israel desprevenido, lo que permitió el éxito inicial de la Operación Badr. Las lecciones de estas operaciones subrayan la importancia de un enfoque estratégico integral en las operaciones de información, combinando engaño, protección de la información y adaptación en tiempo real.

Conclusiones

Luego de haber revisado en el presente capítulo el impacto de las operaciones de información en dos hechos bélicos de gran relevancia, como lo fueron la II Guerra Mundial y la Guerra de Yom Kipur, se puede afirmar la gran relevancia que tiene este tipo de operaciones en los resultados de las acciones que se realizan de forma cinética, ahorrando en muchas ocasiones un mayor derramamiento de sangre o derroche de recursos para quienes las emplean de forma asertiva.

Desde una perspectiva teórico - doctrinaria referida a INFOOPS, se aprecia que, tanto el mando aliado con su Operación Bodyguard y los planificadores egipcios con las operaciones Granito, lograron generar una ventaja de la información sobre sus adversarios para los fines que buscaban con ello. Independiente de lo anterior, ambos casos tuvieron resultados diferentes en el contexto de las operaciones Overlord y Badr, respectivamente, pero que no obedecieron a los efectos de las INFOOPS, por tanto, se puede mencionar que estas últimas siempre constituirán un aporte para las operaciones principales.

Derivado de lo anterior, constituye casi un imperativo para los comandantes y sus estados mayores el buscar la ventaja de información, ya que permite contar con la iniciativa en términos de comprensión situacional, toma de decisiones y comportamiento de los actores relevantes. Es por esto, que al considerar el muy reconocido ciclo OODA[2], se puede evidenciar que las INFOOPS constituirán un

[2] Observar, orientarse, decidir y accionar.

verdadero aporte para proteger y acelerar el propio, mientras se busca afectar y ralentizar el del adversario, logrando efectos que repercutirán finalmente en los resultados de las operaciones militares.

Así, los efectos generados en retener fuerzas acorzadas alemanas en el paso de Calais, sumado a divisiones completas del Eje amarradas en Noruega o los Balcanes, para el caso de la II Guerra Mundial, o el logro en concentrar fuerzas egipcias en el Canal de Suez sin levantar mayor alerta, en adición a mostrar un estatus de encontrarse poco entrenados para cruce del mismo canal, para el caso del Yom Kipur, constituyen a todas luces un triunfo en generar una ventaja de la información que se tradujeron en éxitos para las operaciones militares.

Para ambos casos, se realizó un análisis basado en el conocimiento actual de las INFOOPS, con la estructura y alcances propios de ellas. En ambas épocas, los planificadores consideraron la generación de engaño o decepción militar, conforme a los tiempos y doctrinas vigentes.

Las INFOOPS han estado presentes a lo largo de toda la historia militar, aunque utilizando doctrinas y estructuras diferentes. Es poco probable que Napoleón haya pensado en combinar distintas IRCs, como MILDEC o MISO, durante la Batalla de Austerlitz. La disposición de las fuerzas en el terreno, ocultamiento de las unidades de artillería y caballería, sumando actividades de engaño, efectivamente lograron confundir a los rusos y austriacos, quienes al atacar dejaron sus flancos expuestos. Incluso, desde la propia historia militar chilena, se puede apreciar que las acciones realizadas por las tropas nacionales previo al

asalto y toma del Morro de Arica, con las fogatas en el campamento de Chacalluta que simulaban presencia de tropas, tampoco debieron fueron resultado de un detallado plan de MILDEC del nivel operacional.

Finalmente, y desde la perspectiva histórica, existen evidencias para poder concluir que las INFOOPS han estado presente, más de manera conceptual que ligadas a una definición rígida, en todos los conflictos armados. Si bien es cierto que los recursos y tecnologías han ido variando (fogatas, telégrafo, guerra electrónica, ciber operaciones, etc) junto con el carácter de la guerra, sin embargo, buscar influir en las decisiones de los comandantes y líderes adversarios ha sido siempre un factor predominante para el triunfo en cualquier empresa bélica.

Referencias Bibliográficas

Beaches of Normandy. (s.f.). *Operation Bodyguard*. https://www.beachesofnormandy.com/articles/Operation_Bodyguard/?id=05cba00f2f

Cochran, E. (1998). *The egyptian staff solution: operational art and planning 1973 Arab – Israeli War. Newport*: Naval War College.

Department of the Army. (2023). *ADP 3-13 INFORMATION*. Washington DC: Department fo the Army.

Donovan, M. (2002). *Strategic deception: Operation Fortitude*. Carlisle: US Army War College.

Dunstan, S. (2009). *The Yom Kippur War: The Arab-Israeli War of 1973*. McFarland.

Ejército de Chile. (2017). D-10001 *"El Ejército".* Santiago, DIVDOC.

Ejército de Chile. (2019). DD-10001 *"La Fuerza Terrestre"*. Santiago, Chile: DIVDOC.

El Gamasy, M. (1993). *The October war: Memoirs of Field Marshal El Gamasy of Egypt*. American University in Cairo Press.

Estado Mayor Conjunto. (2023). *DNC-5-0 "Doctrina para la Planficación Conjunta"*. Santiago: Estado Mayor Conjunto.

Estado Mayor Conjunto. (2024). *DNC 3-7 "Operaciones de Información"* (2do Borrador). Santiago, Chile: EMCO.

Haig, Z. (2020). *Novel interpretation of information operations in today's changed operational environment*. Budapest: National University of Public Service.

Herzog, C. (1975). *The War of Atonement*, October, 1973. Boston: Little, Brown and Company.

Jennings, N. A. (2023). *Fighting with agility: The 162nd Armored Division in the 1973 Arab-Israeli War*. Military Review. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2023/Fighting-with-Agility/

Kissinger, H. (1982). *Years of upheaval* . Little, Brown and Company.

Ministerio de Defensa. (2017). *Libro de la Defensa Nacional de Chile*. Santiago: MDN.

NATO. (2023). *Allied Joint Publication-10.1 Information Operations*. (P. e. autor, Trad.) NATO.

Pattison, P. (s.f.). *D-Day Deception: Operation Fortitude South*. English Heritage. https://www.english-heritage.org.uk/visit/places/dover-castle/history-and-stories/d-day-deception/

Shazly, S. (1980). *The crossing of the Suez: The October war, 1973*. Third World Centre for Research and Publishing.

CAPÍTULO 2

¿Ambiente o Dimensión de la Información?

Teniente Coronel Martín Muñoz Lepe[3]

Introducción

Las operaciones militares, sin importar su naturaleza (ya sean de guerra o distintas a la guerra), se desarrollan en contextos únicos e irrepetibles. Por lo tanto, la estrategia que se plantee para abordar el problema militar que una operación conlleva, estará supeditada a un correcto análisis y comprensión del ambiente operacional donde se desarrolle, considerando que, si no se toma en cuenta este ambiente, el problema militar estará mal identificado y/o la estrategia formulada no abordará adecuadamente el problema de fondo.

Por otro lado, desde la llegada de la era de la información, el desarrollo e incorporación del concepto de operaciones de información al léxico militar ha experimentado un frenético progreso en ejércitos referentes y sus alcances han impactado en el ámbito regional y nacional. Esto se evidencia a través de diversas publicaciones académicas y doctrinarias, además de la adaptación de organizaciones militares para institucionalizarlo y la inclusión de sus actividades asociadas en la planificación de operaciones militares. De esta forma, se introduce un

[3] Teniente Coronel del Ejército de Chile. Oficial de Estado Mayor del Ejército de Chile y del Ejército de Argentina. Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica, Academia de Guerra del Ejército de Chile. Actualmente, es profesor de la ACAGUE. ✉ martin.munoz@acague.cl.

nuevo paradigma que plantea que, para conducir y ganar batallas, es necesario lograr la superioridad en la información. Es decir, se ha transitado desde un esquema que prioriza la maniobra mediante el movimiento con apoyo de fuego y técnico, hacia un diseño donde el empleo coercitivo es solo una parte de esta, pues en esto se integran el apoyo a la población, las operaciones psicológicas y un manejo integral de la información en un área de responsabilidad determinada.

En consecuencia, este capítulo profundiza sobre la creciente importancia de la información en el ámbito militar contemporáneo, desplazando su rol de instrumento secundario a convertirse en un factor decisivo para el éxito. Seguidamente, se realiza una breve discusión bibliográfica sobre el concepto del ambiente de la información, para luego interconectarlo con el ambiente operacional.

Finalmente, se distingue la relación entre dominios y dimensiones, profundizando en la dimensión de la información y sus respectivos entornos y capas. Entre los hallazgos es posible aseverar que el ambiente de información, más allá de ser una parte del ambiente operacional, constituye una dimensión transversal a todos los dominios.

La información como recurso crítico

La información siempre ha sido una herramienta esencial para lograr ventajas en una guerra, sin embargo, esta no ha sido reconocida como un arma en sí misma. La evolución de las tecnologías de la información y las comunicaciones (TIC), la más la creciente dependencia de sistemas tecnológicos en todos sus ámbitos, incluso las operaciones militares; han

cambiado esta percepción radicalmente. Actualmente, estas tecnologías han facilitado la difusión de mensajes que al ser percibido de diferentes maneras según los actores intervinientes, pueden generar efectos específicos. A su vez, permiten el acceso a fragmentos de la verdad, un ejemplo de ello es el caso de la guerra entre Rusia y Ucrania, donde la información se ha convertido en un recurso esencial para lograr el éxito en una operación militar.

Más aún, conflictos recientes como la segunda guerra de Nagorno Karabaj, han demostrado la relevancia que ha alcanzado la información como elemento decisivo en el campo de batalla, siendo el control y la gestión de esta los ejes centrales dentro de la planificación y funciones de combate,

Históricamente la información ha sido y será considerada un elemento decisivo y crítico dentro de las operaciones militares. Por ejemplo, Napoleón utilizaba información precisa sobre las fuerzas enemigas y del campo de batalla para sorprender a sus adversarios. Keegan (2003) destaca la combinación entre información y movilidad que ejecutaba Napoleón para maximizar y obtener ventajas, las cuales permitieron desarrollo lo que se conoce como “guerra de maniobra”.

Otro ejemplo histórico, lo constituye la campaña aliada del Día “D” durante la Segunda Guerra Mundial. Previo al desembarco en Normandía en 1944, los aliados usaron información clave sobre las fuerzas alemanas, de las condiciones meteorológicas y sobre los efectos de las operaciones llevadas a cabo, permitiéndoles actuar en el momento

oportuno y confundir al adversario respecto al lugar del desembarco. Según Ambrose (2002), esto permitió a los aliados ubicarse en una posición geográfica ventajosa, lo cual fue crucial para el éxito de la mencionada operación.

A lo largo de la historia, los tomadores de decisiones, representados por los comandantes, han comprendido el valor superlativo de la información, utilizándola no solo para influir en el campo de batalla físico, sino también para afectar la moral de las tropas y la percepción pública. La manipulación de la información puede ser considerada una capacidad dentro del campo de batalla para lograr oportunidades que vayan en directo beneficio de las fuerzas en términos geográficos, psicológicos y morales. Un ejemplo de lo anterior, es el uso de las operaciones psicológicas para debilitar la moral en el adversario. Freedman (2013) señala que, durante la Guerra del Golfo en 1991, las fuerzas estadounidenses emplearon tácticas de desinformación y de campañas psicológicas para reducir la moral de las tropas iraquíes, complementando con acciones militares directas.

Actualmente, la rápida creación, distribución y acceso a información han transformado la guerra, ya que la digitalización y tecnología han incidido directamente en la capacidad de influir, persuadir, confundir, coaccionar o engañar, haciendo aún más desafiante el escenario. Pues, el volúmen de información al que se puede acceder contrasta con la necesidad de gestionarla eficazmente.

En consecuencia, a medida que más personas interactúan y realizan

actividades en el ciberespacio, las narrativas y la información tienen una influencia creciente en los conflictos y la inestabilidad. Las acciones e imágenes de las unidades militares desplegadas son observadas, interpretadas y redistribuidas, afectando la percepción pública y las decisiones de los actores involucrados. La capacidad de aprovechar estas tecnologías en constante evolución ofrece oportunidades a nivel global, las cuales pueden ser utilizadas de diversas formas dependiendo de los objetivos de quien gestione la información.

El ambiente de la información

El concepto de ambiente de la información ha cobrado gran relevancia en los estudios de defensa y seguridad, a raíz de dependencia excesiva de las tecnologías de la información en las operaciones militares. En este contexto, el ambiente de la información se comprende como actores, sistemas y factores que interactúan dentro del dominio informacional, influyendo en el proceso de toma de decisiones y en el desarrollo de los conflictos. Las operaciones militares ya no se limitan exclusivamente a los ámbitos físico y geográfico, hoy dependen en gran medida del control y la influencia sobre el flujo de información.

En el marco de la doctrina militar estadounidense, particularmente para el Departamento de Defensa de los Estados Unidos (DoD, 2020), a través del JP 3-13, define el ambiente de la información (AI)[4] como "la agregación de individuos, organizaciones y sistemas que recopilan,

[4] En el transcurso del capítulo al hacer referencia al ambiente de la información se utilizará la sigla AI.

procesan, diseminan o actúan en función de la información". Desde la perspectiva norteamericana es posible destacar que, el AI no es únicamente un espacio físico o cibernético, sino que incluye aspectos cognitivos y sociales, donde la información fluye y afecta el comportamiento de los actores involucrados en el conflicto.

En otro sentido, la Organización del Tratado del Atlántico Norte (OTAN) considera que el AI está compuesto por tres dimensiones principales: física, informacional y cognitiva. La dimensión física contempla los medios de comunicación y redes a través de los cuales la información se transmite, mientras que la dimensión informacional corresponde al contenido de la información en sí, y en tercer lugar la dimensión cognitiva se relaciona con la forma en que los seres humanos perciben, procesan y actúan sobre la información. Este enfoque destaca la importancia de influir en la percepción del adversario y otros actores clave, ya que la interpretación de los datos informativos puede ser determinante en la estrategia de un conflicto (NATO, 2021).

No obstante, desde una perspectiva académica, Rid (2012) plantea que el AI debe entenderse como un espacio estratégico donde no solo las fuerzas armadas, sino también actores no estatales, medios de comunicación y poblaciones civiles interactúan para moldear la percepción de la realidad. Por tanto, el control del flujo de información puede ser tan decisivo como el control físico de un territorio. La "guerra de la información", tal como lo sugiere Rid, transforma la manera en que se desarrollan los conflictos, priorizando la manipulación de la percepción y el uso de redes de información como armas en sí mismas.

Por otra parte, Alford (2016) en una investigación sobre ciberseguridad aborda el AI desde una perspectiva técnica, enfatizando que las infraestructuras críticas de información, como las redes de comunicación y los sistemas de gestión de datos, son esenciales para la efectividad de las operaciones militares. En este contexto, el control y la defensa de estos sistemas se convierten en pilares fundamentales del éxito estratégico, especialmente en operaciones cibernéticas, donde los ataques pueden degradar significativamente la capacidad del adversario para coordinar y ejecutar acciones militares.

Consecuente con lo planteado, se puede concluir que la definición de AI ha evolucionado hacia una comprensión más amplia que incluye no solo la tecnología (medios y redes), sino también los actores humanos y sus percepciones. En los conflictos contemporáneos, la capacidad de controlar y explotar el AI es tan importante como el control del terreno físico, un ejemplo es la guerra entre Rusia y Ucrania, donde ambos bandos utilizan redes sociales, operaciones cibernéticas y propaganda para influir en la opinión pública internacional y en las percepciones de sus adversarios.

La dependencia de las infraestructuras de información también presenta vulnerabilidades críticas, debido a que las operaciones de ciberataque dirigidas a sistemas de información pueden interrumpir la capacidad del adversario para coordinar fuerzas, afectando tanto las operaciones tácticas como las estratégicas. Según Alford (2016), la protección de las infraestructuras críticas de información es un componente vital de cualquier estrategia militar.

En conclusión, el AI es, sin lugar a duda, multidimensional, abarcando el entorno físico, los contenidos informacionales y los factores cognitivos asociados con la percepción humana. Estos componentes interactúan de forma dinámica y compleja, influyendo en los conflictos militares y en el proceso de toma de decisiones de los actores involucrados.

Por lo tanto, para los fines de este capítulo se entenderá por AI al espacio compuesto por infraestructuras físicas, contenido informacional y percepciones cognitivas que interactúan para influir en la toma de decisiones y en las operaciones militares, donde el control y la manipulación de estos elementos crearán efectos asociados a una acción o inacción de la audiencia y actores que, en su conjunto, pueden determinar el curso de un conflicto.

La dimensión de información en el ambiente operacional

Las operaciones militares, sin importar su naturaleza, se llevan a cabo en un contexto estratégico único e irreproducible, incluso cuando las condiciones parecen similares. Colin S. Gray, en su obra "The Strategy Bridge" (2010), enfatiza la importancia del contexto estratégico, señalando que cualquier estrategia será ineficaz si no se ajusta al entorno en el que se aplica. Por tanto, un análisis adecuado del contexto es primordial en cualquier tipo de conflicto (Gray, 2010). En el mismo orden, el éxito depende en gran medida de la correcta comprensión del ambiente en el que se desarrollan, dado que la estrategia o solución a un problema está directamente relacionada con su entorno

único. Es decir, una operación militar cobra sentido únicamente si considera el Ambiente Operacional (AO), donde la información desempeña un papel fundamental en los tiempos contemporáneos.

Debido a que es un concepto esencial dentro de la planificación y ejecución de las operaciones militares indistintamente, ya que todo lo que se suscita en el entorno afecta positiva o negativamente en las actividades que se llevan a cabo. Las operaciones militares se basan en el enfrentamiento de las amenazas presentes en un espacio geográfico específico, con la finalidad de imponer condiciones favorables y alcanzar una misión mediante la ejecución de diversas tareas.

Uno de los aspectos más importantes es conocer y comprender las capacidades reales de los medios empleados en las operaciones, ya que estas no dependen únicamente de la cantidad o características de los recursos disponibles (como sistemas de armas o recursos humanos), sino también de cómo el AO impacta en su uso. En otras palabras, el éxito de las operaciones militares está profundamente influenciado por las características del área o teatro de operaciones, que pueden ofrecer tanto ventajas como limitaciones. Por ejemplo, según Beevor (1988), en la batalla de Stalingrado durante la Segunda Guerra Mundial, la comprensión del AO fue clave para el éxito soviético. Los comandantes soviéticos aprovecharon el invierno ruso, las condiciones urbanas y la falta de suministros de las fuerzas alemanas para rodearlas y destruirlas. Este análisis abarcó no solo el terreno físico, sino también las vulnerabilidades logísticas y morales del adversario. De manera similar, durante la guerra de Vietnam, Estados Unidos subestimó el ambiente

social y político de Vietnam del Norte y el Vietcong. La Ofensiva del Tet mostró que, aunque el ejército estadounidense obtuvo un triunfo militar, el impacto psicológico y propagandístico de las operaciones del Vietcong debilitó la opinión pública que estaba a favor de la guerra, lo que demuestra que el AO trasciende el plano físico del campo de batalla.

En el AO contemporáneo es evidente que, aunque cada conflicto tiene su propia dinámica y particularidades, existen condiciones, circunstancias e influencias regionales y globales que afectan y condicionan el entorno, tales como la inestabilidad política, las problemáticas migratorias, los conflictos violentos y la economía global. Estos factores afectan el presente y condicionan el futuro de los conflictos, puesto que, los conflictos actuales tienden a presentar patrones comunes, como un alto nivel de complejidad sistémica y humana, la prevalencia de conflictos internos e interestatales, y una notable presencia de grupos armados insurgentes en un contexto de prolongada conflictividad. Este último punto es relevante, dado que se estima que prevalecen intereses geopolíticos de actores estatales en busca de recuperar o mantener sus influencias.

Lo anterior presenta un entorno complejo, marcado por dos fenómenos relativamente novedosos. El primero es el uso de fuerzas bajo el umbral de la agresión, también conocido como Zona Gris del conflicto. El segundo, es la prevalencia de amenazas híbridas en el uso del poder, que incluyen ciberoperaciones, campañas de información y terrorismo. El objetivo de esto es lograr una mayor efectividad en el uso de la fuerza, generando a la vez una mayor dificultad para que la voluntad

contraria pueda llevar a cabo sus operaciones. Por lo tanto, desde un punto de vista estratégico, es necesario prever y gestionar la fuerza para hacer frente a estos escenarios de conflicto.

Así, los dominios de ciberespacio y espacio se han integrado a los tradicionales dominios terrestre, naval y aéreo, sin que estos últimos hayan perdido su vigencia. Esta integración subraya la necesidad de abordar los problemas actuales mediante soluciones integrales a nivel estatal, con interconexiones y relaciones múltiples de naturaleza heterogénea. En este contexto, las fuerzas militares desempeñan un papel importante, pero no son las únicas responsables.

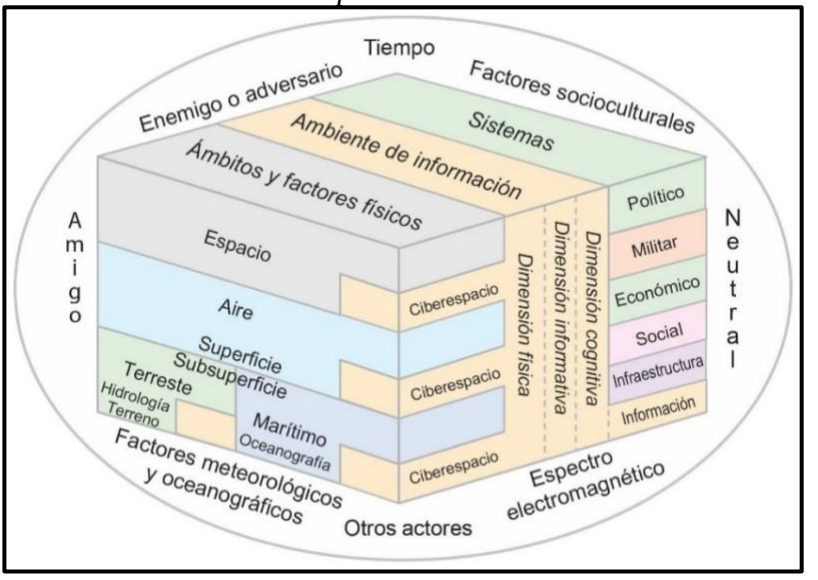
En el ámbito nacional, la doctrina conjunta define el AO como una combinación de condiciones, circunstancias e influencias que afectan tanto el uso de las capacidades militares como el proceso de toma de decisiones del comandante (DNC 2-04, 2016). Para comprender este entorno de manera efectiva, es necesario adoptar una visión integral que trascienda las fuerzas y capacidades de combate del adversario en un área de operaciones determinada, toda vez que existe un conjunto de otras variables y actores que, en constante interacción, influyen en factores sociales, culturales, lingüísticos, psicológicos, técnicos y físicos. Estos afectan la forma en que los tomadores de decisiones y los sistemas automatizados interpretan la información.

Por tanto, este enfoque holístico debe abarcar no solo la dimensión física y humana, sino también la dimensión informacional, ya que estas dimensiones influirán transversalmente en todos los dominios (terrestre,

marítimo, aéreo, espacial y ciberespacio). Gráficamente, el AO se representa tradicionalmente de acuerdo con la Figura N°1.

Figura 1

Visión holística del ambiente operacional



Nota: Joint Planning 5-0, 2020.

Esta perspectiva holística de observar el AO permite visualizar los diferentes dominios, variables, AI y otros aspectos interrelacionados y de cuya interacción y comprensión depende el entendimiento correcto de un problema militar. Así, el análisis del AO también incluye la evaluación de los sistemas y subsistemas que abarcan los factores PMESII[5] del adversario, de las propias fuerzas y actores neutrales que pueden influir en el desarrollo de las operaciones conjuntas.

[5] Políticos, Militares, Económicos, Sociales, Infraestructurales e Informativos.

Con ello se pretende resaltar que la comprensión del AO es esencial para identificar las condiciones necesarias que permitan alcanzar los objetivos que se establezcan, evitando efectos no deseados que pudieran obstaculizar el cumplimiento de la misión. Además, este conocimiento facilita la evaluación del impacto del adversario y otros factores, como la población civil, en el logro del plan y el estado final deseado. Desde una mirada más pragmática, se podría considerar que el ambiente se utiliza para describir el sistema que rodea a una operación militar desde una perspectiva física y no física.

No obstante, esta imagen (ver Figura 1) puede llevar a errores en su interpretación derivados de la interacción de la información en el AO, dado que este modelo representa el AI como una parte del AO y no necesariamente afectando al AO en su conjunto. Además, la figura indica que el ambiente de información se compone de tres dimensiones: cognitiva, física e informativa, abarcando el dominio del ciberespacio.

Esto permite plantear la siguiente cuestión:

¿Las dimensiones (física, informacional y cognitiva) son exclusivas del ambiente de la información o son transversales a todos los dominios?

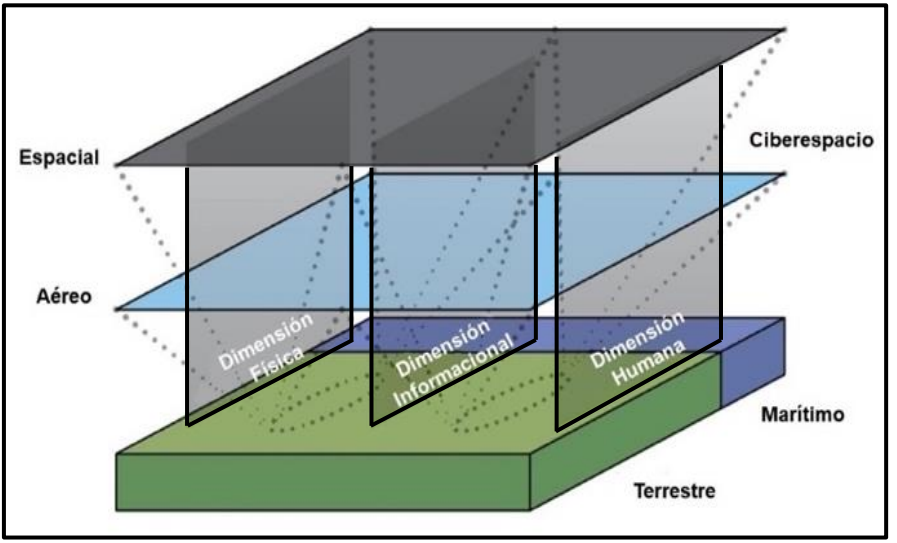
El AO se define a través de cinco dominios (tierra, mar, aire, espacio y ciberespacio), donde las dimensiones (física, informativa y humana) repercutirán en cada dominio. Por lo tanto, comprender las dimensiones físicas, informativas y humanas de cada dominio permitirá a los comandantes observar al adversario y a sus propias fuerzas, evaluar el

entorno operacional y anticipar los impactos de sus operaciones.

En consecuencia, son las dimensiones evidentemente trasversales a los cinco dominios definidos y en ningún caso exclusivas del AI, considerando además que, las acciones en una dimensión influyen en los factores de las otras dimensiones.

Figura 2

Ambiente Operacional: perspectiva de sus dominios y dimensiones



Nota: Field Manual 3-0.

Este nuevo enfoque no debe cambiar el concepto central de cómo entender el ambiente de información, sin embargo, como se observa en la Figura 2, en lugar de un AI separado, se debe considerar que las dimensiones físicas, humanas y de la información están presentes en cada dominio de la guerra. En otras palabras, no es necesario tener un AI aislado, porque la información está presente y es persistente en cada dominio. Por tanto, es más preciso referirse a la dimensión de la

información. Este nuevo enfoque, que ya ha sido integrado por el Ejército de los Estados Unidos, proporciona claridad y evita capacidades de información aisladas. En última instancia, es a través de estas dimensiones que se puede lograr una ventaja relativa sobre el adversario, incluida la ventaja informativa.

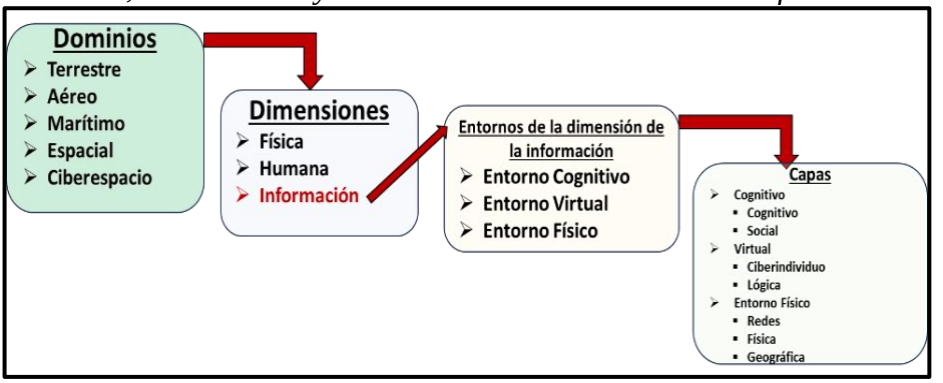
Si bien todas las dimensiones son relevantes para la comprensión del AO en su conjunto, se debe considerar que la dimensión de la información es el principal espacio donde se lleva a cabo el proceso de toma de decisiones, porque es en esta instancia donde los humanos y los sistemas automatizados observan, conciben, procesan, orientan, deciden y actúan sobre datos, información y conocimiento.

Dimensiones y entornos de la dimensión de la información

Como se ha mencionado, el AO se define a través de cinco dominios: terrestre, aéreo, marítimo, espacial y ciberespacio. Cada uno de estos dominios incluye tres dimensiones: física, humana y de la información (ver Figura 3).

Figura 3

Dominios, Dimensiones y Entornos de la Dimensión de la Información



Nota: ACAGUE, 2024.

La comprensión de las tres dimensiones de cada dominio, por parte de los tomadores de decisiones y sus asesores, es fundamental para evaluar y anticipar los impactos que tienen en las operaciones militares, al igual que para crear efectos en todos los dominios, según la aproximación operacional estimada, es decir, los dominios deben considerarse interrelacionados, contemplando tanto aspectos físicos como no físicos. Por ejemplo, los efectos en el dominio terrestre, como la destrucción de un nodo de comunicaciones adversario, puede ejecutarse desde plataformas aéreas, marítimas o terrestres. Esto se puede apreciar con la acción de la Fuerza Aérea sobre un cuartel general (HQ) adversario. Este mismo efecto puede apoyarse mediante la negación de espacio en la dimensión de información, utilizando la guerra electrónica para suprimir las defensas aéreas del HQ adversario. Simultáneamente, la dimensión humana puede ser influenciada a través del dominio cibernético mediante mensajes dirigidos a la población militar o civil, debilitando así la credibilidad del liderazgo del

comandante afectado.

Al analizar cada dimensión se puede establecer:

Dimensión física: Esta dimensión incluye las características y capacidades materiales, tanto naturales como artificiales, que existen dentro de un entorno específico. Cada dominio es inherentemente físico, abarcando elementos como el terreno, el clima, las fuerzas militares, la radiación electromagnética y los sistemas de armas. Las actividades o condiciones en esta dimensión generan efectos en las dimensiones humana y de información. Además, comprende la infraestructura tecnológica que soporta el flujo de información, incluyendo satélites, redes de comunicación y servidores (NATO, 2021).

Dimensión humana: Interacción entre individuos y grupos, cómo comprenden la información y los eventos, toman decisiones y actúan dentro de un entorno operativo. La voluntad de lucha emerge de la compleja interrelación entre la cultura, la emoción y el comportamiento. Influir en estos factores es crucial para alcanzar los objetivos militares, ya que implica la percepción y procesamiento de la información. Por tanto, este enfoque busca impactar en las decisiones y comportamientos de audiencias clave, incluyendo adversarios, civiles y aliados, así como otros actores en el área asignada para el cumplimiento de la misión.

Dimensión de la información: Es aquella que tiene directamente relación con el contenido, los datos y los procesos que utilizan los individuos, los grupos y los sistemas de información para comunicarse. Esta dimensión contiene la información misma, incluyendo texto e

imágenes, además, incluye el flujo o las vías de comunicación de esta.

Cabe mencionar que el intercambio de información puede ser realizado de variadas maneras, como mensajes, datos y cualquier tipo de información que se transmite a través de los medios disponibles, incluyendo aquellas asociadas a las operaciones de desinformación y propaganda. Es precisamente en esta dimensión dónde se llevarán a cabo las operaciones de información, ya que constituye el espacio conceptual intrínsicamente relacionado con los procesos de toma de decisiones, donde humanos y sistemas automatizados observan, crean, procesan, orientan, deciden y actúan sobre los datos, información y conocimiento.

Se caracteriza por una demanda extremadamente alta de acceso a fuentes digitales con una conectividad virtual e interpersonal casi en tiempo real y a una escala sin precedentes.

Finalmente, considerar que todas las actividades tendrán un efecto en el entorno cognitivo, ya sea diseñadas para ese efecto, como debido a la acción o inacción. Mediante el entendimiento y comprensión de la dimensión de la información, los efectos pueden diseñarse para influir en el comportamiento del adversario cuando observan, orientan y actúan sobre los datos, la información y el conocimiento.

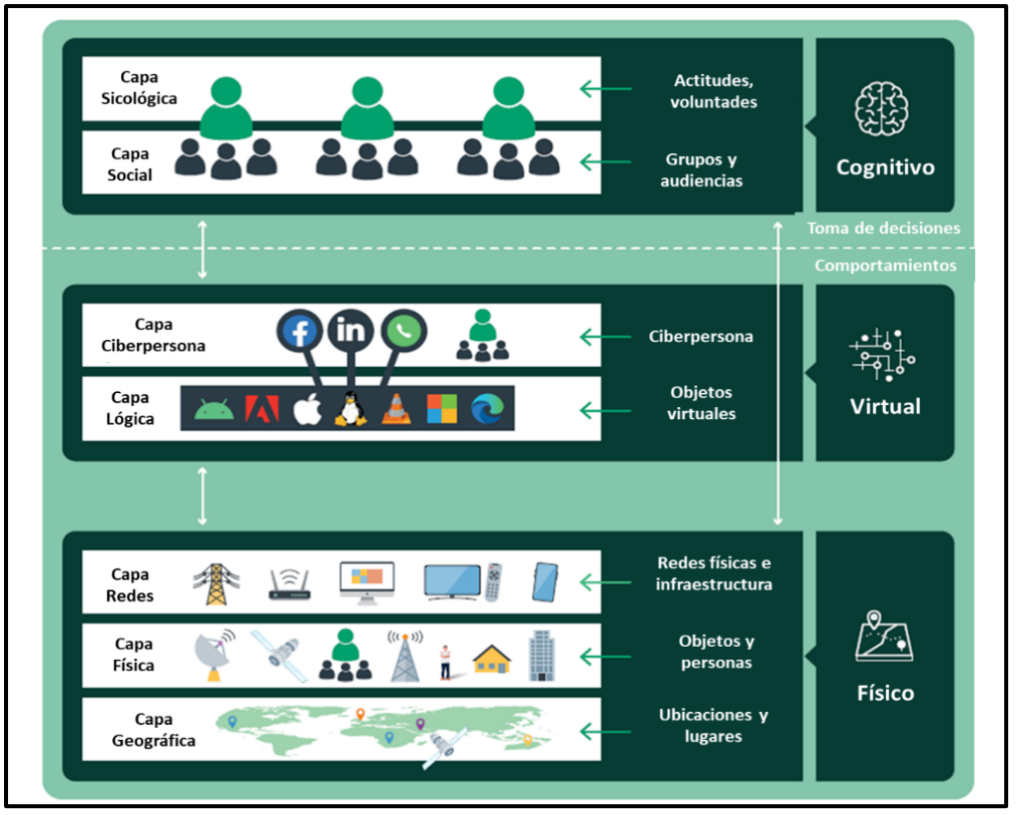
Entornos de la dimensión de la información

La dimensión de la información comprende tres entornos: cognitivo, físico y virtual, cada uno, a su vez, compuesto por varias capas que permiten un análisis preciso del ambiente para desarrollar efectos que

generen cambios en actitudes y comportamientos. La naturaleza interconectada de los entornos junto con sus capas, aumentan la oportunidad de identificar potenciales blancos, además de aspectos interrelacionados dentro del entorno de la información.

Figura 4

Entornos de la dimensión de la Información



Nota: Adaptación del AJP-10.1, 2023.

En conformidad con lo descrito por la NATO (2023), los entornos se describen de la siguiente manera:

***Entorno cognitivo*:** considerado el entorno principal, donde los efectos inciden en la "forma de pensar" de los individuos, lo que impulsa los comportamientos y toma de decisiones. Todas las acciones en otros entornos y sus capas afectan en última instancia al entorno cognitivo. Está constituido por dos capas: psicológica y social. La **capa psicológica** considera el espacio individual donde se interpreta la información, sin la necesidad de transmitirla. Esta capa es intangible, dónde se incluyen los procesos de voluntad, cohesión, percepciones, creencias, intereses, valores, objetivos, decisiones y comportamientos de los individuos.

En tanto la **capa social** es donde la información toma contexto en cómo los comportamientos de los individuos se ven influenciados por las presiones del entorno sociocultural, y donde las redes interpersonales y la cultura influyen en la toma de decisiones de los individuos. Abarca todas las formas de interacción, por ejemplo, entre personas con las esferas económicas y/o políticas. Un factor relevante en esta capa serán los tomadores de decisiones claves dentro una audiencia, donde su credibilidad, nivel de influencia y alcance, entregarán información a los tomadores de decisiones sobre cómo producir una mayor influencia en una determinada audiencia.

***Entorno virtual*:** donde comúnmente las audiencias interactúan de manera virtual. Se compone de dos capas: **ciberpersona** y **lógica**. La primera se refiere a cómo los individuos de una audiencia se manifiestan como un perfil en línea e interactúan a través de seguidores y suscriptores con contenidos digitales. Esto incluye tanto al público individual (por ejemplo, perfiles de Twitter) como grupal (por ejemplo, grupo de

WhatsApp). Los individuos pueden tener múltiples personalidades digitales y los actores virtuales pueden operar como personas a través de inteligencia artificial (por ejemplo, chatbot de respuesta atención al cliente). Además de su influencia física, los influenciadores claves pueden impactar a una audiencia a través de la capa de ciberpersona.

La segunda y última capa del entorno virtual, denominada **lógica**, contiene menos actividades perceptibles por el ser humano en la forma de procesamiento, almacenamiento y transmisión de datos analógicos/digitales e información. Es el entorno virtual donde se encuentran los servicios y recursos que se utilizan para intercambiar datos, tales como servicios de redes sociales y almacenamiento de archivos. Esta capa también incluye las configuraciones de red, protocolos de transferencia de datos, dominios y otros procesos electromagnéticos o virtuales. Esta capa es casi exclusiva al dominio del ciberespacio donde las acciones pueden afectar la confidencialidad, integridad o accesibilidad de los datos.

***Entorno físico*:** el cual da cuenta de las áreas geográficas donde habitan las audiencias, incluidos todos los objetos físicos y la infraestructura que los soporta. Es el espacio donde se desarrollan las actividades físicas y donde las personas, naciones, estados, culturas y sociedades interactúan. Se compone de tres capas: 1) La **capa redes** es la infraestructura de redes físicas que subyace a las capas virtuales. Esta capa es donde se lleva a cabo la transmisión y recepción de datos en bruto no estructurados, entre un dispositivo y un medio de transmisión físico. Esta capa incluye las capacidades que permiten la comunicación, como

antenas de radio, transmisores y receptores satelitales, además de aquellos que convierten los bits digitales en señales analógicas o viceversa para su transmisión y recepción; 2) La **capa física** es donde las audiencias interactúan y donde reside la infraestructura física técnica de comunicaciones y la humana. La infraestructura humana está compuesta por aquellas áreas físicas que facilitan la comunicación, como un mercado, un lugar de reunión o lugares de cultos religiosos. Se debe considerar que las palabras y las imágenes son parte de información física y no virtual y; 3) La **capa geográfica** explora cómo las audiencias habitan la Tierra. También analiza cómo la geografía física y el clima afectan la forma en que las audiencias se logren comunicar.

Conclusiones

A lo largo de la historia, la información ha constituido un recurso relevante en la planificación y ejecución de las operaciones militares, pero la evolución de las tecnologías de la información y las comunicaciones (TIC) han incrementado su relevancia a niveles sin precedentes. Actualmente, la información no solo robustece el proceso de toma de decisiones en el campo de batalla, sino que también influye en la moral de las tropas, la percepción pública y el desenlace de los conflictos. Particularmente, en la era digital, la capacidad de gestionarla y explotarla ha adquirido una importancia central en los conflictos modernos, debido a la influencia que ejerce en las narrativas en el ciberespacio, el uso de la información como arma psicológica y la necesidad de gestionar grandes volúmenes de datos presentan nuevos desafíos para los comandantes y sus estados mayores.

Respecto a la multidimensionalidad del ambiente de la información, cabe señalar que este no solo contempla los aspectos tecnológicos, como las infraestructuras de comunicación y los sistemas de gestión de datos, sino que también incluye dimensiones cognitivas y sociales, lo cual complejiza la efectividad de las operaciones militares, ya que dependen tanto del control físico del terreno como de la capacidad de influir en la percepción y comportamiento de los actores intervinientes en el conflicto.

Por otra parte, es necesario destacar la importancia de la comprensión integral del AO, toda vez que la efectividad de las operaciones militares depende en gran medida de la comprensión profunda del ambiente, por lo cual este análisis no solo debe considerar las capacidades físicas y tácticas del adversario, sino también factores sociales, culturales, psicológicos y de información que influyen en la dinámica del conflicto. Al considerar estos elementos interrelacionados, los planificadores y comandantes pueden anticipar mejor los impactos de sus decisiones y maximizar el potencial de éxito en sus misiones.

Lo anterior conlleva la necesidad de integrar las dimensiones de información en todos los dominios, porque a medida que evoluciona el conflicto, la información se convierte en un elemento presente y crítico en cada dominio de este. La integración de las dimensiones física, humana e informativa en la planificación y ejecución de operaciones no solo proporciona una ventaja estratégica, sino que también mejora la toma de decisiones en entornos complejos. Puesto que, reconocer que la información es inherente a cada dominio, permite abordar los desafíos

contemporáneos de manera más efectiva, evitando la fragmentación de capacidades y promoviendo un enfoque más coordinado.

Se deja en evidencia que existe una interconexión de dimensiones y entornos. Las diversas dimensiones presentes en el AO—física, humana e informativa—no actúan de manera aislada, sino que están interrelacionadas. Las decisiones en un dominio pueden influir significativamente en otros, lo que subraya la importancia de una visión holística al planificar y ejecutar operaciones. Esta interdependencia resalta la necesidad de comprender la dinámica de estas dimensiones para anticipar y evaluar los efectos de sus acciones en todos los niveles de la conducción militar.

Como se ha mencionado previamente, la dimensión de información emerge como un elemento crítico en los conflictos modernos, donde la manipulación de la percepción y el flujo de datos pueden alterar la realidad. El reconocimiento de los entornos cognitivo, físico y virtual, al igual que sus capas, permite desarrollar estrategias que no solo influyan en el comportamiento de las audiencias, sino que también maximicen la efectividad de las operaciones. En un contexto donde la información fluye rápidamente, la capacidad de influir en la cognición humana se convierte en un factor decisivo para el éxito de las operaciones militares.

Como corolario, es necesario señalar que es inoficioso observar el AI como un componente paralelo al AO, muy por el contrario, es necesario observarlo como una dimensión que se encuentra presente en mayor o menor medida en todos los dominios (propio de un problema

multidominio). Por lo tanto, se sugiere observarlo como una dimensión y su interpretación se encontrará supeditada al correcto análisis que emerja de su entorno y respectivas capas.

Referencias Bibliográficas

Alford, M. (2016). *Cyber Security and Critical Information Infrastructure Protection*. Palgrave Macmillan.

Ambrose, S. E. (2002). D-Day, June 6, 1944: *The Climactic Battle of World War II.* Simon & Schuster.

Departamento de Defensa de los Estados Unidos. (2020). *Joint Publication 3-13*: Information Operations.

DNC 2-04 (2023), Ministerio de Defensa Nacional, *Preparación de inteligencia del ambiente operacional conjunto* (JIPOE)

DNC 3-07 (2013). *Operaciones de Información.* Ministerio de Defensa Nacional.

Freedman, L. (2013). *Strategy: A History*. Oxford University Press.

Gray, C. S. (2010). *The Strategy Bridge: Theory for Practice*. Oxford University Press.

Keegan, J. (2003). *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda. Knopf.*

NATO. (2021). AJP-3.10 *Allied Joint Doctrine for Information Operations.* Brussels: NATO Standardization Office.

NATO. (2023). AJP-10.1 *Allied Joint Doctrine for Information Operations.* Brussels: NATO Standardization Office.

Rid, T. (2012). *Cyber War Will Not Take Place*. Oxford University Press.

CAPÍTULO 3

Evolución doctrinaria de las operaciones de información y los desafíos para un empleo integral

Coronel Ricardo Kaiser Onetto[1]

Introducción

Las operaciones de información (INFOOPS – *information operations*) no es una modalidad nueva de hacer la guerra. En efecto, ha estado presente desde tiempos memoriales, pero con otras formas de planificación y ejecución. Un ejemplo de ello, es relatado por Homero en lo que fuera la ardua conquista por la ciudad de Troya. Habiendo sido asediada por largos diez años, los atacantes griegos no habían podido sobrepasar los altos muros, por lo que el ingenio los hizo fabricar un inmenso caballo donde penetraron la ciudad amurallada con cientos de guerreros en su interior (National Geographic, 2023).

Así, muchos ejemplos de la historia militar nos permiten dar el contexto de la evolución doctrinaria de las INFOOPS. Para ello, el presente capítulo toma como referencia la doctrina de Estados Unidos, país que Chile mira de cerca para incorporar sus tácticas, técnicas y

[1] Oficial de Ejército con la especialidad de Estado Mayor. Actualmente se desempeña como Jefe de Estado Mayor de la División Doctrina, Jefe del Departamento de Doctrina Operacional y Equipamiento y Jefe del Centro de Lecciones Aprendidas del Ejército. Correo: ricardo.kaiser@ejercito.cl

procedimientos a la doctrina propia.

Si damos un salto en el tiempo a lo que hoy se concibe como las INFOOPS, conceptualmente se puede definir que “es el empleo integrado de las capacidades relacionadas con la información, en coordinación con otras líneas de operaciones para influir, perturbar, dañar o usurpar la toma de decisiones de adversarios, protegiendo, al mismo tiempo la propia” (Wade, 2021). Estas capacidades, surgen y avanzan cada día, requiriendo de un esfuerzo sincronizado y coordinado para su empleo.

Sin embargo, para llegar a esa definición será necesario poner en contexto el tránsito histórico-doctrinario que han sufrido las INFOOPS, aspecto que es relatado con detalle y basado en fuentes relacionadas con el tema en cuestión.

En marzo de 2019, un anuncio clave efectuado por el Teniente General Fogarty sobre la transformación del Comando Cyber del Ejército de EE.UU. (ARCYBER – *Army Cyber Command*) en un Comando de Guerra de la Información marcó un hito relevante en la forma de abordar y combatir los desafíos en la era de la información (Underwood, 2019).

Desde su creación, los norteamericanos han aprovechado poco a poco el poder de la información tanto en lo que ellos denominan la

competencia[2], como en el conflicto. Pero para que la transformación del ARCYBER fuera realmente eficaz a la hora de hacer frente a los desafíos del siglo XXI y sirvan de referencia para la doctrina propia, es necesario examinar su evolución en busca de los esfuerzos efectuados con anterioridad para operar en el ambiente de la información, la cual está en constante expansión y rápida evolución.

Por lo tanto, en este capítulo se analizan las INFOOPS desde una mirada evolutiva doctrinaria, donde el auge de las tecnologías relacionadas con la información (el medio), el poder de la narrativa (el mensaje) y la importancia de los medios de comunicación han incrementado la relevancia de la información en la guerra moderna.

Finalmente, la hipótesis planteada para el presente capítulo del tema de investigación central de la Academia de Guerra (TICA) es que las INFOOPS están en constante evolución doctrinaria por las tecnologías emergentes, la necesidad de revisar la narrativa y la influencia de las capacidades esenciales con la información para ganar la iniciativa en este ambiente.

Tecnología, narrativa y medios de comunicación social. Paragua doctrinario de las IO

Aprovechar la información en la guerra no es nada nuevo. Como señaló el ex secretario de Defensa Ash Carter el 2016: “a lo largo de la

[2] La competencia militar abarca la gama de actividades y operaciones empleadas para alcanzar objetivos políticos y negar a los adversarios la capacidad de alcanzar objetivos perjudiciales para Estados Unidos.

historia de la guerra, los militares han buscado la ventaja a través de acciones destinadas a afectar la percepción y el comportamiento del adversario" (Carter, 2016, p. 1). A partir de su afirmación, la guerra en la era de la información busca lograr el efecto de afectar las percepciones y comportamientos de la amenaza[3]. Para lograr este fin, es necesario utilizar tres medios claves: la tecnología, la narrativa y los medios de comunicación. Hoy, en el siglo XXI, la convergencia de estos medios ha alterado drásticamente el entorno informativo hasta un punto en el que ya no pueden ignorarse o abordarse por separado y que ha dado paso a una evolución doctrinaria sobre la materia.

En este debate sobre la comprensión de la guerra en la era de la información son fundamentales los ingredientes que sirven de componentes críticos. El primero de ellos es la tecnología. El desarrollo de tecnologías nuevas y más complejas a lo largo de la historia ha mejorado enormemente la capacidad de las Fuerzas Armadas (FAs) para enfrentar el conflicto. En simple, el ritmo de las tecnologías de la información ha aumentado exponencialmente. Como afirma David Alberts et al. (2004, p. 44): "la capacidad para emitir información, distribuirla a una gran audiencia o entregarla de forma más focalizada, incluso a individuos en movimiento, ha aumentado de forma espectacular". Desde la imprenta en 1440 hasta Facebook en el 2000, el

[3] En el capítulo se hará referencia al concepto "amenaza" de acuerdo con lo establecido en el MDO-90906: "DICCIONARIO MILITAR", Ed. 2022, es cual establece la siguiente definición de amenaza: "Todas las acciones, reales o percibidas, provocadas consciente o inconscientemente, por un eventual adversario a quien se le supone la intención y capacidad para afectar negativamente los intereses propios, en el corto o largo plazo".

rápido auge de las tecnologías de la información ha cambiado para siempre la forma de ver el mundo.

Complementaria de la tecnología es la narrativa. Lo que se dice es a menudo más importante que cómo se dice. El profesor John Arquilla (2007) se hace cargo al señalar: "Lo que importa, incluso, más que los canales de información... es el tipo de contenido que se transmite...". Por décadas, este concepto de narrativa, se ha plasmado en formas de información pública, diplomacia militar y, recientemente, como comunicación estratégica.

Finalmente, está la importancia de los medios de comunicación. Si antes sólo informaban de acontecimientos recientes, "ahora transmiten las actividades en tiempo real" (Leonhard, 1998, p. 23), en consonancia con la velocidad de las tecnologías emergentes. El poder de los medios de comunicación se ha exacerbado aún más con la llegada de las redes sociales y sus efectos de largo alcance a la hora de ocultar lo real de lo falso.

Así pues, con estos tres componentes necesarios para accionar en las INFOOPS desde una mirada doctrinaria, el debate continúa en cómo su convergencia a lo largo del tiempo "plantea nuevos y complejos desafíos para las operaciones militares" (Carter, 2016, p. 1) y que será necesario observar en el futuro. En esa dirección, la doctrina nacional debiese transitar a textos donde se aborden las tecnologías de manera aislada (posteriormente se hará referencia a las capacidades de INFOOPS). También un texto abocado a la comunicación estratégica, que amplíe la

información pública y que permita tener un marco para desarrollar narrativas que persuadan a las audiencias.

Evolución doctrinaria de las INFOOPS: El caso de los Estados Unidos

La historia está repleta de ejemplos de INFOOPS. Al hacer el recorrido, encontraremos aquéllos en los que la tecnología, narrativa y medios de comunicación desempeñan un papel clave. En la experiencia estadounidense estas tres áreas se repiten una y otra vez.

La Guerra Civil norteamericana marca un momento crucial de su historia para entender las INFOOPS. Por primera vez se percibe el advenimiento e importancia del telégrafo. Como señala John Arquilla (2007, p. 5), "el telégrafo permitió el mando, control y coordinación de enormes ejércitos en vastas zonas".

También tenía sus puntos vulnerables, como su susceptibilidad a ser atacado y cortado. Tal fue la importancia concedida a las líneas telegráficas y el ferrocarril que, en 1864, el general Sherman dispuso de 8.000 soldados para protegerlos de los confederados (Castel, 1992). Fue el telégrafo el medio clave del que se valió el presidente Lincoln para llegar a las masas y dar a conocer su discurso de que la Guerra de Secesión era una guerra contra la esclavitud. Este poderoso mensaje, redactado tras la sangrienta batalla de Antietam, golpeó el corazón de la Confederación y, como tantas otras poderosas narrativas, estuvo "basado en las emociones" (Dempsey, 2018, p. 23).

Con la llegada de la Primera Guerra Mundial, el presidente Wilson

creó el Comité de Información Pública (CIP) bajo la dirección de George Creel, al tiempo que aplicaba una estricta política de censura a la prensa (Daly, 2017). Como lo señalara Creel, esta organización se convirtió en la primera voz de EE.UU. en el país y en el extranjero, con la capacidad de desarrollar películas, medios impresos e imágenes fijas. Con la censura minimizando el accionar de reporteros en el campo de batalla, el CIP trajo la historia a casa y el afianzamiento de narrativas a nivel nacional complementadas con los avances tecnológicos (Creel, 2012).

La Segunda Guerra Mundial y el ataque a Pearl Harbor, en diciembre de 1941, dieron paso para que el presidente Roosevelt creara la Oficina de Información de Guerra (OIG) cuya tarea era asumir las responsabilidades de la narrativa bélica (Congress, S/F). Desde la disolución del CIP, no se había logrado penetrar lo suficiente las audiencias extranjeras o enviar mensajes directamente a la población estadounidense. La OIG trabajó para cambiar esta situación, tratando de continuar la labor que el director del CIP, George Creel, había comenzado con anterioridad para "hacer comprender a nuestro propio pueblo y a todos los demás pueblos las causas que obligaron a Estados Unidos a tomar las armas" (Creel, 2012, p. 5).

Quizás el mayor legado de la OIG fue el establecimiento de los programas de radio de la Voz de América (VoA – *voice of America*) que aún se emiten en todo el mundo. Al mismo tiempo que EE.UU. se esforzaba por contar y compartir su historia con el mundo, las capacidades relacionadas con la información como la guerra electrónica (EW – *electronic warfare*), la criptología (hoy relacionado con

ciberoperaciones) y el engaño o decepción (MILDEC – *military deception*), comienzan a madurar.

La Guerra Fría fue testigo de la continua mejora de las tecnologías y, al mismo tiempo, de un esfuerzo persistente en estrategias de información de Estados Unidos y de la Unión Soviética. La Ley Smith-Mundt de 1948 se convirtió en la base de muchas de las actividades de información de EE.UU. en el extranjero, y sentó las bases para la creación de la Agencia de Información de Estados Unidos (USIA – *United States Information Agency*) (Romano, 2015).

El Ejército norteamericano se enfocó en disuadir la agresión soviética de una eventual guerra nuclear. Los estrategas militares del Pentágono buscaron los mejores métodos para detener su ventaja contrarrestando con ataques asimétricos no nucleares. Además, "la Unión Soviética descansó importantemente de la EW o *radioelectrionyaborba* (combate radio electrónico), amenaza que también debió ser contrarrestada" (Armistead, 2004, p. 21). Fue un período en que comenzaron a surgir las ideas de la planificación basada en efectos.

A lo largo de las décadas, EE.UU. siguió mejorando sus capacidades tecnológicas con computadores (NCO – *network computer operations*), operaciones psicológicas (PSYOP – *psycological operations*), EW, inteligencia de señales (SIGINT – *signal intelligence*), operaciones espaciales, y muchas otras capacidades y sistemas. Aunque gran parte de los conceptos operativos se centraban en lo que se conoció como batalla

aero-terrestre, no podía ignorarse el rol clave de la información y las capacidades relacionadas con ella.

Al final de la Guerra Fría, en 1989, el ejército estadounidense mantenía su superioridad tecnológica y la operación Tormenta del Desierto de 1991, sirvió de laboratorio para lo que se conocería como la "primera guerra de la información" (Campen, 1992, p. 1).

Sin embargo, las acciones ejecutadas por el General Aideed de Somalia, quien manipuló a los medios de comunicación para mantener a las fuerzas estadounidenses, militarmente superiores, en desventaja durante la mayor parte de las operaciones de 1993, es un hito clave para comprender el manejo de la información.

En efecto, con el uso de una cámara de vídeo de $600 dólares, Aideed cambió para siempre la política exterior estadounidense en la región, convirtiéndose en un verdadero guerrero de la información. Sus acciones en Somalia, quizás más que cualquier otra operación militar estadounidense hasta la fecha, demostraron el poder innato de la información.

A partir de entonces, el uso de la información para equiparar el balance del poder fue reconocido al instante y desde los inicios de la década de los 90´ fue establecido en la doctrina norteamericana (Armistead, 2004).

Guerra de la información y guerra de Mando y Control. La transición a las operaciones de información

La siguiente cita es útil para comprender la diferencia entre guerra de la información (IW – *information warfare*) y guerra de mando y control (C2W – *command and control warfare*). La primera surge en 1976, cuando el Dr. Thomas Rona, escribiendo para el Departamento de Defensa, la describió de la siguiente manera:

> Las contramedidas destinadas a degradar el flujo de información del enemigo y, a la inversa, proteger nuestra propia información contra su interrupción o engaño, y la explotación para nuestros propios fines de la inteligencia extraída de los canales de información del enemigo, forman parte de la guerra de la información en el contexto de otras operaciones militares.
>
> De hecho, la maniobra de la guerra de la información puede iniciarse muchos años antes de que comiencen las hostilidades; también puede permanecer oculta por mucho tiempo del adversario. La guerra de la información permea e impacta a toda la estructura militar de los posibles beligerantes. Este impacto abarca desde la definición de la misión, pasando por el desarrollo y despliegue de sistemas de armas, hasta el resultado de los enfrentamientos. (Rona,

1976, p. 63)

En su libro *Force without War*, Barry Blechman y Stephen Kaplan examinaron 215 despliegues de fuerzas norteamericanas entre 1946-1975, cuyo propósito era "influir en las percepciones y comportamiento de líderes de países extranjeros" (Blechman, 1978, p. 5). Esto significaba que fuerzas militares, que tradicionalmente operaban en zonas de conocida conflictividad, se enfrentaban cada vez más a situaciones complejas que no eran precisamente de combate. Muchos militares consideraban que la guerra se perdía a través de los medios de comunicación (Blechman, 1978).

Con una acelerada velocidad de la tecnología y la construcción de narrativas, el Ejército y los medios de comunicación entraron en una especie de "colisión" cuando se acercaba Tormenta del Desierto a principios de 1991. Las acciones de Estados Unidos y sus aliados -explotando el conocimiento y aprovechando la información- "aportaron a la guerra un grado de flexibilidad, sincronización, velocidad y precisión desconocido hasta entonces" (Blechman, 1978, p. ix).

Así, de las lecciones aprendidas desde el final de la Guerra Fría, quizá el resultado más importante fue la valoración que tuvo el manejo de la información. Quedó claro, por tanto, que el contrincante que controlara la mayor cantidad de información, con su respectiva capacidad de manipularla mediante una campaña de influencia, tendría una ventaja considerable. Esto se hizo evidente inmediatamente después

de la caída de la Unión Soviética, cuando se inició la planificación desarrollando una nueva estrategia, estrictamente clasificada, sobre el uso de la información como herramienta enfrentar el conflicto. De hecho, "el primer documento, el TS3600.1 del Departamento de Defensa, se mantuvo como ´*Top Secret*´ durante todo su uso debido a la naturaleza restrictiva de su clasificación" (Armistead, 2004, p. 22).

Aunque esta publicación inició un diálogo sobre la IW en el Departamento de Defensa de EE.UU., su clasificación acabó frenando un intercambio doctrinal más general. Así pues, seguía existiendo la necesidad de una estrategia que se adaptara a estas revoluciones tecnológicas, por lo que nace el nuevo concepto de guerra de mando y control (C2W). Publicado oficialmente como "Memorando de Política 30 del Jefe del Estado Mayor Conjunto (CJCS MOP 30 por su sigla en inglés) ´*Guerra de Mando y Control*´ del 8 de marzo de 1993" (Armistead, 2004, p. 22). Este documento expuso, por primera vez en un formato no clasificado, la interacción de las diferentes capacidades que otorgaban una ventaja en la IW.

La C2W como fue originalmente concebida, contenía los siguientes cinco pilares:

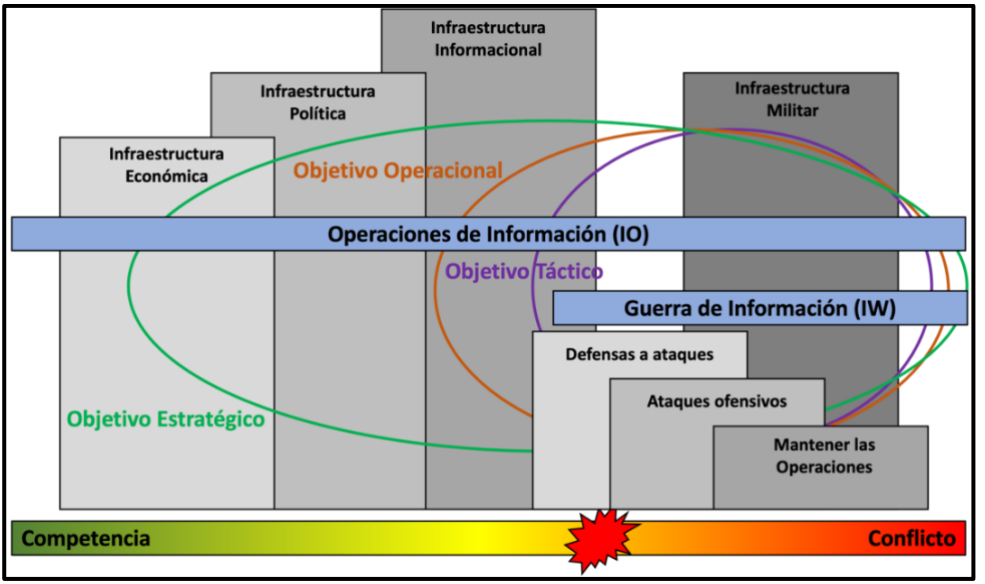
- Destrucción
- Decepción
- Operaciones psicológicas
- Seguridad de las operaciones
- Guerra electrónica

Muchos sectores del Ejército se mostraron reticentes a estos cambios doctrinales. Sin embargo, la capacidad de integrar las diferentes capacidades militares para llevar a cabo análisis nodales contra blancos de mando y control (C2) adversarios, fue elogiado con gran entusiasmo por otros (Armistead, 2004).

Las instituciones de las FAs de EE.UU. desarrollaron células de C2W y comenzaron a entrenarse en esta nueva doctrina a mediados de los noventa. Pero existía un conflicto entre el CJCS MOP 30 y la doctrina TS3600.1 porque la IW era una cuestión más amplia como multiplicador de fuerzas, a diferencia de la C2W que era más restringida al aplicarse sólo a los cinco pilares (Armistead, 2004).

Es por ello por lo que el concepto aún no satisfacía la necesidad de operar en el ambiente de la información, ya que su definición, en esencia era el empleo integrado de las capacidades militares para negar información, influir, degradar o destruir las capacidades de C2 del adversario. Al incluir operaciones ofensivas y defensivas, la C2W ofensiva estaba destinada a atacar el C2 adversario, centrando su accionar en el personal, equipo, comunicaciones e instalaciones de C2. Las defensivas, para proteger los sistemas de C2 propios, negando la eficacia del adversario mediante medidas activas y pasivas (Ortega, 2011). Como se infiere, la C2W estaba relacionada, principalmente, con la afectación de la plataforma tecnológica en el marco de la IW, más no se hacía cargo del ambiente de la información y las capacidades relacionadas que operan en él. Para ilustrar lo señalado previamente, el siguiente gráfico es útil para comprender las diferencias.

Figura 1
Ámbitos de acción de las INFOOPS *y la IW*



Nota: Armistead, L. (2010). Information Operations.

Aunque no del todo satisfactorio, el concepto de C2W dio paso a la creación de nuevas unidades en la mitad de los noventa. Por ejemplo, el Centro Conjunto de Guerra Electrónica de la Base Aérea Kelly en San Antonio, Texas, fue renombrado el año 1993 como Centro Conjunto de Mando y Control y que más tarde, en 1999, sería nombrado Centro Conjunto de Operaciones de Información (Armistead, 2004).

La doctrina siguió desarrollándose tras la publicación del CJCS MOP 30. Así pues, se produjo un impulso concertado para tener una mejor comprensión de los conceptos en el ámbito del Departamento de Defensa de EE.UU. Ello dio paso a la publicación doctrinaria "S3600.1, ´Operaciones de Información´ del 9 de diciembre de 1996" (Kuehl, 2002,

p. 36). El documento buscó aclarar las diferencias con la doctrina anterior y por primera vez introducía el uso de CNO como capacidad de IO. Sin embargo, aún existían vacíos, los que se completaron con la aparición de la publicación doctrinaria, JP 3-13, "Joint Doctrine for Information Operations" del 9 de octubre de 1998 (Kuehl, 2002).

Por primera vez el Departamento de Defensa de EE.UU. publicaba un documento no clasificado para difundir ampliamente los principios doctrinales implicados en la consecución de las INFOOPS. Además de su publicación doctrinaria, debido a que estas campañas de influencia se realizarían mucho antes del inicio de las hostilidades, la Casa Blanca y el Departamento de Defensa se dieron cuenta de que se requería de una mejor coordinación. Fue necesaria una interacción entre las agencias y ministerios gubernamentales para dar un renovado énfasis a esta nueva estructura organizativa de las INFOOPS (Kuehl, 2002).

Finalmente, el siglo XX terminaba con los potentes efectos del internet, que se interconectó a un ritmo sin precedentes en la historia, ganando un espacio individual en la forma de comunicarse. Así se presentaba el mundo al entrar al siglo XXI.

Las operaciones de información y los desafíos para un empleo integral

Aunque el término y los propósitos de las INFOOPS eran nuevos, las cinco capacidades esenciales (los 5 pilares de INFOOPS: EW, CYBEROPS, MISO – Military Information Support Operations –, MILDEC y OPSEC – operations security) tienen una larga historia

propia (Paul, 2008).

En otrora, las preocupaciones estratégicas eran normalmente una cuestión global, pero esa concepción ha cambiado considerablemente. Hoy, numerosos acontecimientos de nivel táctico pueden escalar rápidamente para afectar al área de responsabilidad de un comandante mediante el uso de tecnología avanzada o medios de comunicación masiva como las redes sociales. En efecto, con tecnologías emergentes, incidentes más pequeños pueden desencadenar una situación internacional o estratégica. Asimismo, las nuevas capacidades que han surgido de la unión de la tecnología y la información desafían permanentemente a los elementos del poder nacional, incluidos los factores militares, diplomáticos y económicos (Armistead, 2004).

Ataque a sistemas computacionales, desinformación utilizando redes sociales, la infoxicación en la internet (Duro, 2017) y la amenaza a la infraestructura crítica son una constante en las operaciones militares. El auge de las redes sociales ha exacerbado aún más los efectos de la red, permitiendo la mayor difusión posible de información y desinformación a la velocidad de la luz. Singer y Brooking (2018, p. 18) señalan que "en el transcurso de una década, las redes sociales han cambiado todo. Atacar el centro de gravedad más importante de un adversario -el espíritu de su pueblo- ya no requiere bombardeos masivos ni toneladas de propaganda. Basta con un teléfono inteligente y unos segundos de ocio… y cualquiera puede hacerlo".

Hoy, las INFOOPS buscan desarrollar un conjunto de principios

doctrinales para utilizar y retener el poder de la información. Su objetivo principal es afectar el proceso de toma de decisiones del adversario y, por lo tanto, su esfuerzo principal será accionar sobre esa persona, o grupo de personas, para que haga o deje de hacer una determinada acción (Armistead, 2004). Para influir en el proceso de toma de decisiones del adversario, las INFOOPS utilizan muchas capacidades diferentes, como podría ser la decepción, MISO y EW en un esfuerzo coordinado y sincronizado, a lo largo del tiempo, para dar forma e influir en el ambiente de la información. Todo lo anterior, apoyado con operaciones de cooperación civil-militar (CIMIC – civil military cooperation) y la comunicación estratégica.

Ahora bien, ¿cuáles son los desafíos para un empleo integral?

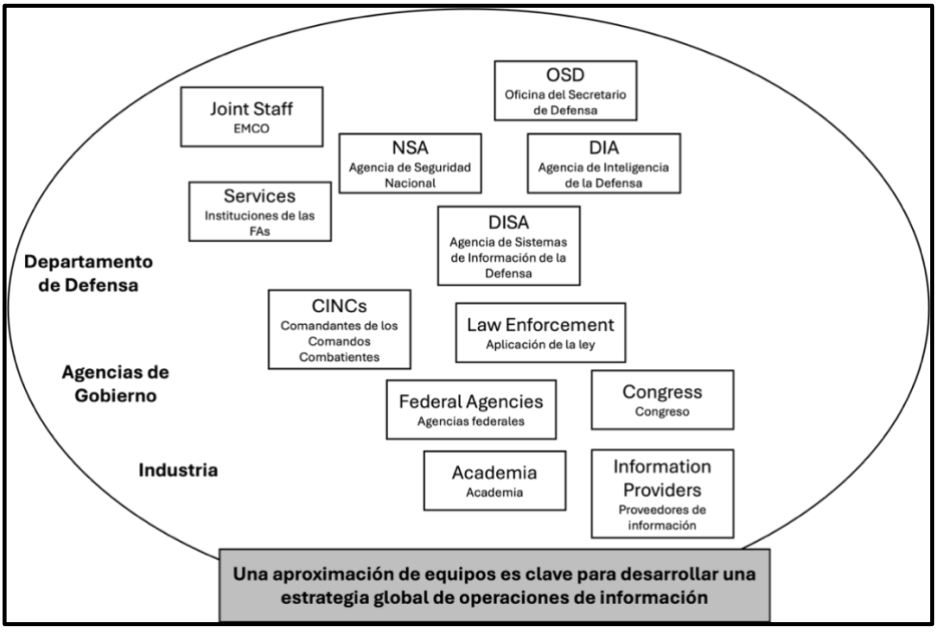
Países referentes de la OTAN y particularmente EE.UU. tienen una sólida experiencia al respecto. Por lo tanto, para dar respuesta a esta pregunta, nuevamente la doctrina norteamericana es pertinente de revisar, para luego reflexionar respecto algunos desafíos doctrinarios que tendría Chile, en términos de INFOOPS.

Por definición, las INFOOPS suelen separarse en ofensivas y defensivas para comprender mejor la relación entre las distintas capacidades y sus actividades interrelacionadas. La mayoría de las capacidades ofensivas de las INFOOPS, en el caso de EE.UU., son empleadas por el Departamento de Defensa, el Departamento de Estado, la Agencia Central de Inteligencia (CIA) y la Casa Blanca. Aunque estas organizaciones no controlan todas las capacidades ofensivas de las INFOOPS que conduce el Gobierno de EE.UU., en general tienden a ser

responsables de la gran mayoría de ellas. Sin embargo, no sucede lo mismo en la arquitectura defensiva de las INFOOPS, porque estas capacidades tienden a estar mucho más diseminadas entre agencias o ministerios. En efecto, es factible afirmar que cada organización es responsable, en última instancia, de maximizar su propia estructura defensiva, ya sea en forma de seguridad de la información, protección de la fuerza o seguridad de las operaciones (Armistead, 2004).

Figura 2

Colaboradores de Operaciones de Información



Nota: Armisted, L.(2010). Information Operations.

Como se puede visualizar en la figura 2, la arquitectura general de las INFOOPS en el gobierno de los EE.UU. no es sencilla ni fácil de entender. Sin embargo, las relaciones han evolucionado a lo largo de los

años. Muchas organizaciones que fueron creadas originalmente para llevar a cabo determinadas tareas hoy generan cooperación entre agencias. Por ejemplo, el Secretario de Defensa del Presidente Clinton inició un esfuerzo para mejorar las relaciones en el Departamento de Defensa respecto a INFOOPS. De esta manera, desarrollaron, en conjunto con otras agencias, una arquitectura organizativa más coherente. Del mismo modo, la administración Bush también introdujo cambios, al crear el Departamento de Seguridad Nacional (Homeland Security Department - HSD) y una serie de reorganizaciones que fueron intentos evidentes para cambiar la estructura del gobierno estadounidense por una arquitectura más acorde con la era y los desafíos de la información (Armistead, 2004).

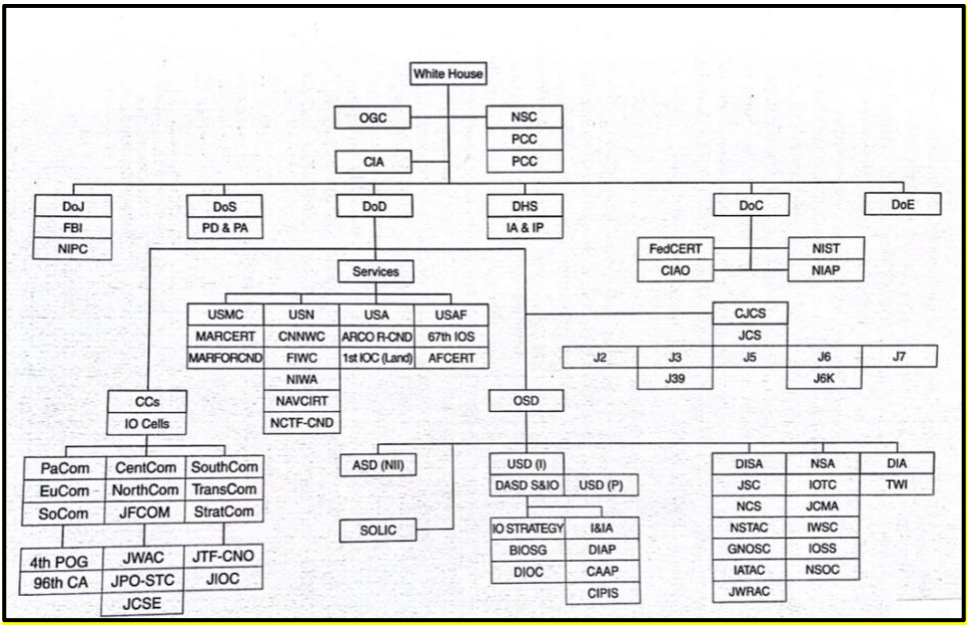
Un aspecto relevante por mencionar desde la perspectiva de los desafíos de integración es que, en el caso de EE.UU., las INFOOPS son lideradas por el poder político, siendo el presidente de los Estados Unidos quien aprueba la directiva de este tipo de operaciones, y junto al Secretario de Defensa conforman la Autoridad Nacional de Mando (Armistead, 2004). Al igual que en Chile, la guerra declarada debe ser autorizada por el Congreso Nacional. Por lo tanto, es interesante apuntar que, en relación con las INFOOPS, al ser iniciadas mucho antes de las hostilidades, el proceso de aprobación proviene desde lo más alto de la cadena de mando, en este caso, desde el presidente.

Finalmente, el gráfico que se presenta a continuación da cuenta de la relación que tienen las diferentes organizaciones y agencias del gobierno de EE.UU. respecto a las operaciones de información, lo que nos lleva a

reflexionar de los desafíos para nuestra propia realidad nacional. Con ello, damos paso a la parte final de este capítulo, donde se proponen las necesidades doctrinarias en Chile.

Figura 3

Organizaciones relacionadas con las Operaciones de Información en EE.UU.



Nota: Armisted, L. (2010). Information Operations.

Reflexiones finales: Los desafíos doctrinarios para el Ejército de Chile

La experiencia de países referentes, especialmente de los EE.UU., que es uno de los más desarrollados en el ámbito de las INFOOPS, permiten reflexionar acerca de la importancia doctrinaria y los desafíos para Chile. En tal sentido, será importante señalar que la doctrina del

Ejército de Chile proviene de diferentes vertientes, cuya larga explicación no es objeto de este capítulo. Sin embargo, para dar un contexto, es importante señalar que una de ellas son las experiencias militares que remiten las unidades del Ejército, y otra, es la revisión doctrinaria de los países referentes, principalmente de los EE.UU., Inglaterra, España y Alemania.

Nuestro actual reglamento de operaciones de información, el RDO-20909, data del año 2010, y es una adaptación de las 5 capacidades iniciales de la C2W de los norteamericanos. Por tal razón, durante el año 2024, se inició la actualización del texto doctrinario, siendo liderado este trabajo por la Academia de Guerra del Ejército (ACAGUE), con los aportes de fuentes de países referentes[4]. Esta actualización busca ampliar el concepto de C2W hacia el de operaciones de información, en el marco de la maniobra en el ambiente de la información, todo esto a través de las capacidades esenciales y relacionadas con ella.

La Dirección de Operaciones del Ejército de Chile, es quien lidera el tema relacionado al desarrollo institucional de las INFOOPS, llevando adelante uno de los desafíos visualizados, cual es el de continuar con un esfuerzo conjunto de trabajo entre la DOE, la ACAGUE y la División Doctrina, para establecer un paraguas que, desde la perspectiva doctrinaria, se pueda desarrollar y logre sincronizar a este tipo de

[4] Durante el año 2024, la Academia de Guerra contó con alumnos extranjeros provenientes de EE.UU., España y Alemania, quienes aportaron a la actualización del RDO-20909.

operaciones de forma transversal en la Institución.

A partir de la evolución doctrinaria requerida y la realidad actual de distintos entornos operativos que podría enfrentar el Ejército de Chile, los principales desafíos doctrinarios a enfrentar son los que a continuación se detallan:

- Concretar la actualización del RDO-20909 "OPERACIONES DE INFORMACIÓN", el cual está en vías de realizarse.
- Robustecer el cuerpo doctrinario relacionado con OPSEC, MILDEC, CIBEROPS y EW.
- Asimismo, los reglamentos de CDef (Ciber Defensa) y de EW, que también se estructuran en base a las capacidades esenciales de la C2W.
- Por su parte, el MDO-90903 "ENMASCARAMIENTO, OCULTACIÓN Y DECEPCIÓN", debería ser actualizado en su contenido hacia el concepto de "decepción militar", como una de las capacidades esenciales de las INFOOPS que permiten accionar en el ambiente de la información.
- Con los ajustes anteriores, se debería desarrollar manuales y cartillas que operacionalicen tácticas, técnicas y procedimientos específicas para cada una de las capacidades esenciales.
- Como una forma de cerrar el ciclo completo, se debiera actualizar los textos doctrinarios de las capacidades relacionadas de Asuntos Civiles y Administración Territorial (ACAT) y el de Información Pública. Ambos deberían transitar hacia contenidos más amplios y relacionados con las INFOOPS. Por ejemplo, ACAT, podría

evolucionar al concepto de CIMIC y el de información pública, quedar plasmado en un texto de comunicaciones estratégicas, donde se explique la relación y desarrollo de narrativas y mensajes para direccionar a las audiencias y al público objetivo de las INFOOPS.

Los medios de comunicación enfrentan retos y presiones, ya que el auge de blogueros, bots y trolls, que intentan confundir lo real de lo falso, influye enormemente en la opinión de escritores, periodistas y en el ciudadano o público en general. Por lo tanto, nunca había sido mayor el nexo existente entre la guerra y la información.

Con el mundo en este estado, el Comando Cibernético del Ejército de los Estados Unidos es una buena aproximación doctrinaria para nuestra realidad, para hacer frente a las amenazas actuales y emergentes. Aunque el anuncio del Teniente General Fogarty, del 14 de marzo de 2019, solo identificaba las capacidades de la guerra cibernética y electrónica (EW), y su sincronización a través de las IO, es una excelente aproximación para enfrentar los desafíos de la maniobra en el ambiente de la información, estableciendo sólidas narrativas, comprometiendo los medios de comunicación y emplear las tecnologías de las capacidades esenciales en beneficio propio.

Referencias Bibliográficas

Armistead, L. (2004). *Information Operations: Warfare and the Hard Reality of Soft Power.* Brassey's.

Arquilla, J. (2007). *Information Warfare and Strategy.* Routledge.

Barry Blechman, S. K. (s.f.). *Force without War*. The Brooking Institution.

Campen, A. (1992). *Information, Truth, and War in the First Information War*. AFCEA International Press.

Carter, A. (2016). *Strategy for Operations in the Information Environment*. Obtenido de Department of Defense: https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

Castel, A. (1992). *Decision in the West: The Atlanta Campaign of 1864.* University of Kansas Press.

Creel, G. (2012). *How We Advertised America.* Forgotten Books.

Daly, C. (2017). *How Woodrow Wilson's Propaganda Machine Changed American Journalism*. Obtenido de Smithsonian Magazine: https://www.smithsonianmag.com/history/how-woodrow-wilsons-propaganda-machine-changed-american-journalism-180963082/

David Alberts, J. G. (s.f.). *Understanding Information Age Warefare.* Command and Control Research Program.

Duro, S. (2017). *¿Qué es la infoxicación digital y cómo puedes evitarla?* Obtenido de Webempresa: https://www.webempresa.com/blog/que-es-infoxicacion.html

Kuehl, D. (2002). *Information Operations, Information Warfare and Computer Network Attack: Their Relationship to National Security in the Information Age.* Obtenido de Int. Law Studies: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context

Leonhard, R. (1998). *The Principles of War for the Information Age.* Presidio Press.

Library of Congress. (2024). *Office of War Information*. Obtenido de Library of Congress: Research Guides: https://guides.loc.gov/rosie-the-riveter/office-of-war-information

Martin Dempsey, O. B. (2018). *Radical Inclusion.* Missionday Books.

National Geographic. (2023). *¿Es real la historia del caballo de Troya?* Obtenido de National Geographic: https://www.nationalgeographicla.com/historia/2023/01/es-real-la-historia-del-caballo-de-troya

Ortega, R. (Mayo-Junio de 2011). *La guerra asimétrica y las operaciones de información*. Military Review.

Paul, C. (2008). *Information Operations: Doctrine and Practice (First Edition).* Praeger Security International.

Romano, S. (2015). *La guerra psicológica como guerra permanente: Estados Unidos en América Latina*. Obtenido de Voces en el Fénix: https://vocesenelfenix.economicas.uba.ar/la-guerra-psicologica-como-guerra-permanente-estados-unidos-en-america-latina/#:~:text=Esto%20fue%20promovido%20con%20la,la%20gente%20de%20otros%20pueblos%E2%80%9D

Rona, T. (1976). *Weapon Systems and Information War. Office of Net Assessment.* Obtenido de Department of Defense: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf

Singer, P.W. (2018). *Like War: The Weaponization of Social Media.* Houghton Mifflin Harcourt.

Underwood, K. (2019). *Army Cyber to Become an Information Warfare Command. Signal.* Obtenido de AFCEA: https://www.afcea.org/signal-media/technet-augusta-22-coverage/army-cyber-become-information-warfare-command

Wade, N. (2021). *INFO21 SMARTBOOK: Information Operations & Capabilities.* The Lightning Press.

CAPÍTULO 4

Las Operaciones de Información en el conflicto actual

Teniente Coronel Cristian Retamal Valenzuela[1]

Introducción

La evolución del carácter de la guerra nos obliga a mantener un constante monitoreo sobre los distintos eventos que afectan el devenir de los conflictos armados. Es así como nacen distintas clasificaciones y tipologías de la guerra que ayudan a comprender este fenómeno político y social de gran complejidad. Claramente la evolución de la sociedad y la tecnología afectan la forma de hacer la guerra, es decir, la estrategia misma, por lo cual uno de los grandes desafíos es identificar las tendencias e incluso anticiparse a los impulsores que afecten el campo de batalla futuro.

Hoy, uno de los impulsores del ambiente operacional futuro (AOF) es la disputa por la dimensión cognitiva. Asimismo, otras formas de conflicto son la guerra irrestricta y el conflicto en la zona gris. De igual manera, un nuevo empleo de la fuerza contempla la ejecución de operaciones de información junto a un amplio espectro de operaciones

[1] Teniente coronel del Ejército de Chile. Oficial de Estado Mayor del Ejército de Chile y del Ejército de Estados Unidos de América. Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica, Academia de Guerra del Ejército de Chile. Máster en Estudios Operacionales, Command and General Staff College Ejército de Estados Unidos de América. Actualmente, es profesor de la ACAGUE. ✉ cristian.retamal@acague.cl.

que consideran la integración de medios militares y no militares en un esfuerzo interagencial desde el más alto nivel.

No obstante, este tipo de operaciones en su esencia no son una novedad. Pudimos observar en el capítulo 1 la aplicación de las INFOOPSs en operaciones realizadas hace más de 70 años. Cabe preguntarse entonces, ¿qué diferencia existe entre las acciones realizadas en las guerras pasadas orientadas a afectar la dimensión cognitiva del adversario respecto de la actualidad? ¿Por qué hoy pareciera tener un rol más significativo en el desarrollo de las operaciones militares? El engaño ha sido parte del arte de la guerra desde tiempos de Aníbal, sin embargo, existen ciertas consideraciones sociales y tecnológicas que hoy, más que nunca, hacen que las INFOOPSs sean más efectivas e influyentes en el desarrollo de los conflictos actuales.

De esta forma se estima que, en la actualidad, los impactos de las operaciones de información en la guerra actual son decisivos, producto del incremento de la valorización de la información como fuente de poder y debido a las características propias de la sociedad post moderna.

En efecto, este capítulo tiene como propósito explicar las razones del éxito y la preponderancia que tiene el desarrollo de operaciones de información en el conflicto actual, para lo cual nos basaremos en algunos ejemplos aplicados de Rusia y China, países que han sido referentes en el uso de este modo de emplear medios militares y no militares en un esfuerzo sincronizado desde el más alto nivel de la conducción.

Para lo anterior, en una primera parte, se analizará el valor intrínseco de la información en el más amplio espectro del conflicto desde una perspectiva económica, doctrinaria y relacionada con el poder. En segundo término, se abordarán las características e impactos de la postmodernidad basados en los postulados de Jean-François Lyotard, el concepto de ambigüedad y las particularidades de las generaciones más influyentes de esta era. Finalmente, se efectuará una síntesis del fenómeno considerando la identificación central del problema y proponiendo alguna posible solución.

En efecto, el actual ambiente estratégico caracterizado por las particularidades de la sociedad postmoderna, en un entorno de revolución industrial de las TICs, y de generaciones marcadamente influidas por ella, sumado a la gran importancia que hoy en día posee la información en las operaciones militares, han generado las condiciones ideales para poder ejercer una influencia decisiva en la dimensión cognitiva desde una perspectiva trinitaria del conflicto. No obstante, lo anterior, el desarrollo del pensamiento estratégico, basado en la aplicación del pensamiento crítico sustentado en la filosofía del conflicto y el pensamiento creativo en el arte de la guerra, podrán ser una solución factible a tan complejo escenario.

Marco teórico

Antes de adentrarse en las razones particulares que sustentan la tesis del presente capítulo, se estima pertinente establecer un marco teórico conceptual y temporal que nos permita enfocar la discusión sobre las INFOOPS tomando como referencia dos conceptos centrales que se

analizarán: la seguridad, la información y el conflicto actual.

El concepto de seguridad posee una amplia gama de acepciones y está presente en diversos textos doctrinarios de la comunidad de defensa de muchos países referentes. Sin embargo, es fundamental comprender que todo concepto con mucha historia y uso extensivo tendrá múltiples interpretaciones. Por lo mismo, se considerará la definición de seguridad de Giovanni Manunta (1999), en su publicación "What is security?".

El autor deja en claro la necesidad de comprender el concepto de seguridad de forma operativa para superar los diferentes contextos y utilizarlo para saber atribuir responsabilidades y cargas institucionales a los actores públicos para resguardar los intereses de una sociedad sin sacrificar las libertades ciudadanas o la soberanía de los Estados. (Manunta, 1999)

En este sentido, la seguridad (operacional) es un constructor dinámico que permite coordinar elementos identificables superando las intenciones o intereses posibles cuando hay vulneración a la seguridad. El autor lo presenta con el siguiente esquema. [S= f (A, P, T) Si] entendiendo S: seguridad; f: en función de; A: asset, el activo a proteger; P: protector, qué o quién cuidará al activo; T: Threat, la amenaza; y todos estos elementos en una Si: "a given Situation", o situación dada, un contexto específico. Si alguno de estos elementos deja de estar presente, no podemos estar hablando de seguridad. Si no existe un activo específico, qué se va a proteger, si no hay amenaza, que justifica protegerlo y sin un protector, no existe esfuerzo para salvaguardar al

activo. Para el autor, todos estos elementos deben estar presentes para poder hablar de seguridad y adicionalmente, la interacción de estos se da en una situación específica. Sin un contexto definido, cuándo, cómo, por qué, no podremos hablar de seguridad (Manunta, 1999).

Sin distinción de un contexto y todos los elementos que constituyen la seguridad, el uso de los instrumentos que dispone el Estado puede darse en mal uso e incluso oponerse a la responsabilidad primordial que tiene con sus ciudadanos, protegerlos (Manunta, 1999).

En segundo lugar, Hernández (2014) desarrolla el concepto de información analizado por Floridi, destacando que ésta es un concepto elusivo, primitivo, pero casi omnipresente. Su definición puede ser abordada desde tres perspectivas:

- La información **como** realidad (lo que es la información): como patrones de señales físicas independientes del significado y de la verdad.
- La información **sobre** la realidad (de qué habla el contenido informacional): posee contenido semántico y se puede calificar de tener carácter alético.
- La información **para** (actuar sobre/en) la realidad: podemos hablar de instrucciones, algoritmos, información genética para la codificación de aminoácidos, etc.

Para efectos del presente capítulo será de suma importancia el enfoque aludido por Floridi en su primera acepción, la información como

realidad. En este sentido podemos apreciar que la naturaleza y esencia del concepto se encuentra muy ligada a la dimensión cognitiva del ser humano.

Bajo otra perspectiva, la información es un concepto inserto en el contexto de la "toma de decisiones", particularmente en una actividad fundamental del comandante como lo es "la comprensión situacional". Según el Departamento del Ejército de EE.UU. (2019), la comprensión se logra mediante el procesamiento de data, información y conocimiento. En dicho contexto la información es definida como "datos que se han organizado y procesado con el fin de proporcionar un contexto para un análisis posterior".

Asimismo, existe el concepto occidental del ambiente de la información como parte del ambiente operacional cuya definición considera que es el conjunto de individuos, organizaciones y sistemas que obtienen, procesan, difunden y explotan esa información. Se compone de tres dimensiones interrelacionadas: involucra aspectos físicos, informáticos y cognitivos (Ministerio de Defensa Nacional, 2023, p.16).

Por su parte, el segundo concepto central a analizar se refiere a la definición de "conflicto actual". Para el presente capítulo, se considerará la definición teórica del conflicto continuo (contemplada tanto en la doctrina nacional conjunta como en la de la OTAN) y, a la vez, la perspectiva china y rusa de la guerra irrestricta y el conflicto en la zona gris, respectivamente. Ahora bien, temporalmente se considerarán como

conflictos actuales aquellos sucedidos durante el presente siglo a partir del inicio del fenómeno denominado “Primavera Árabe”.

Incremento de la valorización de la información como fuente de poder

La información como insumo para de la toma de decisiones siempre ha sido importante a lo largo de la historia militar, sin embargo, los alcances de las operaciones de información en la guerra actual han marcado una significativa diferencia posterior a la era moderna. Uno de los argumentos principales que sustentan esta parte de la tesis expuesta es el incremento de la valorización de la información como fuente de poder, la cual se podrá demostrar con evidencia histórica, primero, producto del incremento sustancial del valor de la información como instrumento de transacción en la economía mundial, segundo, respecto a la evolución de la información en el ámbito de la seguridad y defensa durante el siglo XXI y tercero, como fuente de poder.

Incremento sustancial del valor de las empresas que gestionan información

Hoy en día la información es un bien cada vez más preciado en el contexto de la economía mundial. Con un mundo globalizado e interconectado en sofisticadas plataformas tecnológicas, la información durante el presente siglo ha incrementado ostensiblemente su papel en la cadena de valor.

Según INVERSIS (2022), el “dato” -que ya definimos como el insumo básico de la información- está transformando al mundo,

comenzando a identificarse como el nuevo "oro" del siglo XXI o como parte de una nueva revolución industrial, lo que devela el alto valor intrínseco que significa que uno de los principales bancos de España emita esta declaración.

En el mismo sentido, según Nurton (2022), el Director General de la Organización Mundial de la Propiedad Intelectual "OMPI", el Sr. Daren Tang, afirmó que ***si la digitalización es el motor de la economía del futuro, los datos son su combustible***, destacando además que en un mundo interconectado, es esencial comprender la naturaleza y el valor de los datos. Lo anterior, reafirma que la información, cuyo significado se relaciona al procesamiento de data, cobra un especial valor en la estructura de la economía digital.

Asimismo, el Informe sobre la Economía Digital de 2019 emitido por la Comisión de Naciones Unidas sobre Comercio y Desarrollo "UNCTAD", afirma que ésta "sigue evolucionando a una velocidad vertiginosa, impulsada por la capacidad para recopilar, utilizar y analizar un volumen masivo de información que las máquinas puedan asimilar (datos digitales) sobre prácticamente cualquier cosa" (Conferencia de las Naciones Unidas para el Comercio y Desarrollo [UNCTAD], 2019, p.1). De igual forma, señala que ha surgido una "cadena de valor de los datos", vinculando el origen de la recopilación de éstos en calidad de "datos brutos", con la obtención de inteligencia digital, logrando así monetizar el producto final con fines comerciales.

En razón a las empresas que gestionan información, Carrière-

Swallow y Haksar (2019) en el foro del Fondo Monetario Internacional (FMI), establecen que los datos son un insumo crítico en la economía global junto con el capital, la mano de obra, la tierra y el petróleo, los cuales proveen la materia prima para la generación de algoritmos de la inteligencia artificial.

En el mismo informe sobre economía digital, pero en su versión 2021, UNCTAD señala que el valor de los mercados de datos ha aumentado de forma sustancial desde el 2016 en todas las economías analizadas en dicho documento. Lo anterior, ha sido evaluado por el mundo de la inversión, generándose un incremento de los precios en las acciones de las plataformas digitales, cuya labor principal es la recopilación y procesamiento de datos.

Como antecedente a considerar, según UNCTAD (2021), luego de la abrupta caída de las bolsas internacionales a principios del 2020 producto de la pandemia del COVID-19, la recuperación fue, comparativamente superior para las plataformas digitales globales respecto del índice compuesto de la Bolsa de Nueva York. De esta forma, "entre el 1 de octubre de 2019 y el 21 de enero de 2021, el índice compuesto de la Bolsa de Nueva York aumentó un 17 %. En el mismo período, las tasas de crecimiento del precio de las acciones de las empresas seleccionadas fueron al menos 3 veces mayores: Facebook (55 %), Alphabet (incluido Google, 56 %), Alibaba (57 %), Microsoft (64 %), Amazon (90 %), Tencent (113 %), Apple (144 %) y Baidu (147 %)" (UNCTAD, 2021, p.27). Lo anterior, tuvo como consecuencia cambios considerables en la capitalización bursátil de dichas empresas,

demostrando con ello, la mayor valorización de los datos e información dentro de la cadena de valor que conforma la inteligencia digital.

Evolución de la información en el ámbito de la seguridad y defensa durante el siglo XXI

Una vez apreciado el incremento sustancial del valor de la información, podemos identificar su evolución en el ámbito de la seguridad y defensa durante el siglo XXI, bajo una perspectiva estructural, doctrinaria y de explotación.

En cuanto a lo estructural, las mayores potencias mundiales de occidente agrupadas en la OTAN, así como Rusia y China, han implementado una serie de políticas y organizaciones que han abordado como tema central la "información". Transversalmente, es importante destacar que ésta constituye uno de los elementos del poder nacional más influyentes del siglo XXI. Tal como lo menciona Liaropoulus (2022), es natural que la información desempeñe un papel central en cualquier tipo de confrontación sociopolítica en función a una era altamente impactada por las TICs, donde los Estados también deben tener en consideración la dimensión cognitiva del conflicto y la guerra de las narrativas.

Respecto a la OTAN, se destaca la creación del "Centro de Excelencia de Comunicaciones Estratégicas", con sede en Riga, Letonia, a partir del 2014, el cual genera conocimiento relevante respecto de las comunicaciones estratégicas asociadas a diversas áreas tales como la diplomacia, asuntos públicos, operaciones de información y operaciones psicológicas, entre otras. Asimismo, el Laboratorio de Investigación

Forense Digital (DFRLab) del Atlantic Council fundado el 2016, es la primera organización de su tipo con experiencia técnica y política en desinformación, tecnologías de conectividad, democracia y el futuro de los derechos digitales.

Por su parte, según Hakala y Melnychuk (2021), en octubre de 2019, entró en vigor la ley "internet soberana" en la Federación Rusa, que permite al gobierno desconectarse de la internet global a su discreción, permitiendo con ello que sólo el 10% del tráfico de internet ruso se enrute a través de servidores extranjeros para 2024. En tal sentido, "el Kremlin considera que el control sobre su espacio de información interno es esencial para su seguridad: una amenaza al espacio de información podría percibirse como una amenaza a la soberanía del Estado" (Hakala y Melnychuk, 2021 p.12). Se suma a lo anterior, la creación de una nueva unidad estructural en el Ministerio de Asuntos Exteriores de la Federación de Rusia (Departamento de Seguridad de la Información Internacional). Según los autores Krutskikh, Zinovieva, Bulva, Alborova & Yudina (2021), una característica relevante de este organismo es su naturaleza multisectorial, tomando en cuenta aspectos de seguridad de las TICs a través del prisma del derecho internacional, sus consideraciones políticas, militares y económicas, y las direcciones regionales y globales de las relaciones exteriores en función a la política de la Federación de Rusia.

De igual forma, China ha publicado una nueva ley de protección de información personal a partir de noviembre del 2021, la cual regula todo tipo gestión de datos cuyos alcances han sido analizados de manera

preocupante por organizaciones occidentales. Tal como lo mencionan Brussee y Von Carnap (2024), la disponibilidad en línea de información trascendental de China se encuentra bajo amenaza, considerando que esta potencia asiática ha tenido una tendencia a la "segurización" de muchos ámbitos del poder nacional. Dicho proceso ha sido analizado por el reporte MERICS (2024) bajo dos enfoques: primero, la menor transparencia del gobierno chino difundiendo cada vez menos información; y, segundo, implementando medios tanto regulatorios como técnicos para bloquear el acceso a información potencialmente sensible desde el exterior.

Desde un enfoque doctrinario, en el instrumento militar, el concepto de "comunicaciones estratégicas" ha evolucionado de manera importante, transformándose para la OTAN durante el año 2023, en una nueva función primaria del mando que alberga todas las actividades de información que se planifican y ejecutan dentro de las operaciones militares. En dicho contexto, "las comunicaciones estratégicas militares (STRATCOM) son fundamentales para el éxito de las operaciones de la alianza, contribuyendo a la implementación de la orientación política a través de su dirección estratégica militar y operaciones conjuntas" (Ministerio de Defensa del Reino Unido, 2023, p.xvii). De esta forma, se evidencia que este pacto de seguridad colectiva tiene como prioridad el desarrollo cognitivo del empleo de los medios militares y no militares para influir en el ambiente de la información. Específicamente, según el Ministerio de Defensa del Reino Unido (2023), la nueva función J-10 "STRATCOM" permite a un comandante comprender a las audiencias y

dar forma continua al entorno de información en apoyo a las operaciones militares, abarcando cuatro disciplinas: 1) Comunicación Estratégica, 2) Operaciones de Información (INFOOPS), 3) Asuntos Públicos Militares (MIL PA), y 4) Operaciones Psicológicas (PSYOPS).

Respecto a las mismas "Operaciones de Información" y reforzando el marco teórico inicial establecido, cabe destacar que la OTAN -a través de sus países miembros- ha publicado y mantenido en una constante actualización, diversos textos doctrinarios en donde el concepto de "información" se encuentra presente bajo distintos enfoques. Según el Ministerio de Defensa del Reino Unido (2023) encontramos a la información como:

- **Instrumento del poder nacional**, el cual reconoce la prevalencia de la era de la información, la creciente importancia del entorno de información, el enfoque centrado en el comportamiento y su papel para influir en los tomadores de decisiones. Su esencia se encuentra en la narrativa, que orienta las operaciones y por la cual siempre se debe competir.
- **Función conjunta**, la cual es fundamental para la toma de decisiones y la manera en que se informa e influye a las audiencias. Su tarea principal es planificar y sincronizar el empleo de operaciones psicológicas, asuntos públicos militares, guerra electrónica y ciberoperaciones, entre otras, las cuales deben coordinarse e integrarse durante todo el proceso de las operaciones, siendo coherentes con la narrativa dispuesta.

- **Función de asesoría de EM (INFOOPS)**, la cual coordina e integra la dirección y guía de la función primaria "Comunicaciones Estratégicas" horizontalmente dentro de cada cuartel general militar de la OTAN. Esta función conduce a la comprensión de las audiencias, a través de la evaluación del ambiente de información, para identificar los efectos cognitivos dentro de las audiencias, que se planificarán como actividades de información y se coordinarán con el proceso de targeting conjunto.
- **Actividad de información**, la cual puede ser realizada por cualquier capacidad o medio, enfocada a crear efectos cognitivos en una audiencia determinada.
- **Ambiente de la información**, el cual se define como un entorno compuesto por la información misma, los individuos, organizaciones y sistemas que reciben, procesan y transmiten la información, y el espacio cognitivo, virtual y físico en el que esto ocurre.
- **Parte de la jerarquía cognitiva y relación entre datos, información, conocimiento y comprensión**, el cual sitúa la información desde su nivel más bajo (datos) hasta el más alto (comprensión), este último necesario para que los comandantes puedan tomar las mejores decisiones y materializar el control de las operaciones de manera efectiva.

Por otra parte, una potencia referente en la explotación del ambiente de la información es Rusia, cuya doctrina constituye un enriquecido marco conceptual que muchos centros de investigación occidentales se

esfuerzan por analizar y comparar. De esta forma, Hakala y Melnychukse (2021) analizan conceptos doctrinarios generales rusos como la "confrontación de información", la cual alberga la "guerra informática-tecnológica" cuyo homólogo occidental sería la ciberguerra. Esta confrontación implica una dimensión psicológica significativa de efectos cognitivos en los tomadores de decisiones adversarios y población civil en general. En efecto, uno de los medios para lograr esta superioridad en el ambiente de la información es la guerra informática-tecnológica.

Dentro de las mismas comparaciones efectuadas por Hakala y Melnychukse (2021), se evidencia un enfoque más integral respecto a la conceptualización rusa de lo que en OTAN se define como ciberespacio como parte del ambiente operacional. Es así como la doctrina rusa establece el concepto de "espacio de información" o "esfera de información", la cual se refiere a actividades para formarla, transformarla y almacenarla, así como influir en la conciencia individual y pública, la infraestructura de la información y la información misma.

Por su parte, se destaca que en la doctrina rusa se ha desarrollado un concepto de "armas de información" (no existente ni homologado en la OTAN), el cual considera más allá de los medios digitales. En términos prácticos dicho concepto cubre una amplia gama de actividades, principalmente enfocadas en influir en la dimensión cognitiva del soldado y población civil, incluyendo la difusión de desinformación, la guerra electrónica, la degradación de sistemas de navegación, las operaciones psicológicas y la destrucción de las capacidades informáticas del adversario.

Otra forma de resaltar la importancia que tiene algún concepto es el interés de los mandos militares en escribir sobre ello. Es así como en el año 2013, el Jefe del Estado Mayor General ruso, general Valeri Gerasimov, efectúa una profundo análisis de los desafíos para la defensa, derivado de fenómenos sociales asociados a la "Revolución de Colores", "Primavera Árabe" y movimiento de "Maidán", que, a su juicio, afectaron la seguridad nacional rusa, destacando que el papel de los métodos no militares para lograr objetivos políticos y estratégicos ha aumentado significativamente en razón al poder de las armas con efectos letales. Análisis posteriores de los dichos de Gerasimov señalan que "la guerra ahora se lleva a cabo en una proporción cerca de 4:1 de medidas no militares y militares" (Bartles, 2016, p.61), haciendo hincapié en una supremacía cuantitativa respecto a esta forma de hacer la guerra.

El poder de la información

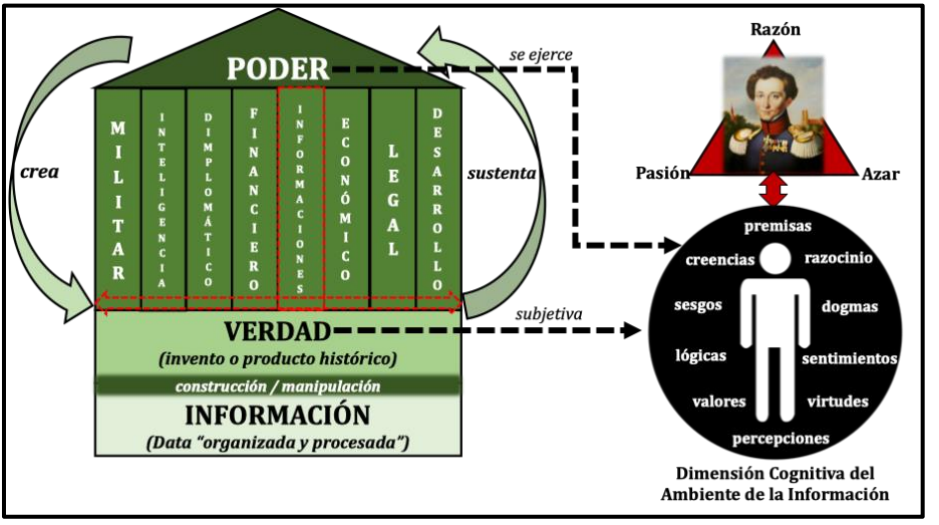
Basado en los postulados de Michel Foucault la información es la base fundamental para la construcción de la verdad, y sobre ésta, el ejercicio del verdadero poder. Según Vásquez (2011), Foucault define el poder como "la capacidad que tiene un determinado sujeto de imponer su verdad, como la verdad para el otro". Cabe destacar que el sustantivo "sujeto" podría ser reemplazado por "actor", como parte de las dinámicas e interacciones presentes en el Sistema Internacional. De esta forma, uno de los objetivos del poder sería, justamente, crear una verdad, la cual forje la realidad que sea socialmente asumida por la población afectada por el ejercicio del poder.

Ahora bien, la pregunta clave sería cómo poner en práctica dicha acción de influencia, ya que una de las conclusiones más relevantes de Foucault respecto al poder es que éste se "ejerce" en vez de ser adquirido o incluso traspasado (observando el poder como un bien desde una perspectiva económica). Así pues, Vásquez (2012) señala que Foucault desarrolla herramientas metodológicas que permiten comprender la historia de los discursos a base del concepto de "genealogía", conformando subjetividad en la construcción de esta verdad.

Foucault, tomando como referencia a Nietzsche, cuestiona la esencia objetiva de la verdad, a través de la construcción de la historia por medio del discurso. De esta manera, el ejercicio del poder se centra en la competencia y supremacía por el establecimiento de la verdad en una dialéctica de voluntades, utilizando todos los medios necesarios para influir en la dimensión cognitiva del sujeto afectado por el ejercicio del poder.

Figura 1

Influencia de los elementos del poder nacional en la dimensión cognitiva del ambiente de la información



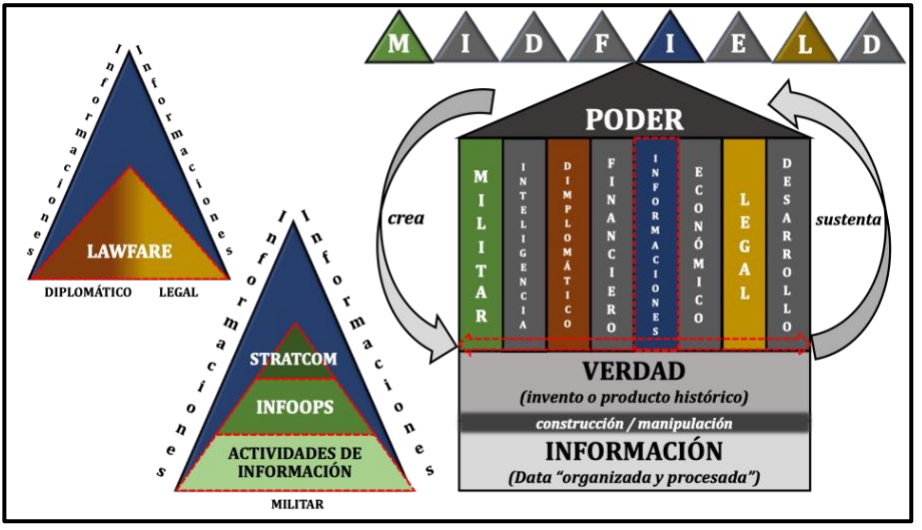
Nota: Elaboración propia

En la figura 1 se aprecia la conexión existente entre la información y el poder, cuya finalidad, en el contexto de la naturaleza de la guerra, es influir dentro de la dimensión cognitiva del oponente tomando como referencia la teoría de Clausewitz. Así, el análisis de la figura muestra de abajo hacia arriba inicialmente los "datos", los cuales constituyen la materia prima de la información, transformándose en el elemento esencial para la construcción de la verdad. Tomando en consideración los postulados de Foucault, la acción de "construcción de una verdad" y su imposición sobre otras, devela la esencia misma del poder. En este sentido, la gestión de los datos e información para dicha construcción podría formar parte de lo que se conoce como manipulación de la

información. Esta verdad sustenta los diferentes ámbitos del poder, los cuales desde la perspectiva del Estado y dada la doctrina estadounidense, obedecen al acrónimo en inglés "MIDFIELD" (militar, informacional, diplomático, financiero, de inteligencia, económico, jurídico y de desarrollo) (Joint Chief of Staff, 2018, p.II-8). Es aquí donde se destaca el ámbito "informacional", el cual gestiona la información como herramienta del poder siendo ésta transversal por todos los demás ámbitos expuestos.

Figura 2

Integración de la información con el instrumento militar y legal en el contexto del ambiente de la información



Nota: Elaboración propia

En la figura 2 se aprecia la interacción existente entre la componente militar e informacional dentro de los ámbitos del poder. En ella, se logra observar que la sincronización de los medios que actúan en el ambiente

de la información proviene desde el más alto nivel , donde las "comunicaciones estratégicas", las "operaciones de información" y las "actividades de las información" en los niveles de la conducción estratégico, operacional y táctico, respectivamente, se cuadran en esta lucha que bien nos ilustra Foucault en la relación del poder con la verdad; aquella construcción subjetiva que influye en la dimensión cognitiva del público objetivo, podría ser parte de la población, del conductor militar, o bien del tomador de decisiones político que conduce la guerra.

Asimismo, se puede observar la integración del elemento del poder diplomático y legal con informaciones, donde nace el nuevo concepto "Lawfare"[2] acuñado por Charles J. Dunlop, general retirado de la USAF, quien en 2001 publicó un paper respecto al debate legal sobre la legitimidad de la guerra de Kosovo en 1999 (The Lawfare Institute, 2004).

En función de lo anterior, podemos aludir al ejemplo de China respecto del conflicto y disputa por el "Mar de China Meridional" o "Mar del Sur de China". Partiendo por la instalación y difusión del nombre mismo del mar en disputa, se evidencia la lucha por el dominio de la información que China ha establecido exitosamente. Tal como lo indican los autores Morris, Mazarr, Hornung, Pezard, Binnendijk y Kepe (2019), China ha recurrido cada vez más a narrativas jurídicas, estudios académicos y propuestas diplomáticas para legitimar su postura sobre las disputas territoriales y socavar los reclamos de otros Estados. Respecto

[2] Aquella estrategia de empleo (o mal uso) de la ley como sustituto de los medios militares tradicionales para lograr un objetivo operacional.

a lo mismo, China ha tratado de interpretar aspectos legales, creando excepciones dentro del orden existente, promoviendo y protegiendo sus propios intereses.

Tomando el mismo país como referencia, Elizondo (2019) cita a Michael Mazarr, quien detalla las acciones de la zona gris por parte de China en dicho conflicto, destacando la ambigüedad, la asimetría y el incrementalismo, este último partiendo con una guerra de narrativas, propaganda y uso de la historia en favor de la postura propia, es decir, generando las instancias para imponer una "verdad histórica" que quiebre el statu quo respaldado por el derecho internacional.

Ahondando a los ejemplos específicos del caso de China, los autores Morris, Mazarr, Hornung, Pezard, Binnendijk y Kepe (2019), señalan que dicho país ha implementado diferentes tácticas de la zona gris, apuntando al uso de la información, destacando lo siguiente:

- Afirmación y refuerzo de la idea que la jurisdicción de China sobre el mar del sur de China se basa en derechos históricos y zonas de pesca tradicionales anteriores a la CONVEMAR[3].
- Utilización de argumentos legales en su documento de postura sobre la disputa con Filipinas para reiterar y reafirmar las razones de por qué China decidió ignorar la sentencia y por qué el tribunal arbitral que falló sobre el asunto no tiene jurisdicción sobre el caso.
- Declarar una Zona de Identificación de Defensa Aérea (ADIZ) en el mar del Este de China.

[3] Convención de las Naciones Unidas sobre el derecho del mar.

- Regular la pesca para fortalecer el control administrativo sobre las áreas en disputa bajo el pretexto de la protección de la vida marina. Por ejemplo, en diciembre de 2013, el Congreso Popular Provincial de Hainan, en China, aprobó una ley que exigía a los buques pesqueros extranjeros obtener permiso chino antes de operar en una zona que cubre dos tercios del Mar del Sur de China.
- Financiar investigaciones sobre enfoques alternativos al derecho internacional, reforzando de manera más prominente, el derecho del mar y las leyes económicas internacionales que favorecen la posición de China. Esta estrategia incluye el establecimiento de un centro judicial marítimo internacional para brindar respaldo legal a los reclamos territoriales de China.

Como se logra apreciar, el caso de la República Popular China obedece a una manipulación de hechos y datos aparentes que tratan de difundir la construcción de una verdad, tomando como referencia el mapa de los nueve guiones. Tal como lo señala Elizondo (2019), China reinterpreta el concepto de "aguas históricas" y propone una ambigua conceptualización para fundamentar sus derechos, evitando así, utilizar el lenguaje jurídico de la CONVEMAR e incorpora conceptos opacos, sin acompañarlos de una delimitación clara.

"En términos de Holmes y Yoshihara, China logró crear una «apariencia de soberanía» sobre las islas disputadas, sus aguas y su espacio aéreo. A partir de allí, solo se trató de convertir esa apariencia en realidad" (Elizondo, 2019, p.337). En el mismo texto, se destaca que Xi Jinping afirmó, en 2016, que no pretendía la militarización de las

instalaciones en las islas Spratly y que no abrigaba propósitos ofensivos, siendo esto completamente desmentido por muchas pruebas y evidencia de IMINT que se han obtenido a lo largo de los últimos años.

Otro ejemplo en el que podemos apreciar la importancia de la información como un elemento central del poder es el caso de la invasión de Rusia a Ucrania. Si bien, la anexión de Crimea el 2014 es un típico caso de estudio para el empleo de medios "no militares" en el contexto de la zona gris del conflicto, el periodo previo a la invasión rusa del 2022 fue profundamente analizado por el Laboratorio de Investigación Forense Digital (DFRLab) del Consejo Atlántico, el cual observó la ejecución por parte de Moscú, de un juego retórico para fabricar un caso que justificara la agresión en la forma de su "operación militar especial", disfrazándola como una obligación moral de apoyar a los compatriotas en el Dombás, luchando en nombre de todos los rusos contra una Ucrania genocida y sus decadentes aliados occidentales (Aleksejeva, 2023, p.4).

Según el mismo informe (2023), el Kremlin sembró narrativas falsas y engañosas para justificar la acción militar contra Ucrania, encubrir su planificación operacional y negar cualquier responsabilidad por la guerra venidera. Dichas acciones no respaldaban el casus belli del Kremlin, sino que "eran su casus belli", por lo cual se analizó el periodo que representa los 70 días previos a la invasión, catalogando más de 10 mil artículos de 14 medios pro-Kremilin, destacando las siguientes narrativas (Aleksejeva, 2023, p.4):

- Rusia busca la paz.

- Rusia tiene la obligación moral de hacer algo respecto a la seguridad en la región.
- Ucrania es agresiva.
- Occidente está creando tensiones en la región.
- Ucrania es una marioneta de Occidente.

De esta forma, la información manipulada por Rusia, junto con otras actividades de INFOOPS, coadyuvaron a conformar una realidad y verdad fáctica que "obligaba moralmente" al presidente Putin a emplear la fuerza coactiva en el logro de sus objetivos, con el propósito de salvaguardar la seguridad de sus compatriotas. Al estar consciente que la Carta de Naciones Unidas prohíbe el uso de la fuerza para la resolución de controversias, excepto en legítima defensa, Putin estuvo consciente que debía legitimar esta autodenominada "Operación Militar Especial", generando un casus bellis que, al menos, tuviera cierta ambigüedad jurídica para ser justificada en la dimensión cognitiva de su población y de parte de la sociedad global que apoya su régimen.

La información en la toma de decisiones

En la actualidad, el ambiente estratégico se caracteriza por lo ambiguo, lo cual sumado a lo volátil, incierto y complejo, le asigna una condición desafiante para aquellos tomadores de decisiones. En esta lógica, la estrategia -cuyo propósito es determinar los modos más factibles, aceptables y adecuados con los fines y medios disponibles- busca cumplir con su fin sobre la base de una inteligencia lo más certera y oportuna, por lo cual los "datos procesados" cobran una especial

relevancia en dicha ecuación. En virtud de lo anterior, una de las formas para reducir dicha incertidumbre, producida en parte por la ambigüedad, es una adecuada gestión de la información.

De esta forma, y considerando la naturaleza propia de la guerra, el proceso de toma de decisiones requiere necesariamente de una capacidad de resolución sin información perfecta, de una visualización de la existencia de suficiente información que permita decisiones aceptables y la voluntad de actuar sobre la base de información imperfecta. “Lograr el equilibrio entre actuar ahora con información imperfecta y actuar más tarde con mejor información es esencial para el arte del mando” (Departamento del Ejército de EE.UU., 2019, p.2-3).

Según al Departamento del Ejército de EE.UU (2019), existen dos procesos que apoyan la toma de decisiones, la gestión del conocimiento y la gestión de la información, actividades interrelacionadas que construyen la comprensión situacional del comandante y de su cuartel general. Existen cuatro niveles de procesamiento, desde el nivel más bajo hasta el más alto, incluyen datos, información, conocimiento y comprensión.

En el contexto de la toma de decisiones, la comprensión es el conocimiento que se ha sintetizado y al que se ha aplicado juicio para comprender las relaciones internas de la situación, permitir la toma de decisiones e impulsar la acción (Departamento del Ejército de EE.UU., 2019, p.2-4).

Es en este proceso cuando aquella información intencionadamente entregada por el adversario podría ser parte de una operación de información, tal como lo es la "decepción" o MILDEC, la cual influye negativamente en la toma de decisiones aplicando uno de los principios de la guerra más icónico: la "sorpresa" (basada en el engaño).

Características de la sociedad post moderna

El segundo argumento que sustenta la tesis señalada en la introducción se enfoca en el contexto histórico de las características de la sociedad postmoderna, la cual tiene particularidades específicas que potencian los efectos que la mayor valorización de la información, detallada en la primera parte del capítulo, posee como fuente de poder e influencia en el marco de las operaciones de información. De esta forma, los postulados de Jean-François Lyotard explican las principales características de esta época, dentro de las cuales se destacan al ambigüedad y ambivalencia, las cuales han afectado los conceptos de seguridad y defensa. Finalmente, se profundiza en las generaciones protagonistas de la era postmoderna, las cuales poseen características especiales que promueven los efectos de las operaciones de información con un efecto multiplicador.

Postulados de Jean-François Lyotard

La postmodernidad se caracteriza por la desconfianza hacia los grandes relatos que anteriormente legitimaban el conocimiento y la sociedad. Estos relatos corresponden a narrativas globales que

pretendían explicar y dar sentido a la experiencia humana y a la historia. Jean-Francois Lyotard explica la condición postmoderna de nuestra cultura como una emancipación de la razón, transformándose en "la era del conocimiento y la información, los cuales se constituyen en medios de poder; época de desencanto y declinación de los ideales modernos; es el fin, la muerte anunciada de la idea de progreso" (Vásquez, 2011, p.3).

En el caso de la información, antiguamente, los grandes medios de comunicación establecidos (televisión, radios y periódicos) eran apreciados como fuentes fiables y autoritativas de información. En la postmodernidad, hay un escepticismo generalizado hacia estos medios, con una creciente preferencia por fuentes alternativas, entre las cuales destacan las redes sociales y blogs, que ofrecen múltiples perspectivas y a menudo contradicen las narrativas dominantes.

Según Costa (2024) respecto a la fragmentación del conocimiento, éste ya no se organiza en torno a grandes sistemas totalizantes. En lugar de ello, se caracteriza por su descomposición en múltiples pequeños relatos que no buscan la universalidad.

Asociado lo anterior a la información, en la era postmoderna, el conocimiento no se centraliza en grandes enciclopedias o instituciones académicas. Por el contrario, existe una explosión de plataformas digitales (blogs, foros, podcasts y canales de YouTube) que ofrecen información sobre cualquier tema imaginable, fragmentando así la autoridad tradicional de las fuentes de información.

El mismo autor (2024) señala en relación con la legitimidad del saber, que, en la modernidad, el conocimiento se sustentaba a través de estos metarrelatos. Sin embargo, en la postmodernidad, esta legitimación se basa en la performatividad y la utilidad, más que en verdades universales.

Por ejemplo, en la era postmoderna, las noticias y la información a menudo se valoran por su impacto mediático y su capacidad para atraer atención (clickbait), en lugar de por su profundidad o rigor científico. La legitimación del conocimiento se basa en métricas de audiencia y engagement más que en la veracidad o la profundidad analítica. En este sentido, se produce una sensación de éxito más por los resultados de "rating" que por el contenido mismo de la noticia.

Finalmente, en la postmodernidad, la ciencia y la tecnología no se aprecian como herramientas de emancipación, si no como campos fragmentados y sujetos a la lógica del capital y la eficiencia. De esta forma, la tecnología de la información se utiliza para maximizar el tiempo de pantalla y la interacción del usuario, aislando la atención y el conocimiento en función de intereses comerciales, aumentando con ello el vacío y superficialidad de la razón, el conocimiento y rigor científico.

La ambigüedad y ambivalencia en la postmodernidad

Hoy en día vivimos en una época postmoderna en que todo es "relativo". Según Vásquez (2011), nos encontramos viviendo en el dominio de la interpretación y la sobreinterpretación, dotándole de sentido a los hechos. Lo anterior es una condición necesaria para que

podamos conocer la realidad y relacionarnos con ella, distinguiendo el objeto de la ciencia central de la Posmodernidad: la Hermenéutica.

Una de las características más icónicas del mundo occidental contemporáneo es el respeto y promoción de los derechos humanos. Uno de ellos, es la "libertad", y derivado de ésta, la "libertad de expresión", la cual ha sido el perfecto caldo de cultivo para promover la ambivalencia y ambigüedad en la deconstrucción de la verdad moderna. Los sistemas políticos de las democracias occidentales permiten el ejercicio irrestricto de dicha libertad, pese a que ex-post las manipulaciones de información puedan someterse a la justicia, según los eventuales delitos tipificados por dicho marco jurídico.

Por otra parte, Marrero y Trajtenberg (2009) citan a Bauman, quien alude que la "modernidad" se encuentra constantemente preocupada por el "orden". Uno de sus objetivos es construir un relato claro y preciso, con tipologías ordenadas y clasificaciones preestablecidas. En virtud de lo anterior, señalan que Bauman hace una aguda crítica respecto de esta situación calificando de "imposible" lograr dicho resultado. Su tesis apunta a describir como "líquida" la característica central de la actual sociedad, destacando conceptos como ambivalencia, incertidumbre e indeterminación de las formas (Marrero y Trajtenberg, 2009, p.37).

Muestra de lo anterior es el desarrollo del concepto de "conflicto en la zona gris", fenómeno definido (entre distintos autores) como:

> Un espacio operacional entre la paz y la guerra, que implica

> acciones coercitivas para cambiar el statu quo, pero por debajo de un umbral que, en la mayoría de los casos, provocaría una respuesta militar convencional, **desdibujando la línea entre** acciones militares y no militares en condición de incertidumbre de los marcos legales" (Morris, Mazarr, Hornung, Pezard, Binnendijk y Kepe, 2009, p.8).

En ella, podemos apreciar que una de las características centrales de su naturaleza es la ambigüedad y la dificultad de atribuibilidad, estacando los límites difusos entre la paz y la guerra, lo militar y no militar, y entre la seguridad exterior e interior de un Estado.

Volviendo al caso del Mar del Sur de China, la postura de las nueve líneas por parte esta potencia asiática es uno de los casos más icónicos de la ambigüedad actual del derecho internacional. Por una parte, la postura de China podría tomarse desde una perspectiva de reclamación territorial sobre las islas en disputa, aplicando para ello la Convención de Viena. Por el contrario, si las líneas representaran una reclamación marítima de estatus especial de todas las aguas contenidas en ella, entonces aplicaría la CONVEMAR. La construcción de islas artificiales complejiza aún más esta situación, toda vez que da pie para interpretaciones antojadizas del derecho del mar en relación con la definición de qué es una isla y aquellas porciones de tierra que tienen asociada alguna zona marítima bajo su propia jurisdicción.

En el caso ruso, el ejercicio de su doctrina de "control reflexivo" explica el carácter ambiguo de la actual sociedad postmoderna y su ambiente estratégico. Según los autores Giles, Sherr y Seaboyer (2018), dicho concepto corresponde al proceso de transmitir intencionalmente a un adversario cierta información agregada que hará que ese actor tome una decisión apropiada a esa información. Lo anterior destaca una característica clave del control reflexivo: "la necesidad de adaptar la información falsa al objetivo específico y reflejar las respuestas y reacciones del objetivo" (Giles, Sherr y Seaboyer, 2018, p.5). Esto indica que el control reflexivo implica un enfoque mucho más amplio y complejo que el engaño puro o el suministro a un comandante adversario de información falsa para que éste base su toma de decisión. En lugar de consistir solo en desinformación, el control reflexivo contempla un programa compuesto de toma de decisiones dirigidas a través de múltiples vectores, teniendo en cuenta no sólo el procesamiento lógico de la información por parte del adversario, sino también los marcos emocionales, psicológicos, culturales y de otro tipo dentro de los cuales se toman las decisiones.

Según Giles, Sherr y Seaboyer (2018), el control reflexivo posee tres características principales:

1) El enfoque de Rusia para la guerra de la información es holístico *"kompleksnyy podhod"*, es decir, combina ataques digitales-tecnológicos y cognitivo-psicológicos. Mientras que el sabotaje digital tiene como objetivo desorganizar, perturbar y destruir la capacidad de gestión de un estado, la subversión psicológica tiene

como objetivo engañar al adversario, desacreditar a su liderazgo y desorientar y desmoralizar a la población y sus Fuerzas Armadas.

2) Posee unidad de esfuerzo *"edinstvo usilii"*, ya que sincroniza la guerra de la información con medios militares cinéticos y no cinéticos y con efectos de otros elementos del poder nacional. Existe la planificación y coordinación desde el más alto nivel correspondiente a un espectro de actores gubernamentales y no gubernamentales, militares, paramilitares y no militares.
3) Se necesita un esfuerzo estratégico permanente e ininterrumpido *"bezpriryvnost"*. La campaña de la información debe librarse durante tiempos de paz y tiempos de guerra, simultáneamente en todos los dominios y medios nacionales, del adversario e internacionales.

De igual forma los mismos autores (2018), aluden que el control reflexivo potencia sus efectos combinándolos con otras actividades de índole similar:

1) La estratagema militar *"voyennaya khitrost"*, la cual se encuentra "diseñada para confundir al enemigo respecto de la condición, la ubicación y el carácter de la actividad militar propia". Esta acción, a diferencia del control reflexivo, no está necesariamente diseñada para inducir al oponente a tomar una decisión u otra.
2) El concepto ruso de *"maskirovka"*, el cual contempla un complejo de medidas ideadas para confundir al enemigo respecto de la "presencia y disposición de las fuerzas, su condición, preparación, acciones y planes". *Maskirovka* está diseñada explícitamente para

lograr la sorpresa, que no siempre es un propósito del control reflexivo.

3) La diversión *"diversiya"* tiene un propósito diferente, aunque complementario: "desviar la atención del enemigo y dividir sus fuerzas". El elemento reflexivo en *diversiya* es fuerte, sin embargo, está diseñado para producir una respuesta general, mientras que el control reflexivo, en su forma más pura, está diseñado para producir una respuesta específica.
4) Inteligencia/reconocimiento en fuerza *"razvedka boyem"*, la cual contempla la "obtención de información sobre el enemigo mediante una acción ofensiva", pudiendo tener o no un componente reflexivo. En el caso que esta acción táctica complementaria esté diseñada para provocar una respuesta específica que revele información de valor de inteligencia, entonces el control reflexivo aplicaría a los propósitos de *razvedka boyem*.

Al igual que en la anexión de Crimea en 2014, el ejercicio del "control reflexivo" en la región del Dombás, se realizó en primer lugar, mediante personal de servicios especiales de inteligencia disfrazados de "turistas" y segundo, mediante destacamentos conformados por milicias locales *"opolchenie"*, tratando de instalar la idea que esta confrontación correspondía a una guerra civil, en lugar de una guerra híbrida financiada y dirigida desde el exterior, explotando de esta forma la confusión de los límites entre dos tipos de conflictos con apariencias similares.

El ejemplo anterior, tomando como referencia los postulados

modernos del conflicto, alude directamente a una fase de éste denominada crisis, la cual se define como:

> Una situación de tensión que da comienzo al conflicto propiamente tal, la que se produce en el entorno interno o externo de un Estado en tiempo de paz en que están comprometidos intereses importantes de los actores involucrados, existiendo la posibilidad de escalar a una situación de guerra y que puede involucrar el desplazamiento de fuerzas militares e incluso su empleo restringido. (Ministerio Defensa Nacional, 2022, p. 27)

Sin embargo, podemos apreciar que la doctrina rusa emplea los postulados del postmodernismo, toda vez que considera parte de esta fase como un periodo mismo de la "guerra" sin ser parte de ella dada la visión lineal moderna. Lo anterior, les otorgas una ambigüedad e incertidumbre ventajosa dentro del contexto del derecho internacional basado en principios claramente establecidos en la modernidad.

Cabe destacar que el pasado ejemplo se relaciona directamente con el clásico concepto ruso heredado de la era soviética denominado "Periodo Inicial de la Guerra" (IPW por su siglas en inglés), el cual aplica cuando los estados realizan operaciones militares que involucran medios de sus fuerzas armadas que están "desplegados antes del inicio de la guerra para lograr objetivos estratégicos de corto plazo o para crear condiciones favorables para comprometer sus fuerzas principales y

continuar con más operaciones" (Thomas, 2019, p.7-5). Para Rusia el IPW cobra mayor relevancia y asegura la explotación del éxito en las primeras operaciones del empleo masivo del potencial bélico, ya que la ambigüedad reinante del ambiente estratégico permite que los medios contemplados en dichas operaciones sean difíciles de identificar y comprometer.

Según el Cyber Peace Institute (2022), el 24 de febrero de 2022, el día de la invasión rusa a Ucrania, un ciberataque interrumpió el acceso a Internet por satélite de banda ancha. Este ataque deshabilitó los módems que se comunican con la red satelital KA-SAT de la compañía Viasat, que proporciona acceso a Internet a decenas de miles de personas en Ucrania y Europa. Se estima que el propósito del ataque era interrumpir el servicio, afectando el mando y control ucraniano en lugar de acceder a datos o sistemas. En ese caso se observa como Rusia aplicó la doctrina de operaciones en el IPW, efectuando este ciberataque que provocó efectos en las Fuerzas Armadas de Ucrania y su población en general, así como en diversas empresas del rubro energético a lo largo de Europa.

Las particularidades de las generaciones influidas por el postmodernismo

En la actualidad, las instituciones de la defensa en cualquier país cuentan con la cohabitación de tres generaciones dentro de su cuerpo de oficiales (enfocándonos particularmente en los tomadores de decisiones), desde su alto mando (comandantes de nivel brigada o superior) compuestos por la generación "X", pasando por sus mandos medios (comandantes de nivel unidad de combate y fundamental)

conformados por la generación “Y” (más conocidos como “Millennials”) hasta los mandos subalternos y cadetes (comandantes de nivel sección / pelotón) integrados por la generación “Z”.

Cada generación posee una propia visión del mundo, denotando ciertos rasgos que influyen en mayor o menor medida dentro de la dimensión cognitiva del ambiente de la información. Lo anterior se enfoca, particularmente, en su relación con las tecnologías de la información (TICs) y redes sociales, ya que estas herramientas que han facilitado el progreso de la sociedad, para algunos son simples medios y para otros una necesidad vital en su diario vivir.

De las tres generaciones anteriormente citadas, los millennials y Z constituyen el mayor porcentaje del personal activo de las fuerzas armadas que podría superar el 75%. Según Boyer y Livieratos (2022), los millennials son aquellos nacidos entre 1981 y 1997; poseen una visión del mundo marcada por su educación post Guerra Fría, siendo su mayor característica ser “nativos digitales”, pese a que muchos de ellos ya habían terminado la educación secundaria cuando se desarrollaron tecnologías clave como los teléfonos inteligentes y las redes sociales. Por su parte, la Generación “Z”, (también conocidos como "iGen" o "NetGen"), incluye a los nacidos entre 1998 y 2016. Su mayor característica es que son dependientes digitales, debido a que crecieron entre computadores, teléfonos inteligentes y redes sociales. Esto ha influido en su validación social, ya que dependen necesariamente de los “likes” o interacciones positivas digitales para sentirse plenamente integrados a un mundo interconectado.

Ambas generaciones se informan principalmente por redes sociales y están sujetas a la influencia de la ingeniería social, big data e inteligencia artificial en razón a la generación de sus mismas tendencias. Sin embargo, a pesar de haber sido criados como usuarios de las redes sociales, la generación Z no es más hábil para separar los hechos de la ficción e identificar la información errónea que las generaciones anteriores (de hecho, pueden ser más susceptibles a la desinformación) (Boyer y Livieratos, 2022, p.8).

Este acceso permanente a las TICs y en particular, a los medios de comunicación masiva y redes sociales, permite acceder de inmediato y en forma instantánea a toda clase de información difundida por dichas plataformas. La rapidez y efecto multiplicador que poseen las redes sociales con los denominados "retweet" o reenvío de mensajes, permiten la dispersión veloz y muy efectiva de diverso tipo de noticias e información útil que afecta la dimensión cognitiva de las personas, incluidos los tomadores de decisiones.

Lo anterior, sumado a las características de ambas generaciones, podría explicar el éxito de las operaciones de información y la relevancia que hoy en día presentan dentro de la dinámica del conflicto armado. La participación de "bloggers" e "influencers" como fuentes abiertas para el procesamiento de información en la guerra de Rusia-Ucrania es una muestra viva que la combinación de jóvenes "Z", con un teléfono inteligente, internet y alguna plataforma de difusión, permiten aportar al ciclo de inteligencia de manera efectiva.

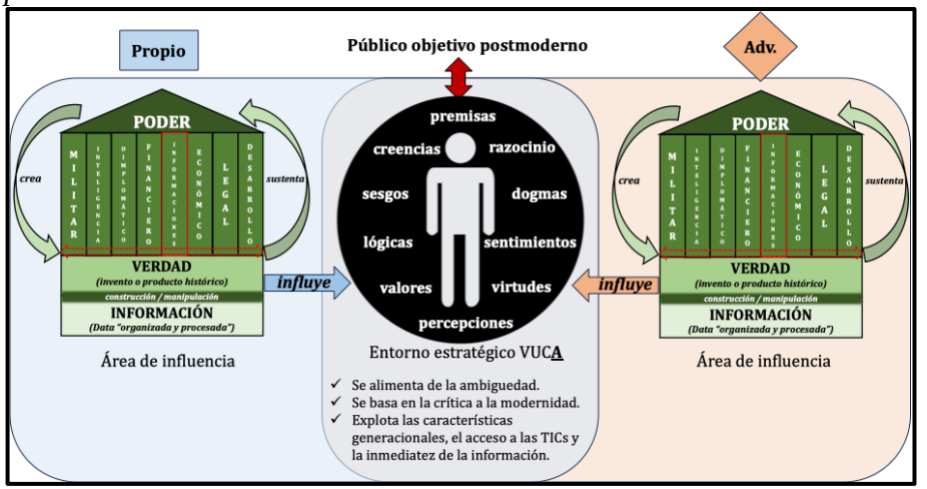
Algunas reflexiones que aporten para una posible solución

Según Costa (2024), Jürgen Habermas critica la postmodernidad por su escepticismo hacia los metarrelatos y la fragmentación del conocimiento y la verdad. En "El discurso filosófico de la modernidad" (1985) y otras obras, propone revitalizar el proyecto de la modernidad mediante la racionalidad comunicativa, el diálogo inclusivo y la deliberación pública. Es en estos puntos, en donde se estima pertinente hacer hincapié para determinar los conceptos básicos que podría considerar una solución a la problemática presentada durante el capítulo.

Haciendo un resumen de este, podríamos establecer que uno de los problemas centrales provenientes del éxito de las operaciones de información en la guerra contemporánea, corresponde a la débil verificación de la información utilizada para la toma de decisiones o que influya en la dimensión cognitiva (en el más amplio sentido incluyendo aspectos morales, psicológicos, anímicos, etc.) del público objetivo.

Figura 3

Lucha por la dimensión cognitiva en el contexto estratégico postmoderno



Nota: Elaboración propia

En la figura 3, podemos observar gráficamente la disputa por la dimensión cognitiva en el ambiente de la información. Esta lucha apunta a que:

> Existe un combate "por la verdad" o al menos "alrededor de la verdad" – una vez más entiéndase bien que por verdad no quiero decir "el conjunto de cosas verdaderas que hay que descubrir o hacer aceptar", sino "el conjunto de reglas según las cuales se discrimina lo verdadero de lo falso y se ligan a lo verdadero efectos políticos de poder" (Foucault, 1980, p. 188).

El actual ambiente estratégico caracterizado por las particularidades de la sociedad postmoderna, la revolución industrial 4.0 con las implicancias del acceso a las TICs de gran parte de la población en general, y de las generaciones millennial y Z en particular, y la gran importancia que hemos podido comprobar respecto al valor de la información en las operaciones militares, han generado las condiciones ideales para poder ejercer una influencia decisiva en la dimensión cognitiva de la sociedad en su conjunto.

Tal como lo menciona Habermas (1985) en su primer punto de revitalización de la modernidad que considera la "racionalidad comunicativa", la principal forma de combatir una posible influencia que un tercer actor quisiera ejercer sobre un público objetivo es el profundo desarrollo del pensamiento estratégico. En efecto, como parte del anterior, el pensamiento crítico, asociado al estudio de la filosofía y su relación con el fenómeno de la guerra, ha capturado la atención de grandes autores quienes han demostrado la directa influencia de las diferentes corrientes filosóficas de la historia con los tipos de guerra que el mundo ha vivido.

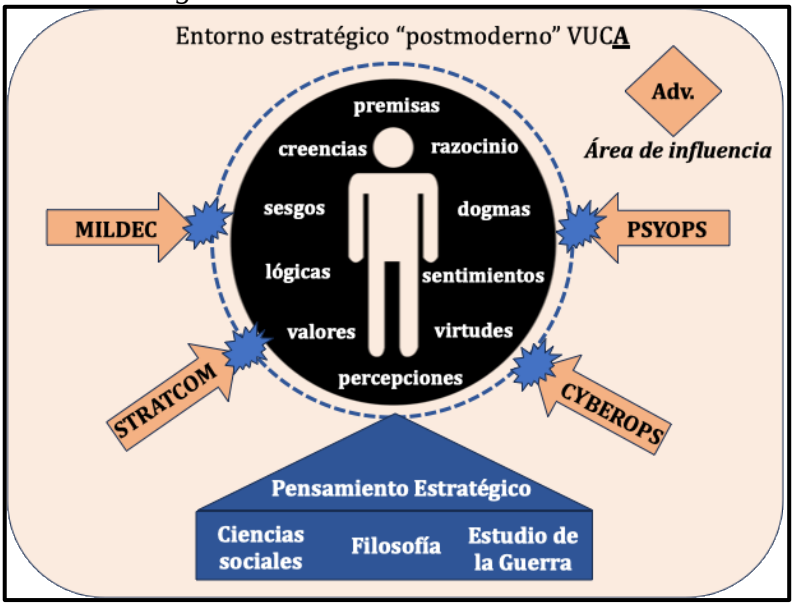
Una de las formas de poder asumir, conscientemente, las diversas verdades impuestas en esta lucha señalada por Foucault, es que el tomador de decisiones -ya sea político o militar en el contexto del conflicto- debe contar con una sólida formación en las ciencias sociales, particularmente, en filosofía. El estudio de la razón, del pensamiento, de la reflexión, de la interpretación textual y de la argumentación, permitirá contar con mejores herramientas cognitivas para poder aplicar un juicio

crítico y de esta manera, verificar la "veracidad objetiva" de esta construcción subjetiva de la que somos objeto de manera constante en esta disputa por la dimensión cognitiva del conflicto.

De igual forma, el desarrollo del pensamiento creativo podrá complementar esta capacidad de análisis objetivo que permita explorar y anticiparse a nuevas formas de afección de las mismas INFOOPS, contando con mejores herramientas para neutralizar los efectos nocivos en la dimensión cognitiva del público objetivo previamente citado.

Figura 4

Una posible forma de neutralizar los efectos buscados por el adversario en la dimensión cognitiva



Nota: Elaboración propia

En la Figura 4, observamos una representación gráfica de la barrera conceptual o cortafuego (firewall) que el pensamiento estratégico constituiría para evitar ser víctimas de las INFOOPS adversarias en un entorno VUCA (especialmente ambiguo dada la naturaleza postmoderna de nuestra sociedad). Lo anterior, sobre la base de un profundo conocimiento en las ciencias sociales, filosofía y estudio de la guerra que permitan al tomador de decisiones poder discernir entre una verdad subjetiva manipulada o una información procesada con una base objetiva y confiable. El estudio de la historia militar cobrará un especial valor en esta formación dada su directa vinculación con la estructura del pensamiento estratégico.

Volviendo a la fórmula de seguridad acuñada por Manunta (1999), [S= f (A, P, T) Si], podremos reemplazar sus variables tomando en consideración los aspectos tratados en el presente capítulo. Sin duda que, para nuestro caso, "A" (asset) será la "Información", la cual constituye la base del poder en cuanto a la construcción de la verdad. Por su parte, "T" (threat) será aquel actor que quiera influir negativamente en el ambiente de la información para afectar la toma de decisiones del conductor político o militar, o bien en la dimensión moral del público objetivo. El contexto situacional "Si" es nuestro ambiente VUCA (especialmente ambiguo) del entorno estratégico postmoderno. Completando nuestra ecuación, dejo para el final el "P" protector del "asset", con el propósito de lograr el concepto operacional de "seguridad" en el ambiente de la información; este protector será aquel actor que logre desarrollar un sólido pensamiento estratégico, con

herramientas cognitivas adecuadas para la gestión de la información.

Conclusiones

Tras analizar las razones del éxito y la importancia de las operaciones de información en el contexto de la guerra actual se puede concluir lo siguiente:

Existen condiciones fundamentales para que las INFOOPS logren su cometido de influir en la dimensión cognitiva del ambiente de la información exitosamente. La sinergia lograda por las condiciones ambiguas del ambiente estratégico, sumado a las características propias del postmodernismo y de las generaciones millenials y Z -particularmente su interacción con las TICs y redes sociales- junto con la importancia de la información en el marco de las comunicaciones estratégicas del instrumento militar, hacen extremadamente complejo el diseño de una estrategia de solución para dicha problemática.

El alcance de las redes sociales, las características de las plataformas tecnológicas y todas aquellas herramientas asociadas a la revolución 4.0, permiten la gestión de gran cantidad de información en poco tiempo con gran inmediatez, afectando masivamente a diversos públicos objetivos. Lo anterior, afecta al individuo desde la perspectiva trinitaria de la guerra como tomador de decisiones guiado por la razón (en el espectro político), por la pasión (en el espectro moral de la población y el combatiente) y del azar (en aquellas decisiones del conductor militar afectas por la incertidumbre).

La concepción subjetiva del poder postulada por Foucault y su relación con la construcción de la verdad, nos permite relacionar la importancia y valor del procesamiento de datos y generación de información, con el ejercicio de este, el cual apunta directamente a la influencia en las mentes y corazones del ser humano.

A lo largo del presente capítulo, hemos podido apreciar con casos empíricos de Rusia y China, que la articulación del poder de la información -visto desde la perspectiva de los elementos del poder nacional- con los otros elementos (MIDFIELD) son y deben ser necesariamente sincronizados desde el más alto nivel de la conducción política para que tengan el efecto deseado. Bajo esta lógica las INFOOPS surgen de la integración del instrumento militar dentro del alero del informacional.

Finalmente, tomando como referencia los postulados de Habermas en su crítica al postmodernismo, se propone una posible forma de neutralizar los efectos de las operaciones de información en nuestra gente que considere el fomento y desarrollo del pensamiento estratégico, cuya base fundamental es la aplicación del pensamiento crítico basado en la filosofía del conflicto y el pensamiento creativo en el arte de la guerra.

Referencias Bibliográficas

Alborova, M., Bulva, V., Krutskikh, A., Yudina, Y. y Zinovieva, E., (2021) *International Information Security: Russia's Approaches.* MGIMO University. https://mgimo.ru/

Aleksejeva, N., (febrero de 2023). *Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine.* Digital Forensic Research Lab. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf

Bartles, Ch., (2016). *Cómo comprender el artículo de Gerasimov*. Military Review, (Marzo-Abril 2016), 55-64. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20160430_art011SPA.pdf

Boyer, A. y Livieratos, C., (16 de junio de 2022). *The Changing Character of Followers: Generational Dynamics, Technology, and the Future of Army Leadership.* Modern War Institute at West Point. https://mwi.westpoint.edu/the-changing-character-of-followers-generational-dynamics-technology-and-the-future-of-army-leadership/

Brussee, V. y Von Carnap, K., (2024). *The increasing challenge of obtaining information from Xi's China*. Mercator Institute for China Studies. https://merics.org/sites/default/files/2024-02/MERICS%20Report%20Online%20information%20on%20CHina.pdf

Carrière-Swallow, Y. y Haksar, V., (23 de septiembre de 2019). *La Economía de los Datos. IMF* Blog. https://www.imf.org/es/Blogs/Articles/2019/09/23/the-economics-of-data

Conferencia de las Naciones Unidas para el Comercio y Desarrollo, (2019). *Informe sobre la Economía Digital 2019*. https://unctad.org/es/system/files/official-document/der2019_overview_es.pdf

Conferencia de las Naciones Unidas para el Comercio y Desarrollo, (2021). *Informe sobre la Economía Digital 2021*. https://unctad.org/system/files/official-document/der2021_es_0.pdf

Costa, P., *comunicación personal*, 02 de septiembre de 2024.

Cyber Peace Institute (junio de 2022). *Case Study VIASAT*. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Dunlop, Ch., (2008). *Lawfare Today: A Perspective*. Yale Journal of International Affairs (winter 2008). https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5892&context=faculty_scholarship

Elizondo, S., (2019). *Estrategia de zona gris y libertad de navegación: El caso del Mar del Sur de China*. Centro Naval, (Boletín 852 SEP/DIC 2019), 326-345.

Foucault, M., (1980). *Microfísica del Poder*. La Piqueta.

Giles, K., Sherr, J. y Seaboyer, A., (octubre de 2018). *Russian Reflexive Control*. Defence Research and Development Canada, Royal Military College of Canada. https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control

Habermas, J. (1985). *El discurso filosófico de la modernidad*. Taurus humanidades. https://sociologiaycultura.wordpress.com/wp-content/uploads/2014/02/habermas-jurgen-el-discurso-filosofico-de-la-modernidad.pdf

Hakala, J. y Melnychukse, J., (junio de 2021). *Russia's Strategy in Cyberspace.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210

Hernández, I. (2014). *Floridi: Información y Filosofía*. *THÉMATA.* Revista de Filosofía (No49, enero-junio). 127-142. https://revistascientificas.us.es/index.php/themata/article/view/302/268

HQ, Department of the Army, (2019). *ADP 6-0 Mission Command "Command and Control of Army Forces".*

INVERSIS, Banco, (26 de septiembre de 2022). *Economía del dato, el valor de la información.* https://www.inversis.es/news/Econom%C3%ADa-del-dato-el-valor-de-la-informaci%C3%B3n.html

Joint Chiefs of Staff, (2018). *Joint Doctrine Note 1-18 "Strategy".*

Liaropoulus, A., (noviembre de 2022). *Information as an Instrument of Power - Lessons learned from the War in Ukraine*. NATO OPEN Publications, vol.7, no.6. https://www.researchgate.net/publication/365635155_Information_as_an_Instrument_of_Power_-_Lessons_learned_from_the_War_in_Ukraine_NATO_OPEN_Publications_vol7_no6_2022/references

Manunta, G. (1999) *What is security?* Security Journal (volume 12), 57–66. https://doi.org/10.1057/palgrave.sj.8340030

Marrero, A. y Trajtenberg, N., (2009). *Bauman, ambivalencia y después. Sus descontentos y los nuestros.* Revista de la Asociación de Sociología de la Educación (Vol 2, num. 1, enero), 34-56. https://dialnet.unirioja.es/servlet/articulo?codigo=2794357

Ministerio de Defensa Nacional. (2023). *DNC–00 "Acción Conjunta para las Fuerzas Armadas".*

Ministerio de Defensa Nacional, (2023). DNC 2–04 *"Preparación de Inteligencia del Ambiente Operacional Conjunto (JIPOE)".*

Morris, L., Mazarr, M., Hornung, J., Pezard, S., Binnendijk, A., Kepe, M. (2019). *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. Bulletin of the RAND Corporation (RR2942), 27-41. https://www.rand.org/pubs/research_reports/RR2942.html.

Nurton, J., (marzo de 2022), *Los datos son el combustible de la transformación de la economía mundial*. OMPI Revista. https://www.wipo.int/wipo_magazine_digital/es/2022/article_0002.html#:~:text=Tang%20afirm%C3%B3%20que%20%E2%80%9Csi%20la,de%20las%20tecnolog%C3%ADas%20de%20vanguardia.

The Lawfare Institute. (s.f.). *A Brief History of the Term and the Site.* Recuperado el 12 de septiembre de 2024. https://www.lawfaremedia.org/about/our-story

Thomas, T., (agosto de 2019). *Russian Military Thought: Concepts and Elements*. MITRE. https://www.mitre.org/sites/default/files/2021-11/prs-19-1004-russian-military-thought-concepts-elements.pdf

UK Ministry of Defence, (2023). *AJP-10 Allied Joint Doctrine for Strategic Communications*. Edition a Version 1 with UK national elements. https://modgovuk.sharepoint.com/sites/IntranetUKStratCom/SitePages/ development-concepts-and-doctrine-centre-dcdc.aspx

Vásquez, A., (2011). *La Posmodernidad. Nuevo régimen de verdad, violencia metafísica y fin de los metarrelatos*. Nómadas. Critical Journal of Social and Juridical Sciences, *(*vol. 29, núm. 1). https://www.redalyc.org/pdf/181/18118941015.pdf

CAPÍTULO 5

La dimensión humana en el contexto de las operaciones de información: Un enfoque psicológico basado en la comunicación, la influencia y la persuasión

Psicólogo (Mgr.) Francisco Javier Urra Riveros[1]

Introducción

En la guerra moderna, las operaciones de información (INFOOPS) han influido en los resultados de los conflictos a través del control y la gestión de la información. Estas operaciones impactan las percepciones y decisiones, apoyan las acciones militares tradicionales, y protegen contra la desinformación enemiga; además en conflictos asimétricos, este tipo de operaciones equilibran el campo de batalla. Con los avances tecnológicos, el ciberespacio también se ha convertido en un nuevo campo de batalla, donde las INFOOPS emplean ciberataques y la desinformación para influir sobre infraestructuras críticas y sistemas de información, entre otros.

Históricamente, la manipulación de la información ha sido una táctica en la guerra, desde el "Caballo de Troya" hasta operaciones más

[1] Psicólogo y Perito Judicial, Magister en Ergonomía (Universidad de Concepción) y Magister en Educación Superior Mención Investigación (Universidad Central); Certificate in Ergonomics and Human Factors (Harvard University), Postítulo profesional en Administración de Recursos Humanos (Universidad Católica del Norte); Diplomado en Salud Ocupacional (Universidad de Chile). Actualmente ejerce como metodólogo en el Centro de Estudios Estratégicos de la Academia de Guerra. Correo electrónico: francisco.urra@acague.cl.

estructuradas como la “Operación Fortitude” en la Segunda Guerra Mundial.

El Departamento de Defensa de los Estados Unidos (2014), afirma que la información es una herramienta poderosa para "influir, interrumpir, corromper o usurpar la toma de decisiones de un adversario con el fin de tomar y compartir decisiones" (JP-3-13, 2014, p. I-1), reconociéndola además como "un instrumento de poder nacional" (Mattis, 2017, como se citó en JP-03-04, 2022, p. I-1).

Este artículo explora la integración de principios psicológicos en las INFOOPS para mejorar su efectividad, considerando aspectos como la defensa cognitiva, la manipulación de la información, y el rol crucial de la influencia, basada en la persuasión y cognición social. Además, se abordan los dilemas éticos asociados al uso de estas técnicas y se ofrecen recomendaciones para su aplicación ética y efectiva en el contexto militar.

1. Principios Psicológicos Aplicados a las Operaciones de Información

En el ámbito de las INFOOPS, es importante considerar la resistencia que los individuos pueden presentar frente a estas técnicas comunicativas. Lario (2019) destaca tres teorías clave que explican dichas resistencias: la reactancia psicológica, la disonancia cognitiva y la teoría de la inoculación (Lario, 2019, como se citó en Ejido, 2023, p. 350). Por lo tanto, reconocerlas permitirá desarrollar estrategias de comunicación persuasiva más efectivas:

1.1 Reactancia Psicológica

La reactancia psicológica se refiere a oponerse a restricciones percibidas sobre la libertad; por ejemplo, cuando se le indica a alguien que no toque un objeto, es posible que sienta la necesidad de hacer lo contrario. Para superar esta reactancia es esencial enfatizar que las personas tienen la libertad de elegir.

Un ejemplo de la aplicación de la teoría de la reactancia psicológica en las INFOOPS la encontramos en una campaña destinada a influir en la percepción de una población local en una zona de conflicto, en el cual, las fuerzas aliadas desean que la población no brinde apoyo a las fuerzas insurgentes; por lo que si se transmiten mensajes como: "*No apoyes a los insurgentes*", es probable que algunos miembros de la población local perciban esto como una imposición que limite su libertad de elección, lo que podría llevarlos a hacer lo contrario, es decir, apoyar a los insurgentes como una forma de resistir la restricción percibida.

Para evitar esta reactancia, el mensaje podría reformularse para subrayar la libertad de la población, por ejemplo: "*Entendemos que la decisión es de ustedes, pero creemos que su comunidad estará más segura si no apoyan a los insurgentes. La elección es completamente de ustedes*". Entonces, reconocer la autonomía de la población, permitirá reducir la resistencia, aumentando la probabilidad de que el mensaje sea recibido positivamente, alineándose con los objetivos de la operación.

1.2 Disonancia Cognitiva y Coherencia

Cuando enfrentan información contradictoria, los seres humanos pueden justificar el cambio en sus creencias o acciones para evitar el malestar cognitivo. Una persona coherente es más resistente a cambiar sus creencias ante mensajes contradictorios; siendo fundamental que el persuasor conozca bien las creencias y actitudes de su audiencia para adaptar su mensaje de manera que resuene con ellos minimizando la disonancia.

Un ejemplo de influencia en la percepción de soldados enemigos es cuando una fuerza militar busca que estos cuestionen su lealtad hacia sus líderes. Aunque los soldados están entrenados para confiar en la autoridad y en su causa, un mensaje que contradiga estas creencias, como: "Su líder lo está utilizando y no se preocupa por su bienestar", puede generar disonancia cognitiva. Este conflicto podría llevar a los soldados a justificar sus creencias y rechazar el mensaje.

En consecuencia, para que el mensaje sea más efectivo, las fuerzas aliadas podrían enmarcarlo de manera que se alinee con la coherencia interna de ellos, reduciendo su disonancia; señalando: "*Sabemos que son soldados leales que valoran el honor y la protección de sus familias. ¿Se han preguntado si sus líderes están actuando realmente de acuerdo con esos valores?"*. Al plantear así la pregunta, el mensaje invitará a los soldados a generar una reflexión respecto de sus creencias sin atacarlas directamente, minimizando la disonancia cognitiva y aumentando la probabilidad de que reconsideren su lealtad.

1.3 Teoría de la Inoculación

Esta teoría sugiere que, al preparar a las personas con información moderada sobre críticas, aumente su resistencia a la propaganda adversaria. La inoculación prepara a las personas para resistir mejor a futuras influencias que puedan desafiar sus creencias. Un ejemplo de la aplicación de esta teoría podría ser el siguiente:

En un escenario donde una coalición internacional enfrenta a un grupo insurgente que intenta ganar el apoyo de la población local, los insurgentes utilizan propaganda para desacreditar a las fuerzas de paz, presentándolas como ocupantes sin interés en la comunidad. Para contrarrestar esta narrativa y fortalecer la confianza de la población, las fuerzas podrían lanzar campañas informativas que reconozcan los desafíos, como dificultades logísticas o malentendidos iniciales, mientras destacan sus esfuerzos continuos y compromiso con la paz y la seguridad de la comunidad. Este enfoque expone a la población a críticas moderadas que los insurgentes podrían utilizar, desarrollando una mayor resistencia a la propaganda insurgente.

Al mostrar transparencia y disposición para superar desafíos, las fuerzas de paz refuerzan su credibilidad, aumentando así la cohesión y lealtad de la población hacia sus esfuerzos, dificultando que los insurgentes cambien las percepciones de la comunidad en el futuro.

Al respecto, Lario (2019) destaca la importancia de la persuasión para superar las barreras psicológicas que puedan dificultar el cambio deseado en la audiencia, señalando "…el persuasor debe tener en cuenta

sus propias intenciones, conocer bien a su público y crear mensajes adecuados a sus objetivos y a las características de la audiencia" (Lario, 2019, como se citó en Egido, 2023, p. 351).

2. Clases de Persuasión Aplicadas a INFOOPS

En las INFOOPS, es crucial examinar el concepto militar de 'STRATCOM' según la doctrina de la OTAN. Este concepto destaca una serie de capacidades esenciales para su implementación efectiva; al respecto, Vásquez (2016), señala que estas capacidades incluyen:

> "Estimar los efectos sobre las percepciones, actitudes, comportamientos (PAC), creencias y acciones de las audiencias objetivo; desarrollar y distribuir, oportunamente y adecuados a cada cultura, mensajes basados en las narrativas; y desarrollar y distribuir, de forma rápida, información específicamente diseñada para influir en las audiencias seleccionadas". (Vásquez, 2016, como se citó en Urra, 2021, p. 74).

El "espectro de la persuasión" abarca diversos enfoques para influir en las PAC[2] de las audiencias. Cada enfoque ofrece una perspectiva única, permitiendo utilizar la persuasión de manera estratégica en

[2] Percepciones, Actitudes y Comportamientos.

diferentes contextos. La Tabla 1 detalla estas aproximaciones, proporcionando una visión integral de su aplicación.

Tabla 1

El Espectro de la persuasión

ESPECTRO	Aproximación	Onotlogía de las RR.II.	Rol de la comunicación	Rol de la persuasión
PERSUASIÓN	Racionalista	Interacciones de los actores con unas preferencias en una estructura dfeanarquía.	Estratégico. Señales con intención de manipular impresiones.	Secundario para los estimulos materiales (coerción, negociación) pero posible comprometiendo a otros a la acción a través de la retórica o produciendo un plan en los que los demás estan dispuestos a comprometerse.
	Comunicativa	Interacciones entre actores con identidades crean compensaciones intersubjetivas del sistema.	Intercambio de reivindicaciones entre actores.	Buenos argumentos pueden crear consenso y conformar como otros ven el mundo.
	Reflexiva	Actores cuyas identidades estan mutuamente implicadas y cuyas acciones generanrespuestas entre los otros.	Estratégico a veces cuando los actoresdirigen las contradicciones en las identidades de los otros.	Cambio en el comportamiento haciendo público sus fallos.
	Post- estructuralista	Discurso manifiesto en la práctica (relaciones de poder, conocimiento).	Fundamental. Discursos estables definen lo que cuenta como válido. Los Actores establecen el discurso.	Todos los actores nacen del discurso, pero los intereses pueden ser distintos, pudiendo resistirse.

Nota: Miskimonn, A. et al, p. 106, 2013; como se citó en Urra (2021).

Por otra parte, Aristóteles, en su obra "La Retórica", identificó tres pilares de la persuasión: logos, pathos y ethos[3]; los cuales han evolucionado incorporando la influencia social y las técnicas cognitivas, entre otras.

A continuación, la siguiente tabla explora las diferentes clases de persuasión aplicables a las INFOOPS, destacando su relevancia y aplicación en escenarios militares:

[3] El logos (persuasión racional), el pathos (persuasión emocional) y el ethos (persuasión ética).

Tabla 2

Tipos de persuasión según Aristóteles

Tipo de Persuasión	Descripción	Aplicación en InfoOps	Autor/Referencia
Persuasión Racional	Implica el uso de explicaciones, argumentos lógicos y presentación de evidencias basadas en hechos para influir en la persona objetivo.	En las InfoOps, la persuasión racional es clave para influir en la toma de decisiones en diferentes niveles de la conducción. Es útil en campañas de contrainformación para desactivar narrativas adversarias que carecen de sustento.	De Abreu, s.f., p.29
Persuasión Emocional	Apela a los sentimientos de la audiencia, utilizando tácticas que evocan emociones como el miedo, la esperanza, la tristeza o la alegría para influir en su comportamiento.	En las InfoOps, la manipulación emocional es decisiva en situaciones de alta tensión. Por ejemplo, imágenes impactantes en campañas de guerra psicológica pueden debilitar la moral del adversario o fortalecer la de las propias tropas.	González, 2013, p.14
Persuasión Ética	Se refiere a la utilización de tácticas persuasivas que respeten principios morales y eviten la manipulación engañosa. El Ethos, o la credibilidad, recae entonces en el emisor, y tienen que ver con su reputación o en la confianza con la que diga su discurso.	En el contexto militar, la persuasión ética es esencial para preservar la legitimidad y la moral de la fuerza militar y la comunidad internacional. Es particularmente relevante en entornos donde el respeto por los derechos humanos es primordial.	Casternao, 2022.

Nota: Elaboración propia

Además de las formas tradicionales de persuasión, existen otras estrategias que pueden mejorar la comunicación: la persuasión social se basa en la conformidad con normas grupales y la influencia de líderes para movilizar a las masas y cambiar comportamientos; la persuasión cognitiva busca modificar creencias mediante argumentos que desafían ideas previas y reconfiguran la percepción de situaciones, y finalmente, la persuasión retórica, que utiliza técnicas discursivas para hacer que conceptos complejos sean más accesibles y memorables.

3. Estrategias de Comunicación Persuasiva

En el contexto de las INFOOPS, las estrategias de comunicación

persuasiva pueden definirse como directrices que guían el uso de técnicas destinadas a influir en las PAC de una audiencia específica, que basadas en principios de la psicología social, buscarán inducir cambios en la actitud o conducta de la audiencia a través de la comunicación. Las estrategias más comunes incluyen el empleo de la reciprocidad, la validación social, la autoridad, la escasez, la consistencia, la apelación emocional; y que, empleando la psicología cognitiva y social, ayudarán a guiar decisiones y fortalecer la cohesión y moral de las fuerzas, facilitando una influencia más precisa y adaptada a los complejos escenarios de la guerra moderna.

3.1 Reciprocidad

El principio de reciprocidad es esencial en psicología y se basa en la tendencia innata de las personas a devolver favores o acciones positivas recibidas. Históricamente, la reciprocidad era crucial para la cohesión y supervivencia en comunidades. En el ámbito de las INFOOPS, este principio puede influir en las PAC de las audiencias, ayudando a moldear la opinión pública a favor de los objetivos operacionales.

Al ofrecer beneficios, asistencia o información útil, se puede generar un sentimiento de obligación que promueva mayor compromiso y cooperación. Según Cialdini (1990), “las personas que transgreden la regla de la reciprocidad al aceptar los buenos actos de los demás sin hacer nada por corresponder, no son del agrado del grupo social” (p. 47).

3.2 Influencia Social Informativa

Los seres humanos están constantemente influenciados por interacciones sociales, las cuales son fundamentales para el aprendizaje y el cambio de actitud. Según Briñol et al. (2007), como se citó en Restrepo, (2019, p. 6): "esta influencia social puede ser intencional o no, y aun así puede provocar cambios en la conducta o pensamiento del interlocutor". Aunque no siempre se refleje en la conducta observable, puede afectar comportamientos no evidentes o pensamientos.

El principio de prueba social indica que las personas tienden a basar sus juicios y decisiones en el comportamiento de otros, especialmente en situaciones de incertidumbre. La validación social se refiere a la tendencia de las personas a asumir que las acciones de otros son correctas si las observan con frecuencia (MINREL, 2019).

En INFOOPS, este principio se puede aplicar mostrando que una figura influyente o una mayoría percibida apoyan una acción o creencia. Un ejemplo es el caso de una modelo estadounidense que opinó sobre el conflicto de Armenia y Azerbaiyán en Twitter en 2020 (ver Figura 1). La influencia social puede hacer que, al ver que otros en su grupo adoptan una postura de duda, los individuos se sientan presionados a seguir ese comportamiento, afectando la moral y cohesión del equipo.

Para contrarrestar esto, es crucial gestionar la percepción pública e interna del liderazgo, con una comunicación clara y consistente sobre los líderes y las metas para mantener la unidad y el compromiso del equipo.

Figura 1

Ejemplo de influencia social informativa

Nota: The Journal.ie. (@thejournal_ire) Vía X (2020).

3.3 Autoridad Como Referente

La influencia de la autoridad ha sido ampliamente estudiada, como el experimento de Milgram (1963), donde observó que las personas estaban dispuestas a seguir órdenes de una figura de autoridad incluso si estas contradecían sus convicciones. Vásquez (2015) señala que "cuando el sujeto obedece los dictados de la autoridad, su conciencia deja de funcionar y se produce una abdicación de la responsabilidad" (p. 15).

Esto muestra que la autoridad es un principio psicológico fundamental, basado en la inclinación de las personas a confiar en expertos o líderes reconocidos.

En INFOOPS, se puede aplicar este principio citando figuras de autoridad como el General Dwight D. Eisenhower, cuyo liderazgo en la Segunda Guerra Mundial sigue inspirando confianza. Según Cialdini (2001), la presencia de una figura de autoridad puede aumentar la persuasión al aprovechar la tendencia de las personas a seguir a quienes consideran expertos o líderes.

3.4 Escasez

El principio de escasez se basa en la idea de que los recursos percibidos como limitados aumentan su atractivo y urgencia, influyendo en el comportamiento y las decisiones. Robert Cialdini (2009) afirma que "las personas tienden a valorar más aquello que perciben como escaso o exclusivo, sin importar si esta percepción refleja una realidad objetiva" (p. 34). Este principio actúa como catalizador para la toma de decisiones, respaldado por la teoría de la reactancia, que sugiere que la percepción de pérdida inminente incrementa el valor subjetivo de un recurso.

En INFOOPS, la escasez puede ser utilizada para crear una percepción de urgencia que afecte la toma de decisiones del adversario. Por ejemplo, difundir la idea de que los suministros vitales están disminuyendo rápidamente puede inducir una sensación de crisis y presión psicológica en las fuerzas enemigas, llevándolas a tomar

decisiones apresuradas y menos racionales.

Cialdini (2009) también destaca que “la percepción de escasez puede llevar a una mayor competencia por el recurso y a un incremento en su valor percibido” (p. 45). Así, la escasez puede aumentar la demanda y desestabilizar al enemigo.

3.5 Empleo de la Consistencia

El principio de consistencia es fundamental en la persuasión y se basa en la tendencia de las personas a actuar de manera coherente con sus palabras y acciones previas. Este principio se usa para persuadir a una audiencia mostrando cómo sus acciones están alineadas con sus valores y creencias anteriores.

En INFOOPS, el principio de consistencia puede ser efectivo al inducir a la audiencia a comprometerse con pequeños pasos que los alineen con el mensaje deseado. Por ejemplo, si se logra que las personas apoyen simbólicamente una causa humanitaria, es probable que se comprometan con decisiones más importantes en el futuro. Este fenómeno, conocido como el "*foot in the door*," explota la necesidad de coherencia interna de las personas.

Un ejemplo sería una campaña que pide a los residentes locales en una región de conflicto que participen en una actividad comunitaria sin implicaciones políticas. Este compromiso inicial podría hacer que los residentes estén más dispuestos a apoyar iniciativas de paz y estabilidad en el futuro. Freedman y Fraser (1966) demostraron que el "*foot in the*

door" aumenta la probabilidad de aceptar solicitudes mayores tras una petición menor. Esta técnica, si se aplica correctamente, puede mejorar significativamente la efectividad de las campañas de persuasión

3.6 Empatía y Apelación Emocional

La empatía y la apelación emocional son estrategias clave en las INFOOPS. La empatía, que implica comprender y compartir los sentimientos de los demás, busca crear una conexión emocional positiva con la audiencia. Esta es efectiva para ganar apoyo al mostrar cómo las acciones impactan en la vida de las personas.

Además, la apelación emocional, que evoca emociones como miedo, orgullo o ira, puede influir en la toma de decisiones y hacer que los mensajes sean más persuasivos y duraderos. Mensajes que destacan un peligro inminente, por ejemplo, pueden intensificar la presión emocional y favorecer los objetivos de la operación.

Un ejemplo de apelación emocional en el contexto militar se puede observar en la fotografía del rescate de un soldado herido cerca de Kandahar (Afganistán), el 24 de junio de 2010. Esta imagen (ver Figura 2), capturada por un fotógrafo de guerra; muestra a un grupo de soldados estadounidenses llevando a su compañero herido mientras se encuentran bajo fuego enemigo. La fotografía se difundió rápidamente en los medios de comunicación, evocando una respuesta emocional intensa entre el público.

Los elementos visuales de la imagen, como la expresión de

desesperación y la determinación visible en los rostros de sus compañeros, generaron una poderosa conexión emocional. Esta representación no solo humanizó la experiencia del conflicto, sino que también reforzó la imagen de los soldados como héroes dispuestos a arriesgar sus vidas por sus compañeros.

Figura 2

Soldados evacuan a un compañero herido cerca de Kandahar

Nota: El País 2022.

La interpretación de la imagen va más allá del simple registro fotográfico; se convierte en una herramienta poderosa de comunicación visual que transmite un mensaje de sacrificio y camaradería. Como resultado, la percepción pública sobre el compromiso y valor de las fuerzas armadas se ve profundamente influenciada por esta representación emocional.

Como señala Jo Adetunji (2024): “la fotografía y las formas fotográficas de ver y representar el mundo pueden convertirse en armas emocionales que cambian la percepción pública”.

Sin embargo, el uso de esta conexión conlleva ciertos riesgos, tales como el denominado “*contagio emocional*”, donde emociones intensas y negativas podrían desbordar a la audiencia, generando respuestas no deseadas, y la presencia de una sobrecarga emocional, afectando la capacidad para tomar decisiones. Para mitigar estos riesgos, se propone el concepto de ecpatía[4], como una habilidad humana, que trasciende a la empatía, la cual surge como un elemento distintivo en la comprensión y gestión de las emociones en entornos complejos, y expuestos a altos niveles de presión psicológica.

Para contextualizar la importancia de la ecpatía en el ámbito militar, es crucial diferenciarla de los conceptos: simpatía y apatía; respecto a la ecpatía, González de la Rivera[5] (2005), la propone y define como “el proceso mental de percepción y exclusión activa de los sentimientos inducidos por otros” (p.4).; centrada en fomentar una conexión emocional genuina mientras se mantienen mecanismos de control para evitar la sobrecarga emocional (ver Figura 3). Esta estrategia implica presentar información de manera que se reconozcan y validen las emociones de la audiencia, ofreciendo soluciones prácticas y

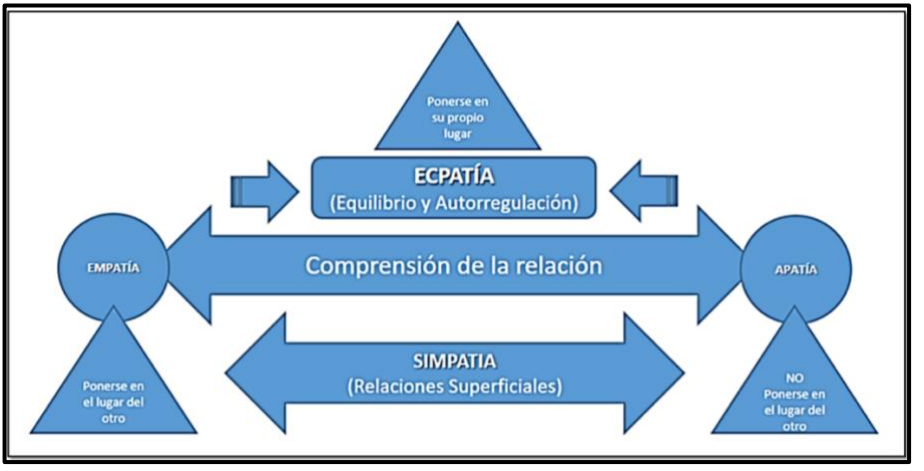
[4] Concepto tomado etimológicamente del griego ekpatheia: “sentir fuera”.

[5] José Luis González de Rivera, médico de la Universidad de Navarra y PHD en Medicina de la Universidad del País Vasco; especialista en medicina interna del Ministerio de Educación y Ciencia de España y especialista en psiquiatría por el Royal College of Physicians de Canadá.

equilibradas que prevengan el impacto negativo del contagio emocional.

Figura 3

Dinámica de las relaciones



Nota: Elaboración propia.

Lo anterior respaldado en las palabras de García (2023), quien describe la ecpatía como "la capacidad de separarse de los sentimientos ajenos, no dejándolos de comprender, sino como resultado de una acción voluntaria que se dirige a evitar el ‘contagio o la inundación emocional’ para esta que no pueda desbordarnos" (p. 5).

4. Estrategias Para el Cambio de Percepciones

En el ámbito de las INFOOPS, el cambio de percepciones juega un papel crucial en la configuración de la realidad e influencia. En la literatura se identifican una serie de técnicas de manipulación de la información empleadas para modificar cómo se perciben los eventos y las intenciones; entre estas estrategias se encuentran:

4.1 El contagio emocional

El contagio emocional se manifiesta como un fenómeno significativo que influye en las PAC, este proceso ocurre cuando las emociones negativas[6], se propagan entre los individuos, afectando su estado emocional y su respuesta a la información recibida; por lo tanto, el contagio emocional podría tener efectos perjudiciales, cuando se presenta en contextos críticos, como una crisis o conflicto.

Es fundamental señalar que, las RR.SS. juegan un rol esencial en las INFOOPS, destacándose como una herramienta clave en la comunicación persuasiva; especialmente mediante esta técnica, transformando la manera en que las organizaciones se comunican con sus públicos objetivo, permitiendo una interacción más directa e inmediata. En el contexto de las INFOOPS, las RR.SS. funcionan como un canal potente para influir en las PAC, facilitando el alcance a una audiencia amplia y segmentada de manera rápida y efectiva; al respecto, las entidades involucradas en INFOOPS podrían utilizar estas redes para difundir mensajes estratégicos, promover campañas de influencia y construir relaciones con el público.

Además, "las redes sociales ofrecen una comunicación más personalizada, lo que facilita el desarrollo de estrategias de persuasión adaptadas a las necesidades y preferencias específicas de cada audiencia" (Becerra et al, 2022, como se citó en Egido, 2023, p. 354). Un ejemplo de contagio emocional se puede observar en las estrategias desplegadas

[6] Miedo o ansiedad.

por usuarios de RR.SS. en el contexto del conflicto entre Israel-Hamas; donde han publicado mensajes (posts) diseñados para provocar un impacto emocional en la audiencia, con el objetivo de inclinar su apoyo hacia Israel, en este caso particular (ver Figura 4).

Estas estrategias aprovechan el contagio emocional al transmitir mensajes cargados de contenido que buscan generar respuestas emotivas, con el fin de influir en la percepción de los individuos con una de las partes en conflicto.

Figura 4

Ejemplos de contagio emocional en redes sociales

Nota: Cuenta de Twitter: Israel en español (2023).

En este orden de ideas, Charpentier (2020), señala que el contagio emocional se vuelve nocivo cuando una persona en un grupo cae en desesperación, afectando a todos a su alrededor.

La Tabla 3 presenta estrategias importantes a considerar con el objetivo de contrarrestar la propagación de emociones negativas en el contexto de las INFOOPS:

Tabla 3

Estrategias psicológicas

Estrategia Psicológica	Descripción	Aplicación en InfoOps
Reestructuración Cognitiva	Modificar la forma en que se interpretan los eventos para cambiar percepciones pesimistas y reducir el impacto negativo de las emociones.	Presentar la información de manera que fomente una reevaluación positiva de la situación.
Cambio Atencional	Desviar la atención hacia aspectos positivos o hacia otras áreas de interés para reducir el impacto del contagio emocional.	Enfocar los mensajes en logros y soluciones en lugar de problemas.
Motivación a través del otro	Considerar el impacto emocional en los demás para incentivar una actitud más positiva y constructiva.	Diseñar mensajes que promuevan el bienestar colectivo y el apoyo mutuo.

Nota: Elaboración propia

En definitiva, las RR.SS. amplifican la capacidad de moldear la percepción y el comportamiento en situaciones de alta tensión, lo que puede ser una ventaja o un desafío, y para manejar el impacto emocional y mantener el control informativo, será esencial diseñar estrategias como la reestructuración cognitiva, el cambio atencional y la motivación positiva, lo que ayuda a mitigar efectos adversos y optimizar la efectividad de las INFOOPS.

4.2 El Gaslighting

El término se refiere a una forma de manipulación psicológica que

provoca que una persona dude de su percepción, memoria o juicio. En el contexto de las INFOOPS, se utiliza como una estrategia compleja para desorientar y manipular al adversario distorsionando su percepción de la realidad, y siendo ampliamente discutido en la literatura. Stern (2007) señala que el carácter insidioso de esta táctica: "*es capaz de erosionar profundamente la percepción de la realidad y la confianza en sí mismo*" (Stern, 2007, como se citó en Rosero, 2023); agregando que el gaslighting opera como una forma de abuso emocional para socavar la capacidad de respuesta al generar dudas sobre las propias percepciones. Este análisis es complementado por Abramson (2014), quien señala que esta forma de manipulación "*no tiene necesariamente el objetivo de llevar a la víctima a la locura, sino tan solo generar la suficiente inestabilidad mental como para que el agresor mantenga su posición de poder y control*" (Abramson, 2014, como se citó en Rosero, 2023).

Al respecto, la BBC (2017) señala que la técnica de gaslighting se estructura en tres etapas clave para su implementación: idealización, devaluación y descarte, siendo diseñadas para manipular y controlar la percepción de la víctima.

En la Tabla 4, se presentan estas etapas, adaptadas al ámbito de las INFOOPS, destacando cómo se utilizan para influir y desestabilizar al adversario, al tiempo que se manipula la percepción pública y se mantiene el control narrativo:

Tabla 4

Etapas del Gaslighting en el contexto de las INFOOPS

Etapa	Descripción General	Tácticas Comunes en InfoOps	Objetivo Principal en InfoOps
Idealización	En esta etapa, la víctima "pierde la cabeza" por el manipulador, quien proyecta una imagen de sí mismo como el aliado o fuente de información perfecta. La narrativa se presenta de manera tan convincente que la víctima comienza a confiar plenamente en ella.	- Difusión de información positiva sobre un líder o ideología - Presentación de soluciones aparentemente perfectas a problemas complejos - Creación de una narrativa unificadora que apela a los deseos y miedos de la audiencia	Ganarse la confianza y lealtad del público objetivo, estableciendo una dependencia en la narrativa o fuente de información presentada.
Devaluación	La fase de devaluación "golpea fuerte": la víctima, que antes era adorada y valorada, ahora es incapaz de hacer algo bien según el manipulador. Después de haber probado el ideal, la víctima está desesperada por recuperar la aprobación y confianza.	- Introducción de dudas sobre la capacidad y legitimidad del liderazgo enemigo - Críticas constantes y campañas de desprestigio - Manipulación de hechos para mostrar al enemigo como incompetente o malintencionado	Generar confusión, reducir la moral y la cohesión del enemigo, y hacer que el público objetivo dependa de la narrativa del manipulador para obtener validación y seguridad.
Descarte	En la etapa final de descarte, la víctima es abandonada o minimizada cuando ya no es útil. En las operaciones de información, esto sucede a menudo simultáneamente con la fase de idealización de una nueva víctima o grupo objetivo.	- Abandono de aliados o figuras previamente exaltadas - Cambiar la narrativa para centrarse en un nuevo objetivo o amenaza - Desvío de la atención hacia nuevos frentes de conflicto o distracciones	Deshacerse de los elementos o narrativas que ya no son útiles, mientras se redirige la atención hacia nuevos objetivos o amenazas, manteniendo el control sobre la percepción pública.

Nota: Elaboración propia

El análisis de estas perspectivas revela la versatilidad del gaslighting en el ámbito militar, donde su aplicación puede tener un impacto significativo, por ello es crucial conocer los diversos métodos para contrarrestar estas tácticas manipulativas. Entre las más relevantes se encuentran:

4.2.1 Generación de Dudas Constantes Sobre Ideas y Acciones Propias: Empleada para inducir dudas persistentes en los individuos sobre sus propias ideas y acciones; manipulando la percepción de la realidad, y buscando erosionar la confianza en el propio juicio, provocando que la víctima cuestione continuamente la validez de sus decisiones.

Esta técnica permite desestabilizar al adversario, haciéndolo dudar de sus estrategias y acciones, lo que lleva a una parálisis decisional reduciendo así su eficacia. Por ejemplo, podrían enviar mensajes falsos que sugieran que un reciente ataque fue un desastre, incluso si en realidad fue un éxito; esto podría llevar a la fuerza militar a dudar de la validez de todas sus decisiones anteriores, lo que podría resultar en una disminución de la confianza en sus propias habilidades y en las órdenes de sus superiores.

4.2.2 Generar Sensibilidad Excesiva a las Críticas: El gaslighting puede ser una herramienta poderosa para explotar la sensibilidad excesiva a las críticas, amplificando la susceptibilidad de un individuo, generando dudas constantes sobre sus propias capacidades y decisiones; al enfatizar de manera manipuladora fallos o errores, incluso cuando son mínimos o inexistentes, el gaslighting induce una percepción distorsionada en la víctima, haciéndola cada vez más vulnerable a la autocrítica y menos segura de su juicio; en un contexto militar, esta estrategia puede erosionar la confianza de los líderes en sus habilidades.

Un ejemplo de gaslighting orientado a explotar la sensibilidad excesiva a las críticas podría involucrar la "*manipulación*" de informes para destacar de manera desproporcionada errores tácticos menores cometidos por comandantes en el campo. Estos informes, distribuidos deliberadamente entre los mandos, podrían sugerir que tales errores son síntomas de una incompetencia más profunda. Esta estrategia no solo aumentaría la autocrítica entre los líderes, sembrando dudas sobre su capacidad de mando, lo que puede llevar a una toma de decisiones

vacilante y a la pérdida de confianza en sus propias habilidades; a nivel operacional, esta erosión de la confianza puede afectar la toma de decisiones, donde los líderes se vuelven excesivamente cautelosos, evitan asumir riesgos innecesarios, llegando a depender de la aprobación de superiores, comprometiendo la eficacia de las operaciones militares.

4.2.3 Ocultación de Información: La ocultación de información se convierte en un problema crítico cuando al percibir la manipulación constante de información por parte del adversario, se comienza a retener o distorsionar dicha información. Este comportamiento puede surgir del temor a ser cuestionados de incompetencia. Por ejemplo, en un escenario donde la información es continuamente distorsionada por el enemigo, los miembros de una unidad podrían optar por no informar detalles relevantes a sus superiores, preocupados por las repercusiones de actuar sobre datos potencialmente falsos; el impacto de esta conducta puede ser perjudicial dado que la falta de comunicación dentro de la unidad, comprometería la efectividad y la toma de decisiones en situaciones críticas.

4.2.4 Dificultad Para Tomar Decisiones: La dificultad para tomar decisiones es una manifestación común de la manipulación de información, donde la continua distorsión de datos podría socavar la confianza de la fuerza militar en su propio juicio. Esta situación podría llevar a la fuerza a dudar incluso en decisiones básicas, como identificar el momento adecuado para abrir fuego, por temor a que sus percepciones estén erradas debido a la desinformación; en un entorno donde la información es constantemente manipulada, la duda en torno a

decisiones fundamentales puede paralizar la capacidad de reacción. Al respecto, el impacto de esta falta de confianza será crítica, dado que la incapacidad para tomar decisiones oportunas y precisas podrían llegar a comprometer la efectividad en situaciones donde la rapidez y la certeza son esenciales para el éxito.

4.2.5 Generar un Sentimiento de Ineptitud: Generar un sentimiento de ineptitud es una táctica donde la manipulación constante podría llevar a que los soldados se perciban a sí mismos como incompetentes, a pesar de sus verdaderos esfuerzos. Por ejemplo, si los soldados reciben información falsa que sugiere que sus esfuerzos están fallando, podrían comenzar a cuestionar su capacidad para cumplir con éxito sus objetivos; este sentimiento de ineptitud podría además erosionar su confianza y moral, llevando a una disminución de la motivación y la voluntad para actuar, al considerar que sus esfuerzos son en vano. Como resultado, la cohesión y la eficacia de la unidad podrían verse comprometidas, afectando el desempeño en el campo de batalla.

4.3 El empleo de Fake News

En la actualidad, la proliferación de información errónea persistirá debido al fácil acceso a una abundancia de recursos y a la utilización del híper enfoque en los mensajes, factores que obstaculizan la verificación de fuentes, autores, origen, medios de difusión, impacto y credibilidad de la información. El grupo de investigación Tandoc Et Al (2018) ha identificado en la literatura seis categorías de noticias falsas, las cuales se presentan en la siguiente tabla:

Tabla 5

Estrategias de desinformación en contextos militares

Estrategia de Desinformación	Descripción	Ejemplo en InfoOps en Operaciones Militares
Sátira	Uso de elementos de humor o exageración para ridiculizar o criticar un tema o entidad.	Creación de un video humorístico que exagera las debilidades del adversario para desmoralizar a sus seguidores.
Parodia	Similar a la sátira, pero utiliza información no objetiva para inyectar humor y ridiculizar.	Publicación de un falso discurso en redes sociales, modificando sus palabras para hacer que un lider parezca incompetente o ridículo.
Fabricación	Creación de noticias sin base objetiva pero presentadas en formato de noticias legítimas para aparentar veracidad.	Difusión de un informe falso respecto a una supuesta victoria militar del adversario, utilizando gráficos y formatos de noticias oficiales para engañar al público.
Manipulación	Adulteración de noticias visuales para distorsionar la realidad.	Alteración de imágenes de una fuerza enemiga para hacer que parezcan estar cometiendo actos de brutalidad, con el fin de socavar su legitimidad.
Publicidad	Promoción de un producto, empresa o idea, generalmente con fines comerciales.	Utilización de anuncios en medios digitales que promueven la narrativa de una intervención militar como una operación de paz, para ganar apoyo internacional.
Propaganda	Información creada por entidades políticas para influir en las percepciones públicas.	Difusión de mensajes a través de medios estatales que justifiquen las acciones de las propias fuerzas armadas para mantener el apoyo popular.

Nota: Elaboración propia

La viabilidad de estas categorías se analiza en función de los hechos; por ejemplo, la sátira presenta ciertas desviaciones, mientras que las parodias y las noticias fabricadas incorporan un amplio contexto social que se confunde con la ficción (Tandoc et al. 2018).

Las INFOOPS han evolucionado a lo largo del tiempo, siendo actualmente las acciones más prominentes en la conflictividad moderna. Con la globalización, se ha consolidado la conexión directa con casi toda la población, llegando directamente al usuario final, reflejándose en la denominada "*dimensión de la información*"; empleando diferentes canales de comunicación para influir en la moral, siendo la propaganda una de sus principales tácticas; la cual actualmente digitalizada, ha aprovechado las RRSS para mejorar su rendimiento en términos de

impacto y masificación de contenido.

Por ejemplo, X (otrora Twitter), que surge como una plataforma a través de la emisión de mensajes que pueden llegar a millones de personas de manera instantánea, generando interacciones que permiten construir redes con el objetivo de difundir contenidos persuasivos.

No obstante, también se ha observado el surgimiento de las "fake news", que buscan propagar mensajes con objetivos mayormente políticos; tal es el caso de la difusión de un vídeo en la red social X “en el que varios niños aparecían en el interior de una jaula (ver Figura 4), bajo el título ‘*Niños israelíes cautivos en Gaza*’, haciendo referencia a la toma de rehenes perpetrada por Hamás. No obstante, esta información es falsa” (Badillo, 2023).

Figura 4

Ejemplo de Fake News: Niños israelíes cautivos en Gaza

Nota: Cuenta de Twitter de Dani Lerer (@danilerer)

Al respecto, se puede evidenciar que la plataforma X presenta una doble faceta: por un lado, es utilizada como una herramienta de propaganda moderna, aprovechando la expansión del mensaje en el ámbito internacional o nacional, según el objetivo estratégico y, por otro, "adopta características de una Oficina de Información Pública (PIO), especialmente en las cuentas oficiales de autoridades o líderes de opinión, quienes aspiran a mantener una línea comunicacional clara y contrarrestar el efecto de la propaganda y las fake news" (Cesim, 2022).

Este fenómeno se ha evidenciado durante la guerra ruso-ucraniana, donde las partes involucradas han utilizado X para expandir sus mensajes y acciones político/diplomáticas, ya sea apelando al público occidental o nacional, según sus objetivos estratégicos. En el contexto contemporáneo, el uso de RRSS se ha convertido en un activo estratégico para las operaciones de información, marcando la evolución de la guerra psicológica desde los panfletos hasta los contenidos digitales, llegando a la mente de miles de usuarios en cualquier momento y lugar.

En última instancia, la esencia de la '*guerra psicológica*' persiste, pero la consolidación del multidominio y las tecnologías han permitido expandir en tiempo, presencia y precisión las herramientas para el desarrollo de INFOOPS, desafiando los límites de lo posible según la imaginación de quienes las conducen. Según Deutsche Welle (2023), el conflicto entre Israel y Hamás ha estado marcado por una ola de desinformación en línea, siendo necesario contar con herramientas para distinguir lo que es verdad y lo que es falso. Un ejemplo de esto lo encontramos en la "*Operación Espadas de Acero*", la cual se presenta como una respuesta militar que utiliza los diversos dominios y dimensiones de la guerra moderna, con especial atención al subsuelo, donde se sabe que Hamás opera a través de túneles.

El énfasis en la dimensión de la información subraya la relevancia de la percepción pública y la narrativa para el éxito de una operación militar; al respecto, se puede evidenciar que:

> “La guerra de la información tendrá un papel clave, ya se ha visto como Hamás utilizó redes sociales para visibilizar sus acciones, al mismo tiempo Israel hace lo propio configurando su escenario, dando a conocer lo violento que será su operación, con daño a civiles y que será consecuencia de lo que sucede, finalmente busca también el apoyo internacional y justificar su acción” (Provis, 2023, p. 4).

En este ámbito, se observa que la propagación de falsificaciones suscita indignación, donde la información falsa puede ser controvertida y perturbadora, contando con un potencial para generar emociones como ira y tristeza, lo que podría influir en las posturas adoptadas respecto al conflicto; reconociéndose que las “*fake news*” son particularmente efectivas cuando despiertan emociones fuertes.

El psicólogo Lewandowsky señaló: “las noticias falsas tienden a generar indignación en el receptor”, agregando, "…y sabemos que la gente, le guste o no, interactúa con información que provoca indignación, eso hace que sea más probable que se vuelvan virales" (Lewandowsky, 2023, como se citó en Gorrión, 2023). Para abordar este fenómeno, será crucial aplicar un enfoque cauteloso al acceder a la información; algunas preguntas claves que podrían ayudar a evaluar su veracidad incluyen: ¿cómo afecta emocionalmente este contenido?, ¿refuerza mis puntos de vista?, ¿quién podría beneficiarse al difundir esta historia y por qué?,

¿existen indicios de un origen dudoso?

En tiempos de guerra, las RRSS y los motores de búsqueda han dificultado la verificación de la información y debilitado el vínculo con fuentes confiables, por lo que es crucial examinar la fuente, verificar cuentas y buscar información adicional para detectar sesgos. Las búsquedas inversas pueden ayudar a rastrear el origen de imágenes manipuladas, y el análisis crítico es esencial para evitar la propagación de información engañosa en estos contextos.

5. Las Características Para una Influencia Eficaz

La influencia eficaz es un tema central en la psicología social; al respecto, diversos estudios han identificado una serie de características clave[7]que facilitan la influencia sobre individuos y audiencias. Las más relevantes se encuentran definidas en la siguiente tabla:

[7] La credibilidad, la relevancia del mensaje, la claridad y simplicidad, la repetición y la apelación emocional.

Tabla 6

Factores Claves de la Persuasión en las Operaciones de Información (INFOOPS)

Factor de Persuasión	Descripción	Aplicación en InfoOps
Credibilidad	Se basa en la competencia y la confiabilidad. Una fuente percibida como competente y confiable es más capaz de persuadir a su audiencia.	Establece una base sólida para la persuasión, facilitando la aceptación del mensaje.
Relevancia del Mensaje	Se refiere a su capacidad para resonar con las necesidades, intereses y preocupaciones de la audiencia, aumentando su motivación para procesarlo.	La relevancia asegura que el mensaje capte la atención e interés de la audiencia, incrementando su impacto persuasivo.
Claridad y Simplicidad	Los mensajes claros y directos son más persuasivos porque reducen la carga cognitiva, permitiendo que el mensaje sea fácilmente procesado y recordado.	Mensajes claros y bien estructurados son más efectivos para comunicar ideas, aumentando la probabilidad de aceptación por parte de la audiencia.
Repetición	La repetición aumenta la familiaridad y la preferencia por el mensaje a través del efecto de mera exposición, aunque el exceso puede causar saturación.	Refuerza el mensaje, aumentando la probabilidad de que sea recordado y aceptado, pero debe ser utilizada con moderación para evitar efectos negativos.
Apelación Emocional	Los mensajes que evocan emociones, especialmente positivas, pueden aumentar la receptividad hacia el mensaje, pero deben manejarse con cuidado para evitar manipulaciones.	Las emociones intensas influyen en la percepción y aceptación de los mensajes, siendo una herramienta poderosa en la persuasión si se utiliza de manera ética y efectiva.

Nota: Elaboración propia

Aunque estas características son fundamentales, su aplicación deberá ser evaluada en función del contexto y audiencia. En consecuencia, su credibilidad permitirá establecer una base sólida para la persuasión, mientras que la claridad y simplicidad asegurará que el mensaje sea accesible. Por su parte, la repetición y la apelación emocional podrían amplificar el impacto del mensaje; no obstante, su uso deberá ser equilibrado para evitar efectos adversos como la saturación o la manipulación.

5.1 Requisitos y limitaciones para influir

Para que la influencia sea efectiva, será fundamental comprender las características del mensaje y el perfil de la audiencia a quien va dirigida; lo que permitirá adaptar la comunicación a las necesidades, intereses y valores de los receptores, aumentando la probabilidad de que el mensaje sea recibido positivamente. La tabla 7 presenta los requisitos fundamentales para lograr una efectiva capacidad de influencia:

Tabla 7

Pilares fundamentales para influencia efectiva en el contexto de las INFOOPS

Factor de Influencia	Descripción	Aplicación en la Influencia	Fuente
Conocimiento de la Audiencia	Un conocimiento profundo de la audiencia permite crear mensajes ajustados a sus intereses y preocupaciones, aumentando la relevancia y efectividad de la persuasión.	Adaptar el mensaje a las características específicas del receptor facilita la conexión con la audiencia, aumentando la probabilidad de que el mensaje sea persuasivo.	Petty y Cacioppo (1986); Krosnick y Petty (1995)
Consistencia y Adaptabilidad	La consistencia en el mensaje refuerza la credibilidad, mientras que la adaptabilidad permite ajustar el mensaje según la retroalimentación y el contexto cambiante.	Mantener la coherencia entre las palabras y las acciones refuerza la percepción de autenticidad, mientras que la adaptabilidad asegura que la influencia se mantenga relevante y efectiva.	Cialdini (2009)
Ética en la Influencia	Actuar de manera ética en la comunicación protege la dignidad de la audiencia y fomenta relaciones de confianza a largo plazo.	La influencia basada en principios éticos es más aceptada y respetada, reduciendo el riesgo de rechazo o resistencia por parte de la audiencia, y promoviendo una influencia sostenible.	Beauchamp y Childress (2001)

Nota: Elaboración propia

Sin embargo, a pesar de estos principios, existen diversas limitaciones (Tabla 8) que derivan de diferentes teorías psicológicas y que podrían afectar la capacidad de influencia:

Tabla 8

Limitaciones en el proceso de influencia

Limitación	Descripción	Teorías/Autores	Relación con InfoOps	Ejemplo en InfoOps
Resistencia del Receptor	Las personas tienden a resistir la influencia cuando perciben el mensaje como una amenaza a sus creencias o valores preexistentes.	**Teoría de la Resistencia Psicológica - Brehm (1966)**; Petty y Cacioppo (1986)	En InfoOps, los adversarios o la población objetivo pueden resistir la influencia si el mensaje va en contra de sus creencias profundas o su cultura.	En una operación militar, si se intenta influir en una comunidad con fuertes creencias religiosas, un mensaje que contradice esas creencias podría ser rechazado automáticamente.
Sobrecarga de Información	La exposición a grandes cantidades de información puede reducir la capacidad de procesamiento y la efectividad de la influencia.	**Teoría de la Sobrecarga de Información - Alvin Toffler (1970); Teoría del Procesamiento de la Información - Miller (1956)**; Epstein (1996)	Durante las InfoOps, una sobrecarga de información puede saturar a la audiencia, dificultando que los mensajes clave se asimilen y tengan el impacto deseado.	En una campaña de desinformación, inundar las redes con información contradictoria puede confundir a la población, haciendo que ignoren todos los mensajes, incluidos los correctos.
Desconfianza	La percepción de que el mensaje es sesgado o manipulado puede reducir su impacto y crear barreras perceptuales que dificultan la persuasión.	**Teoría de la Atribución - Heider (1958); Teoría de la Credibilidad de la Fuente - Hovland & Weiss (1951)**; Gillespie y A. N. A. (2015)	La desconfianza en la fuente de información es un desafío crítico en InfoOps, donde la credibilidad de la fuente es clave para la aceptación del mensaje.	En una misión de estabilización, si la población no confía en las fuerzas militares, los mensajes destinados a ganar su apoyo pueden ser ignorados o rechazados por completo.
Factores Individuales	Las diferencias individuales, como la personalidad y las experiencias previas, influyen en cómo se recibe y procesa un mensaje, afectando la efectividad de la influencia.	**Teoría del Autoconcepto - Rogers (1951); Teoría de la Comunicación Interpersonal - Berger & Calabrese (1975)**; Funder (2001)	En InfoOps, los mensajes deben ser adaptados a las características individuales del público objetivo para maximizar su efectividad y evitar interpretaciones erróneas.	En una campaña de influencia dirigida a líderes locales, tener en cuenta su historia personal y sus motivaciones puede determinar el éxito o fracaso de la operación.
Tiempo y Medio de Comunicación	El tiempo y el canal de comunicación elegido son cruciales para captar la atención del público y asegurar que el mensaje tenga el impacto deseado.	**Teoría de la Media Rica - Daft & Lengel (1986); Teoría del Framing - Goffman (1974)**; Thurlow, Lengel y Tomic (2004)	Seleccionar el momento y medio adecuados en InfoOps es vital para que el mensaje llegue de manera efectiva a la audiencia, considerando el contexto operativo y la situación actual.	Durante una crisis, un mensaje difundido a través de redes sociales en tiempo real puede ser más efectivo que un comunicado oficial que tarda horas en ser publicado por los medios.

Nota: Elaboración propia

Por lo tanto, para lograr una influencia eficaz, será indispensable un entendimiento profundo de la audiencia, mantener la consistencia y adaptabilidad en la comunicación, y actuar de manera ética.

No obstante, las limitaciones[8] podrían afectar la efectividad de la influencia; siendo necesario, diseñar estrategias de comunicación persuasiva que sean tanto impactantes como respetuosas.

6. Consideraciones Éticas en el Ámbito de las INFOOPS

En las INFOOPS, la dimensión humana es esencial cuando se emplean enfoques psicológicos centrados en la comunicación y la persuasión. Estas operaciones buscan alterar las PAC tanto de fuerzas adversarias como aliadas, afectando la moral, la cohesión y la legitimidad ante la opinión pública; sin embargo, el uso de técnicas de persuasión plantea dilemas éticos importantes.

El uso de técnicas de manipulación y persuasión puede plantear problemas éticos significativos, como la explotación de vulnerabilidades psicológicas o la difusión de información engañosa, las cuales pueden dañar los objetivos de la operación y la credibilidad de las fuerzas involucradas. Por lo tanto, es esencial aplicar principios éticos: la proporcionalidad exige que las operaciones eviten causar daño innecesario; la necesidad indica que solo se deben usar técnicas intrusivas cuando no haya alternativas; y la transparencia es clave para mantener la confianza pública e internacional, alineada con el Derecho Internacional de los Conflictos Armados (DICA).

Por otra parte, el gaslighting y la desinformación, aunque pueden

[8] Resistencia del receptor, la sobrecarga de información, la desconfianza, los factores individuales y las consideraciones sobre el tiempo y el medio de comunicación.

ser herramientas efectivas, conllevan riesgos como la erosión de la confianza, afectando negativamente la moral de la población. Estas técnicas deben ser manejadas con extremo cuidado para evitar efectos adversos que superen los beneficios estratégicos.

Así también, la empatía, cuando se usa éticamente, puede ser una herramienta poderosa en la persuasión; reconocer y validar las emociones del público sin exacerbarlas destructivamente es esencial para una influencia responsable. Además, el contagio emocional en las redes sociales debe ser manejado cuidadosamente para evitar impactos negativos en la salud mental y el bienestar de la población.

La propagación de noticias falsas en redes sociales plantea desafíos éticos, ya que compromete la confianza en los medios. Las INFOOPS deben basarse en la veracidad y honestidad para no manipular negativamente la percepción pública. En consecuencia, seguir principios éticos permitirá asegurar que la persuasión respete la dignidad de la audiencia, alineándose con los valores del DICA y promoviendo una comunicación responsable.

Conclusiones

El presente capítulo subraya la importancia de integrar principios psicológicos en las INFOOPS para potenciar su efectividad en los conflictos contemporáneos; el trabajo revela cómo la gestión y el control de la información se han transformado en componentes estratégicos esenciales en las operaciones militares, capaces de impactar tanto en el adversario como en las propias tropas.

Derivado de lo anterior, integrar enfoques psicológicos como la comunicación, la influencia y la persuasión no solo permitirá facilitar la modificación de PAC, sino que también fortalecer la cohesión y moral interna, proporcionando una ventaja estratégica significativa.

La eficacia de estas operaciones dependerá en gran medida de la comprensión de las dinámicas psicológicas[9] y sociales, las cuales deberán ser cuidadosamente consideradas para superar las resistencias inherentes al ser humano ante la manipulación informativa.

Así también, el uso de diferentes formas de persuasión[10], amplía la capacidad de las INFOOPS para impactar en diversas PAC, adaptándose a distintos contextos y audiencias; en un entorno cada vez más digitalizado, la correcta aplicación de estos principios será fundamental para mantener la eficacia y cohesión de las propias fuerzas, y evitar ser influenciados por el adversario.

Por otra parte, es imperativo abordar los dilemas éticos asociados a estas operaciones, asegurando que su implementación se guíe por un marco ético riguroso que respete los principios fundamentales de conducta militar. Por lo tanto, se puede concluir que el enfoque psicológico será esencial para el éxito de las INFOOPS en el combate moderno, integrando de manera estratégica comunicación, influencia y persuasión en todos los niveles de la conducción militar.

En consecuencia, para avanzar en este campo, se recomienda

[9] La reactancia psicológica, la disonancia cognitiva y teoría de la inoculación.
[10] Racional, emocional, social, cognitiva y retórica.

investigar el impacto ético de las técnicas de influencia y persuasión, explorando cómo aplicarlas de manera que respeten los derechos humanos y el DICA, manteniendo un equilibrio entre efectividad y responsabilidad. Además, será necesario analizar en profundidad, cómo las nuevas tecnologías influyen en las dinámicas de influencia en las INFOOPS, para poder adaptar estrategias psicológicas a los entornos digitales emergentes.

Asimismo, se deberá profundizar en las técnicas para superar la resistencia del público a los cambios significativos en PAC, siendo importante investigar cómo gestionar la disonancia cognitiva y facilitar la aceptación de nuevas ideas. La evaluación de la credibilidad de las fuentes y la adaptabilidad de los mensajes también es necesario, permitiendo ajustar las estrategias de influencia en respuesta a la retroalimentación y cambios contextuales.

Referencias Bibliográficas

Adetunji J. (2024). *Por qué la fotografía de Evan Vucci del atentado contra Trump es tan impactante.* The Conversación. Recuperado de: https://theconversation.com/por-que-la-fotografia-de-evan-vucci-del-atentado-contra-trump-es-tan-impactante-234704

Alfaro K.; Estrada A.; Saavedra V. (2020). *Disinformation y Misinformation, Posverdad y Fake News*: *precisiones conceptuales, diferencias, similitudes y yuxtaposiciones. Información, cultura y sociedad*: revista del Instituto de Investigaciones Bibliotecológicas, núm. 42. Universidad de Buenos Aires. Recuperado de: https://www.redalyc.org/journal/2630/263062301010/html/

American Presidents (2024). *Conociendo a los Presidentes: Dwight D. Eisenhower*. Recuperado de: https://americaspresidents.si.edu/es/research/object-groups/conociendo-a-los-presidentes-dwight-d-eisenhower

Badillo R. (2023). *Fotos manipuladas y falsos comunicados: estos son los 'fakes' de Israel y Palestina*. El confidencial/Tecnología; Titania Compañía Editorial, S.L. España. Recuperado de: https://www.elconfidencial.com/tecnologia/2023-10-09/fakes-redes-sociales-israel-hamas_3750945/

BBC Mundo (2017). *Gaslighting: el peligroso encanto del abusador que te llena de culpas y te hace dudar de tu cordura.* Mundo, Institucional. British Broadcasting Corporation. Recuperado de: https://www.bbc.com/mundo/institucional-36400007

Brehm, J. (1966). *A Theory of Psychological Reactance*. Academic Press.

Cambridge Dictionary. (2018). *Misinformation*. Recuperado de: https://dictionary.cambridge.org/es/diccionario/ingles/misinformation

Casternao A. (2022). *Ethos, Pathos y Logos: Los tres tipos de persuasión según Aristóteles.* SERCA. Instituto de altos estudios especializados. Blog de Instituto Serca. Centro Especializado en Formación de Posgrado en Psicología, Educación, Logopedia y Trabajo Social. Recuperado de: https://blog.institutoserca.com/ethos-pathos-logos-tipos-de-persuasion/#:~:text=Seg%C3%BAn%20Arist%C3%B3teles%2C%20para%20que%20un,%3A%20Ethos%2C%20Pathos%20y%20Logos

Centro de Estudios e Investigaciones Militares (CESIM) (2022). *El empleo de Redes Sociales en Operaciones de Información.* https://www.infodefensa.com/texto-diario/mostrar/3927936/empleo-redes-sociales-operaciones-informacion

Cialdini, R., (1990). *Influencia: Ciencia y Práctica. Cuáles son los factores determinantes para que una persona diga si a otra. (3ra Ed.).* Barcelona: EBOOK. Recuperado de: https://revolucionesmlm.wordpress.com/wp-content/uploads/2014/07/robert-caldini-influencia-ciencia-y-practica.pdf

Cialdini, R. (2009). *Influence: The Psychology of Persuasion.* Harper Collins E-Books. Recuperado de: https://ia800203.us.archive.org/33/items/ThePsychologyOfPersuasion/The%20Psychology%20of%20Persuasion.pdf

Clark B. (2010). *Las operaciones de información como elemento disuasivo para el conflicto armado.* Military Review Sept-Oct. 2010. Recuperado de: https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20101031_art004SPA.pdf

Charpentier D. (2020). *Contagio emocional: expertos explican en qué consiste y cómo evitarlo.* Comunicado de Prensa. Sociedad; Bio Bio Chile. Recuperado de: https://www.biobiochile.cl/noticias/sociedad/cuerpo-y-mente/2020/04/17/contagio-emocional-expertos-explican-en-que-consiste-y-como-evitarlo.shtml

Dani Lerer [@danilerer]. (2023 octubre 08). *Para los que preguntan, el video de los niños en jaulas no es de niños israelíes en poder de Hamás*. [Tweet]. Recuperado de: https://x.com/danilerer/status/1711096335082881247

De Abreu (s.f.) *Tácticas de influencia y su impacto en la efectividad del líder en educación superior*. Universidad Central de Venezuela. Facultad de Humanidades y Educación. Dirección de estudios de postgrado. Tesis de maestría en psicología de la instrucción. Recuperado de: http://saber.ucv.ve/bitstream/10872/3619/1/T026800003817-0-10DeAbreuDaniel-000.pdf

Egido M. (2023). *La comunicación persuasiva como estrategia de neurocomunicación para las relaciones públicas.* MHJournal Vol. 14 (2); artículo Nº14 (225) - mhjournal.org. Recuperado de: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-49112018000200185

Freedman, J.; & Fraser, S. (1966). C*ompliance Without Pressure: The Foot-in-the-Door Technique.* Journal of Personality and Social Psychology. Recuperado de: https://www.bulidomics.com/w/images/6/6c/Freedman_fraser_footinthedoor_jpsp1966.pdf

García E. (2023). *Que es ser una persona esponja, y porque necesito desarrollar ecpatía*. Centro Psicológico de Madrid (CESPIM). Recuperado de: https://www.psicologiamadrid.es/que-es-ser-una-persona-esponja-y-porque-necesito-desarrollar-ecpatia/#:~:text=El%20exceso%20de%20empat%C3%ADa%20o,empapan%20de%20la%20emocionalidad%20ajena

González L. (2005). *Empatía y Ecpatía. Avances en Salud Mental Relacional* Vol.4, núm. 2 - Julio 2005. Fundación OMIE. Revista Internacional On-line. Recuperado de: https://luisderivera.com/wp-content/uploads/2012/02/ecpatia.pdf

González C. (2013). *Persuasión y credibilidad de marca*. Universidad Abierta Latinoamericana. Facultad de Publicidad. Buenos Aires, Argentina. Recuperado de: https://imgbiblio.vaneduc.edu.ar/fulltext/files/TC113928.pdf

Gorrión T. (2023). *Cómo detectar noticias falsas durante la guerra entre Israel y Hamas*. Deutsche Welle (DW). Recuperado de: https://www.dw.com/en/fact-check-how-to-spot-fake-news-during-israel-hamas-war/a-67187646

Israel en español [@IsraelinSpanish]. (2023, noviembre 04). *En la masacre del 7/10 asesinaron a su abuela*. [Tweet]. Recuperado de: https://x.com/IsraelinSpanish/status/1720944719901901075

Israel en español [@IsraelinSpanish]. (2023, noviembre 04). *Itay, Etty y Sagi Zak: Un abrazo eterno*. [Tweet]. Recuperado de: https://x.com/IsraelinSpanish/status/1720807716677976123

Meisterdrucke (2024). *La procesión del caballo de Troya en Troya, c1760. (The Procession of the Trojan Horse into Troy, c1760)* Giovanni Battista Tiepolo. Recuperado de: https://www.meisterdrucke.es/impresion-art%C3%ADstica/Giovanni-Battista-Tiepolo/762064/La-procesi%C3%B3n-del-caballo-de-Troya-en-Troya,-c1760.html

Ministerio de Relaciones Exteriores de Chile (2019). *Validación social: ¿qué es y por qué es crucial para el marketing?* Pro Chile, Apoyo al E-Commerce. Exporta Digital N°16. Recuperado de: https://acceso.prochile.cl/wp-content/uploads/2019/11/Por-que-es-tan-importante-la-validacion-social-cap-16-def.pdf

Provis M. (2023). *Análisis militar del conflicto de Israel-Hamás. Informe del Observatorio.* Centro de Estudios Estratégicos de la Academia de Guerra. Recuperado de: https://www.ceeag.cl/wp-content/uploads/2023/10/IO-MP-Conflicto-Israel-Hamas-1.pdf

Restrepo D. (2019). *Tácticas de influencia usadas en el discurso político: caso elecciones presidenciales Colombia año 2018. Tesis de maestría en psicología del consumidor*. Fundación Universitaria Konrad Lorenz. Bogotá Colombia. Recuperado de: https://repositorio.konradlorenz.edu.co/server/api/core/bitstreams/9b4d1c59-eb5a-43da-b3d8-0b290e7756f5/content

Rosero D. (2023). *Gaslighting: una técnica de manipulación para dudar de la cordura.* Radio Nacional de Colombia. Actualidad, Salud. Recuperado de: https://www.radionacional.co/actualidad/salud/sabias-que-es-el-gaslighting-y-de-donde-surgio-aqui-te-lo-explicamos

Seisdedos I. (2022). Las mentiras de la guerra de Afganistán al descubierto. El País. Internacional. Recuperado de: https://elpais.com/internacional/2022-01-23/las-mentiras-de-la-guerra-de-afganistan-al-descubierto.html

Urra F. (2022). *Las operaciones militares de decepción: un enfoque desde psicología*. Revista Ensayos Militares, 7(2), 69 - 84. Recuperado de: https://revistaensayosmilitares.cl/index.php/acague/article/view/3

51

US Joint Chiefs of Staff (2022). *Joint Publication JP-3-04. Department of Defense. Information in Joint Operations.*14 septiembre, Recuperado de: https://es.scribd.com/document/660170977/JP-3-04-Information-in-Joint-Operations

US Joint Chiefs of Staff (2012). *Joint Publication JP 3-13. Information Operations. Incorporating Change* 1. 20 November 2014. Recuperado de: https://irp.fas.org/doddir/dod/jp3_13.pdf

Vásquez, R. (2015). *El Experimento de Milgram: el peligro de la obediencia a la autoridad.* Portal Psicología y Mente. Recuperado De: https://psicologiaymente.com/social/experimento-milgram-crimenes-obediencia-autoridad

Vásquez, M. (2016). *Tesis Doctoral: La comunicación estratégica y la diplomacia de defensa en las operaciones en el exterior*. Universidad Complutense de Madrid, Facultad de Ciencias Políticas y Sociología, Departamento de Derecho Internacional Público y Relaciones Internacionales. España. https://eprints.ucm.es/id/eprint/37506/

CAPÍTULO 6

Ejecución de INFOOPS en el nivel táctico: El caso del Ejército de Tierra español

Comandante (Ejército de Tierra de España) Consuelo Delage Gª de Angulo[1]

Introducción

En el marco del Tema de Investigación Central Anual (TICA), el presente escrito pretende ofrecer una visión sobre la aproximación a Operaciones de Información (INFOOPS) en el Ejército de Tierra de España (ET), con un enfoque particular en el nivel táctico.

El Entorno de la Información (EI), así como las funciones y actividades relacionadas, son realidades muy complejas y en continuo desarrollo, que deben incorporarse en las instituciones unidas a un importante cambio de mentalidad y de estructuras. Todo esto hace muy demandante los procesos de adaptación para poder actuar en estos nuevos ámbitos: cognitivo, de la información y el ciberespacio. A través

[1] Comandante de Artillería del Ejército de Tierra (ET) de España. Realizó los cursos de Estado Mayor en la Escuela de las Fuerzas Armadas de España y en la Academia de Guerra del Ejército Chile. Master en Política de Defensa y Seguridad Internacional por la Universidad Complutense de Madrid. Cuenta con los cursos de "STRATCOM Practitioners" y de "INFOOPS" en la Escuela de la OTAN de Oberammergau (NSO). Destinada durante cuatro años en el Cuartel General de la OTAN, NRDC-ESP, y durante tres años en el Regimiento de Operaciones de Información Nº1 (ROI1) del ET. Correo: cdelgra@et.mde.es

del ejemplo español se espera dar luz al proceso de desarrollo e implementación de esta capacidad en Chile.

La información contenida en este artículo se extrae tanto de los avances en doctrina y publicaciones relacionadas, en el entorno de las Fuerzas Armadas (FAs) españolas y de la OTAN, así como de la experiencia de la oficial que firma este artículo en diferentes puestos relacionados con Comunicación Estratégica (STRATCOM) y Operaciones de Información (INFOOPS).

Antecedentes Históricos de las Unidades de Información en España

Desde la más lejana antigüedad ya se empleaban capacidades bélicas para afectar el comportamiento y las decisiones adversarias, principalmente explotando el miedo y el engaño. Sun Tzu defendía las operaciones sobre la psicología adversaria como un multiplicador de la fuerza (Estebaranz M. & Muñoz-Manero F., 2007).

A la hora de difundir información en beneficio de las operaciones marca un hito la aparición de la imprenta. La prensa es muy utilizada por los países en litigio durante el S.XIX, cuando las narrativas pasan de fanfarronear sobre la brutalidad propia (ya mal visto), a desacreditar al adversario, por ejemplo, durante la guerra de Cuba, afectó a España el descrédito que la prensa de EE.UU. hiciera del militar español Valeriano Weyler, causando efectos en las audiencias nacionales en España y provocando una disminución del apoyo social a la guerra (Bolivar, 2024).

Nuevos medios de difusión, como la radio, aumentan la instantaneidad y el alcance de la propaganda y la importancia de los mensajes y narrativas, labor que destaca durante las guerras mundiales y en la guerra civil española. En 1920, el historiador inglés, J. Fuller, emplea por primera vez el término "*Psychological warfare"* (Vazquez M., 1998, p. 40). Ya en el siglo XXI, la eclosión de internet y las redes sociales (RRSS) han causado una nueva aceleración y transformación de la forma de hacer la guerra asociada a la información y las percepciones.

Durante la década de los 80', en el ET se iniciaron los pasos para contar con estructuras que favorecieran la integración de las acciones psicológicas y de información en las operaciones. El **plan RETO** (Reorganización del ET, implementado en 1990) contemplaba 5 unidades de Acción Psicológica en la estructura permanente del ET (encuadradas a nivel división y comandancias), pero esta parte del extenso plan no fue ejecutada por falta del recurso financiero y humano.

A mitad de los 90', en el contexto del **plan NORTE** (nueva organización del ET) se creó una Unidad de Acción Psicológica[2] encuadrada en el Grupo de Inteligencia 1 (GRINT1) de la Fuerza de Maniobra (FMA) (Vazquez M., 1998). Además, habiéndose segregado el arma de Transmisiones de la de Ingenieros, la reestructuración de las

[2] Unidad concebida para planear y conducir PSYOPS en apoyo a misiones de paz y, en determinados casos, de consolidación (apoyo en los niveles Operacional y Táctico), con capacidad para constituir cinco elementos de Apoyo a Operaciones Psicológicas (PSE), en apoyo a FMA, FAR o DIMZ 1, y tres Brigadas subordinadas, así como doce *Táctical Psyops teams* (TPT) para apoyar a cuatro Batallones por Brigada.

unidades, mediante el citado plan, dio lugar a la aparición de los Regimientos de Guerra Electrónica.

En 2005, el GRINT pasó a ser el Regimiento de Inteligencia 1 (RINT 1), integrando el Grupo de Operaciones Psicológicas III (GROPS III/1). Un año más tarde, este regimiento pasaba a depender del Cuartel General Terrestre de Alta Disponibilidad (CGTAD) o *Headquarters NATO Rapid Deployable Corps-Spain (HQ NRDC-ESP)*, ya que cumple funciones en la estructura de fuerzas de OTAN. Este hecho favoreció la participación del GROPS en despliegues donde la OTAN contaba con estructuras PSYOPS, como Afganistán o Irak, adquiriendo así una experiencia inconmensurable. En el caso de Afganistán, se desplegó un PSE en la localidad de QAL-E-NOW, a las órdenes del CJPOTF[3] que la coalición tenía en Kabul, con capacidad de difusión por altavoces y una limitada capacidad de imprenta; donde se ejecutaban interacciones con líderes locales y grupos de interés difundiendo mensajes en apoyo a la operación.

Al mismo tiempo, se conformaba el Batallón de Cooperación Cívico-Militar, heredero de la Unidad de Asuntos Civiles integrada en el Batallón de Cuartel General (CG) de la FMA desde 1996. Con esta unidad, se completaba la capacidad que hasta el año 2020 ha tenido.

[3] Combined Joint Psyops Task Force.

Aproximación doctrinal española a las Operaciones de Información (INFOOPS)

Publicaciones

A la par que se creaban las estructuras orgánicas encargadas de Actividades de Información (AI) se inició el desarrollo de la doctrina. La **3ª edición de la DO1-001: *Doctrina de Empleo de las Fuerzas Terrestres* (2003)**, en su capítulo 8, trata las diferentes Operaciones Conjuntas que implican al ET, entre ellas se encuentran las Operaciones de Información y la Cooperación Cívico-Militar (CIMIC). En su capítulo 17, sobre el conflicto asimétrico, expone las acciones de movilización de masas civiles, intimidación y manipulación de información, destacando la importancia de la lucha contra la desinformación.

En 2005, se aprobaron las Publicaciones Militares (PMET), correspondientes a INFOOPS y Operaciones Psicológicas (PSYOPS)[4] que, a pesar de las nuevas realidades del entorno y procedimientos OTAN, no han sido actualizadas. Pero, aun no habiendo elaborado nueva doctrina nacional, el camino no está abandonado desde 2005. En 2009 se ratificó el AJP-3.10 sobre INFOOPS de la OTAN; esto supuso que, desde el nivel operacional, las actividades relacionadas con INFOOPS pasaban a estar regidas por los principios y procesos descritos en dicho manual. Su siguiente versión fue publicada en 2015.

[4] OR3-001: Orientaciones. Operaciones de Información y OR5 – 011: Orientaciones. Operaciones Psicológicas.

Figura 1

Resumen de publicaciones sobre INFOOPS

Nota: Elaboración propia

En 2018 se publicaba un Concepto Derivado[5] (CODE 02/2018) sobre la función de combate "Información", con la finalidad de "*establecer el marco de referencia para el desarrollo de la Información como función de combate en la Doctrina Nacional específica terrestre, teniendo en consideración los desarrollos en el ámbito de la Doctrina Conjunta Nacional, OTAN y de otros países*" (MADOC, 2018). El mismo año en la Publicación Doctrinal Conjunta para el Empleo de las FAS (PDC1-001), se incorporaba la función conjunta "Información" y

[5] Documento elaborado por el Mando de Adiestramiento y Doctrina (MADOC) que levanta, relacionado con los procesos de cambio previstos en el entorno dentro del horizonte de planeamiento de la institución, las posibles exigencias de capacidades y cambios organizativos para adecuar el empleo, preparación y medios de la fuerza del ET.

se añadía el ámbito cognitivo (AC) como uno de los ámbitos del Espacio de las Operaciones.

El siguiente paso fue, desde el nivel estratégico de las FAs, desarrollar un Concepto Exploratorio del AC y la Doctrina Conjunta de STRATCOM (PDC-10) en 2021, dando el marco desde el más alto nivel para todas las AI. En septiembre del mismo año, se publicaba la 2ª edición de la Doctrina para el Empleo de la Fuerza Terrestre (PD1-001 2ª Ed), en la que se incluye la nueva Función Táctica (FT) Información, así como el concepto de Unidades de Operaciones de Información como unidades de apoyo al combate.

En la actualidad se encuentra en adaptación y ratificación, por parte de España, el nuevo AJP-10.1 "*Allied Joint Doctrine for Information Operations"*, que ya no pertenece a la serie 3 (operaciones), sino que se deriva del AJP-10 STRATCOM, publicado en 2023. De este trabajo surgirá la PDC-10.1 sobre INFOOPS que permitirán la adaptar las publicaciones derivadas en el nivel táctico, tanto de la FT como la actualización del manual de INFOOPS (OR3-001) de 2005.

Acompañando a la doctrina se vienen elaborando en el ET estudios sobre el Entorno Operativo (EO) 2035, en su primera edición de 2019 y en la segunda de 2022, acompañados de sus respectivos modelos de fuerza, conceptos para el combate y de transformación. En todos ellos se destaca la importancia del AC, el Ciberespacial y el EI, resaltando las características de nuevas amenazas y necesidades de capacidades, estructuras y procesos para afrontarlas.

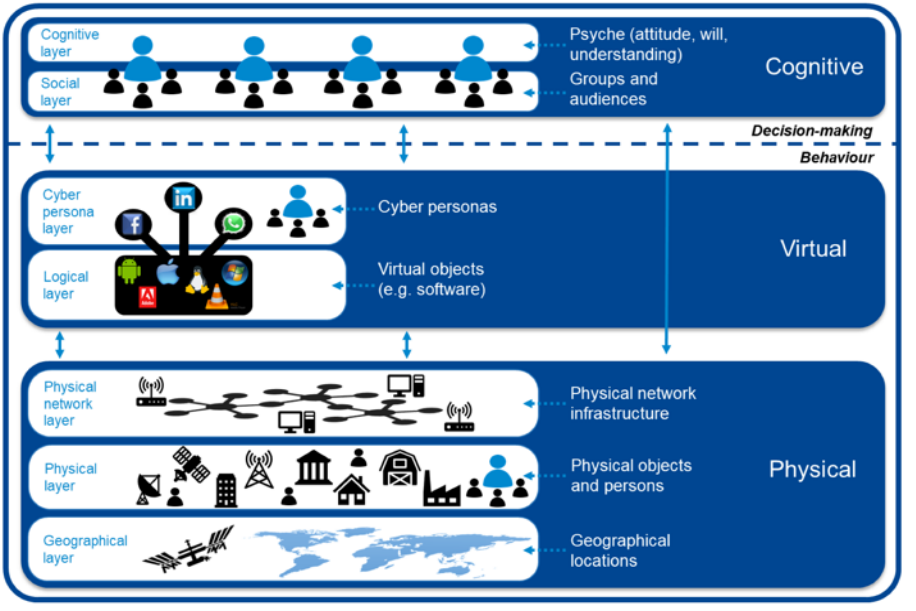
Conceptos Clave

Al enfrentarse a campos tan complejos como son el EI y el AC de las operaciones, uno de los mayores retos es definir claramente los términos que van a guiar los procesos de apreciación, planificación, acción y evaluación.

Dentro del espacio de las operaciones, el concepto más amplio es el Entorno de la Información (EI), presente en las tres dimensiones: cognitivo, virtual y físico, y compuesto de la Información en sí misma, individuos, organizaciones y sistemas que reciben, procesan y transmiten información (Estado Mayor de la Defensa, 2021, p. 14).

Figura 2

Estructura del Entorno de la Información



Nota: AJP-10

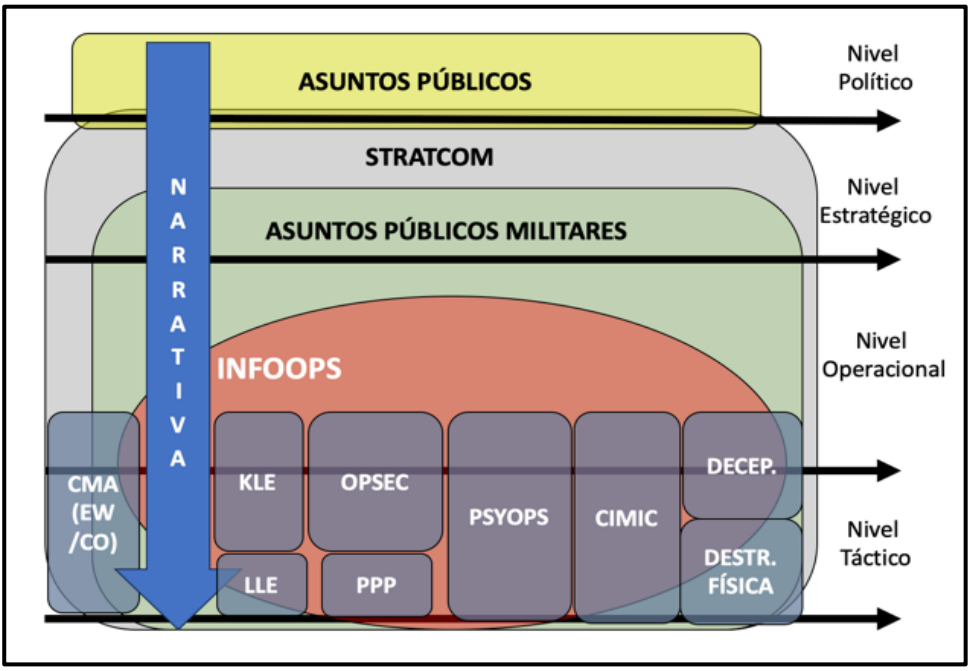
Enfocando una realidad más concreta, el entorno de las operaciones se divide en 5 ámbitos, uno de ellos es el Ámbito Cognitivo (AC), espacio intangible de las operaciones (dentro del EI) que abarca las acciones, procesos y efectos que afectan a las percepciones del ser humano (individual o grupal). Alcanza las voluntades de todas las personas afectadas por el conflicto y a los sistemas de inteligencia artificial, repercutiendo en el resto de los ámbitos (Estado Mayor de la Defensa, 2018, p. 81).

En el AC, el espacio de las operaciones se delimita mediante audiencias. Una audiencia es "*un grupo humano definido, sobre el cual se tiene autorización para realizar una AI concreta en unas condiciones determinadas, en beneficio de las operaciones propias. Las Audiencias pueden ser propias, favorables, neutrales, competidoras o adversarias*" (Estado Mayor de la Defensa, 2018, p. 84).

Dejando a un lado los espacios y entrando en las acciones, y partiendo desde lo general a lo específico, la primera gran responsabilidad es el alineamiento vertical (inter-niveles) de la narrativa, de esto se encarga STRATCOM. La STRATCOM dirigida por el JEMAD es la integración de todas las Capacidades de Comunicación, Técnicas y Funciones de Información, con otras actividades militares, para comprender y modelar el EI, en apoyo del logro de los objetivos de la defensa y de las operaciones (Estado Mayor de la Defensa, 2018, p. 106).

Figura 3

Integración de las funciones de información



Nota: Elaboración propia basado en doctrina

Vista la alineación vertical de las AI, la coordinación en cada nivel se da, desde el CG, a través de INFOOPS, que es la función de Estado Mayor (EM) para analizar, planear, evaluar e integrar AI creando los efectos deseados en la voluntad, entendimiento y capacidad de adversarios, potenciales adversario y audiencias en apoyo a los objetivos de la misión (NATO, 2023)[6]. Estos efectos pueden alcanzarse combinando las siguientes actividades: PSYOPS, Presencia Actitud y

[6] Traducción propia del AJP-10.1.

Perfil (PPP), Seguridad de las Operaciones (OPSEC), Interacción Personal (KLE/LLE/SLE[7]), Guerra Electrónica (EW), Operaciones en el Ciberespacio (CO), Cooperación Cívico-Militar (CIMIC), Destrucción Física y Decepción. Todas ellas pueden agruparse como Actividades Militares de Información (AMI) o AI, acciones, ejecutadas por cualquier medio, diseñadas para lograr efectos en el ámbito AC (NATO, 2023)[8] y el EI. Pueden incluir medidas de protección.

Profundizando en este concepto, la Doctrina Conjunta define Capacidades de Información como unidades, equipos y elementos de apoyo y asesoramiento empleados para promover percepciones y voluntades favorables y protegerse de la influencia del adversario (Estado Mayor de la Defensa, 2018, p. 62). En la misma línea, la última Doctrina de Empleo de las Fuerzas Terrestres define las Unidades de Operaciones de Información como aquellas que operan en el AC coordinando efectos en la voluntad, comprensión y capacidad de audiencias autorizadas, para influir en sus actitudes y comportamientos. Dentro de estas unidades se encuentran las de CIMIC y PSYOPS (MADOC, 2021, p. 3-10).

Todas estas actividades y capacidades se agrupan en una Función Conjunta (FC) para facilitar al Comandante Operacional su integración,

[7] Diferentes tipos de interacción según el nivel: Interacción con líderes de alto nivel /Key Leader Engagement (KLE), entre líderes propios y líderes destacados de los actores en el entorno; Interacción de bajo nivel /Soldier level engagement (SLE) o Local Leader Engagement (LLE), entre mandos o personal propio y creadores de opinión o audiencias aprobadas del entorno de operaciones.

[8] Traducción propia del AJP-10.1.

coordinación y dirección. La FC Información comprende las actividades orientadas a la gestión, denegación y uso de la información, integrándolas con el resto de las actividades militares. Su finalidad última es promover decisiones favorables a las operaciones propias actuando sobre las percepciones, actitudes y comportamientos de audiencias, afectando los procesos de decisión humanos y automatizados (Estado Mayor de la Defensa, 2018, p. 127). No debe confundirse la FC Información con la función INFOOPS, la primera es un constructo conceptual que agrupa actividades y capacidades, mientras, que la segunda es una función de EM que coordina para alcanzar efectos.

La bajada al nivel táctico se hace a través de la FT Información, que comprende las actividades concebidas específicamente para actuar en el AC, mediante su incidencia en el EI, con la finalidad de modificar o reforzar las percepciones, las conductas y las actitudes de las audiencias autorizadas. Comprende las PSYOPS, la comunicación pública, la interacción y la cooperación cívico-militar, la interacción personal, la decepción, la presencia, actitud y perfil de la fuerza y, en general, todas aquellas que sean expresamente diseñadas para actuar en el AC (MADOC, 2024, p. 7-1).

INFOOPS en los Cuarteles Generales (CG) de nivel táctico[9]
Cuartel General Terrestre de Alta Disponibilidad (CGTAD)

El CGTAD es la contraparte nacional del NATO Rapid Deployable Corps Spain (HQ NRDC – ESP), nivel Cuerpo de Ejército (CE). Durante muchos años contó con un asesor de STRATCOM, en equipo de asesoramiento al mando, sin capacidad de decisión o asignación de tareas. Las funciones de IA (Info Activities) / PSYOPS y CIMIC dependían de las Divisiones de Operaciones y Apoyo respectivamente. A partir de 2018, tras la publicación del MC-0628 (NATO Military Policy on Stratcom), se reconfiguró el CG creando una División de Comunicación (COMDIV) en la que se incluyeron tanto G-10 (STRATCOM) como G-9 (CIMIC). En G-10 se integran tanto la "Info Activities Branch" (IAB) como la Oficina de Comunicación Pública Militar (MIL PA)[10].

La IAB es el punto focal sobre el que se estructura la función de INFOOPS, siendo quien asesora y coordina todas las actividades (cinéticas como no cinéticas, con efectos letales y no letales) que afectan el EI. Esta célula analiza el entorno y planea, valora e integra las AI para lograr objetivos deseados sobre audiencias aprobadas en beneficio de los

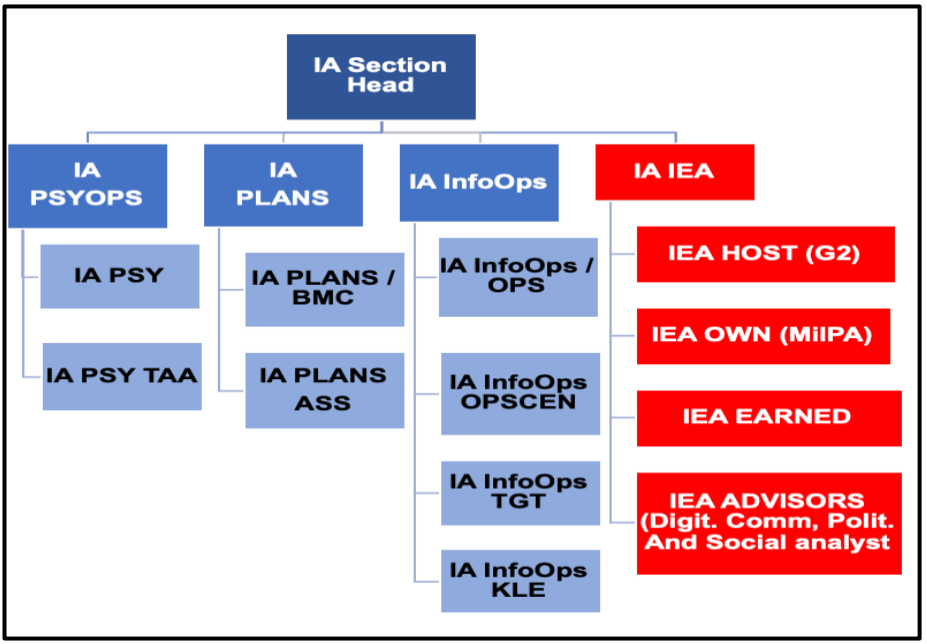
[9] Dado que las INFOOPS son una función de CG, los modelos que se proponen en el presente apartado, especialmente en del CG de CE (CGTAD) por ser el de mayor trayectoria, son fundamentales y primer paso a implementar en una institución que quiera avanzar en la gestión de las actividades y operaciones de información.

[10] El jefe de esta oficina de comunicación, un oficial con los cursos de comunicación necesarios en el ámbito nacional y OTAN, sigue siendo asesor directo del Comandante para temas relacionados con MILPA.

Objetivos de la Operación. Asegura que estas actividades se incluyen en los planes y operaciones en curso, así como la coordinación con los CG subordinados.

Figura 2

Estructura IAB NRDC-ESP



Nota: Elaboración propia según SOI-7020_INFOOPS de NRDC-ESP

Las principales responsabilidades de la IAB como parte de G-10 son:

- **Análisis del EI** (parte del Information Environment Assessment, IEA): Contribuyendo a la comprensión inicial del EO, liderada por G2, manteniendo el proceso y presentando las actualizaciones en los grupos de trabajo (WG).

- **Planeamiento de IA**: Integrándolas en el proceso de planificación en todos los horizontes (Equipos de planificación, BMC y OPSCEN[11]), definiendo objetivos, efectos y tareas relacionados con la información, durante la planificación de la operación, así como en las sucesivas FRAGOs (órdenes fragmentarias) que se desarrollen.
- **Coordinación IA durante la ejecución**: Esta tarea se apoya principalmente en el Grupo de Trabajo Específico (IAWG[12]), al que contribuyen activamente tanto el elemento de planes como el de operaciones de la IAB. Para lograrlo se mantendrá un contacto estrecho con el representante de IA en el OPSCEN y se contribuirá a otros procesos mediante los WG específicos como *Targeting*, Recolección de Información (G2) o Assessment / valoración (G5/3). A través de todos ellos, se extraerán conclusiones para informar al comandante y, en la Junta de Coordinación (CB[13]), también se le presentarán las decisiones necesarias para el proceso de las operaciones, de acuerdo con el Ritmo de Batalla del CG.
- **Contribución al proceso *Targeting***: Unido al punto anterior, se recalca la contribución del personal de IA al *Targeting*, tanto en lo referente a *Targets* relacionados con Información, así como

[11] Equipos de Planificación Táctica (EPT), "Battle Management Cell" (BMC) a medio plazo y el Centro de Operaciones (OPSCEN) para reacción a incidentes y planificación de circunstancias a corto plazo.

[12] Info Activities Working Group. Para más detalle ver apartado específico más adelante.

[13] Coordination Board.

con tareas de Información en apoyo a *Targets* con efectos físicos (por ejemplo, para mitigar efectos colaterales y daños)

- **Contacto con unidades subordinadas** al CG, tanto con las Unidades de Información, así como con Células de los CG de otras unidades de combate subordinadas (G9, G10 o AMI) que tengan cometidos específicos en apoyo de los Objetivos y Efectos de Información.
- **Coordinación (planificación, preparación y ejecución) de KLE:** Son interacciones entre líderes propios y tomadores de decisión de audiencias aprobadas o líderes de otros grupos de interés, con propósitos definidos en apoyo a Objetivos de Información. Es parte del proceso de *Targeting*, diferente a otras interacciones. El elemento encargado en la IAB desarrolla el Plan de KLE y prepara los paquetes de información sobre las audiencias, apoyada por inteligencia y otros especialistas.
- **Valoración de STRATCOM e INFOOPS** para medir la efectividad de las IA ejecutadas: Contribuye a la valoración general de la campaña, proveyendo el adecuado asesoramiento, y es coordinado desde los AWG/ACB[14]. Como parte del Grupo de Planeamiento, el encargado de planes de la IAB se hará cargo de aportar las adecuadas Medidas de Efectividad (MOE).

Este modelo de IAB, por ser el más exhaustivo y seguir las directrices OTAN, es el que, con las adaptaciones adecuadas según el

[14] Grupo de Trabajo y Junta de Valoración de la Campaña / Assessment WG and Coordination Board.

nivel del CG, sirve de modelo para la constitución de las células encargadas de IA en los CG de niveles inferiores.

CG de División (DIV)[15]

En este nivel se constituye una célula AMI (Actividades Militares de Información) que lidera el planeamiento y ejecución de todas las AI que se dan a nivel división (CIMIC, PSYOPS y MILPA[16]). Se encarga del análisis del EI, así como del planeamiento, integración y valoración de las AI en apoyo a la misión (dividido en Operaciones en Curso y Planes). Se tiene presente en todo momento la guía de STRATCOM e INFOOPS recibida de escalones superiores.

El personal de esta célula es el que, en tiempo de paz, constituye la G9 de DIV. Si hiciera falta para la operación se solicitan los refuerzos y especialistas necesarios.

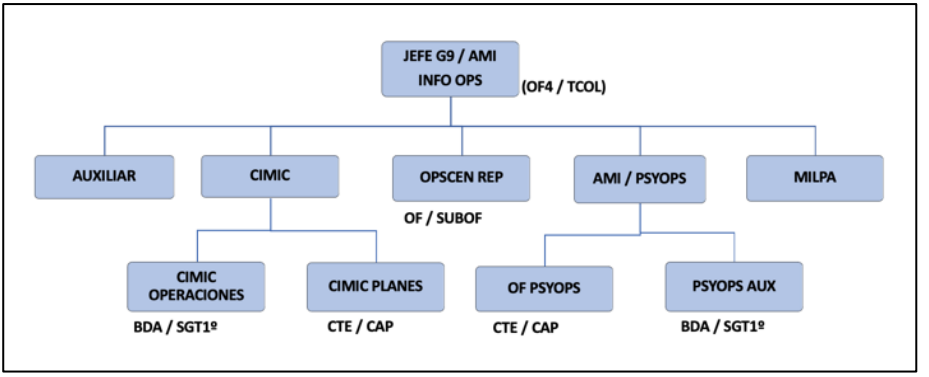
Si el número de personal lo permite, se desdoblará cada elemento (CIMIC/PSYOPS/MILPA) en Operaciones en Curso y Planes. Uno de los integrantes de Operaciones será el representante de AMI en el Centro de Operaciones (OPSCEN). Este puesto no se puede improvisar, ya que juega un papel fundamental en la reacción ante incidentes y necesita instruirse integrado en las dinámicas del OPSCEN.

[15] Parte de la información extraída de la SOP 900 célula de actividades militares de información (AMI)

[16] Comunicación Pública Militar / Military Public Affairs (MILPA)

Figura 3

Estructura célula AMI de DIV



Nota: obtenido de doctrina (MADOC, 2022)

Para todos sus cometidos se apoyará en un EaEI[17] en caso de contar con él. Los cometidos principales de la célula AMI son:

- Analizar y comprender el EI dentro del Área de Operaciones (AoO).
- Contribuir al planeamiento (largo, medio y corto plazo) identificando actores y factores que afectan al EI, integrando las AMI en el planeamiento para lograr los efectos necesarios.
- Coordinar e integrar las AMI con el resto de las actividades militares a través del IAWG y otros grupos de trabajo[18] en los que se solicite apoyo.

[17] Equipo de Apoyo en el EI, estructura operativa que conforma el ROI1 para apoyar las operaciones. Suele formar parte del Núcleo de Tropas Divisionario (NTD). (Ver nota 26)

[18] Targeting, Assessment, Coordination, Collection.

- Evaluar y medir la efectividad de las AMI, contribuir al proceso de valoración de la operación y asesorar al jefe de la DIV sobre las acciones CIMIC, PSYOPS y MILPA.
- Contribuir al proceso de Integración de Blancos (*Targeting*/Fuegos).
- Contribuir, según requerimiento, con los datos necesarios sobre el Entorno Social y de la Información a la documentación generada por el PCDIV (SITREP, ASSESSREP, CIMICREP, PSYREP[19]…).
- Orientar a los mandos subordinados en cuanto a la ejecución de las AMI que permitan conseguir los efectos informativos incluidos en la Orden de Operaciones (OPORD).

CG de Brigada (BRI)

La brigada constituye la Gran Unidad elemental de empleo, su CG debe tener capacidad de planificar AI a su nivel que contribuyan a las acciones en el AC diseñadas por escalones superiores, CE y DIV, responsables principales de AI en el Nivel Táctico. Para ello recibirá el apoyo necesario de escalones superiores y especialistas, de acuerdo a la naturaleza de la operación. Al igual que en DIV se debe constituir una célula AMI, sobre la base de la G9, en la que puede haber personal especializado en PSYOPS, CIMIC y MILPA y, en caso de contar con el apoyo de un EaEI, el contingente necesario para integrar el apoyo (OFEN

[19] Reportes de situación, valoración, CIMIC y de PSYOPS.

y célula de análisis de RRSS).

El concepto desarrollado para el 2035 (Estado Mayor del Ejército de Tierra, 2023) asume que la Brigada 35 será capaz de contribuir a las Operaciones Multidominio (MDO), generando y sincronizando efectos con todos los niveles (Estratégico, Operacional y Táctico), desde y sobre cualquier Ámbito (Terrestre, Marítimo, Aeroespacial, Ciberespacial y Cognitivo). Estos efectos podrán ser físicos, virtuales o psicológicos. También se menciona el AC en el espectro de la brigada a la hora de acometer decepción y ocultamiento, ésta deberá ejecutarse no sólo en la dimensión física sino también en la cognitiva y virtual.

INFOOPS en el Planeamiento[20]

La planificación es un proceso fundamental de todo CG y en el que debe participar personal especializado, con la mirada puesta en este nuevo Ámbito y Entorno. La Publicación Doctrinal (PD) sobre el Proceso de Planeamiento en las Operaciones en el Nivel Táctico (PPO-T) establece que *"durante el PPO-T se deberán establecer las medidas oportunas que permitan la adecuada coordinación, sincronización e integración de todas las AI durante la ejecución de las operaciones, así como su alinea miento con las directrices que emanan de STRATCOM"* (MADOC, 2022).

En los primeros momentos del proceso se inicia la evaluación del

[20] En este apartado se sigue el proceso de planeamiento reflejado en el PPO-T del ET (MADOC, 2022)

EO y como parte central se evalúan los factores PEMSII[21], todos ellos deben abordarse con la mirada puesta en el EI y el AC. Por ejemplo, las narrativas desde el gobierno, posibles líderes clave dentro del ámbito político, infraestructuras de medios de comunicación, postura y características de éstos, así como de los diferentes grupos sociales. También, debe considerarse el estado de la moral de las fuerzas adversarias y los medios con los que éstas cuentan para actuar sobre las percepciones y las actitudes y maniobrar en el EI. Este proceso de comprensión y valoración del entorno debe ser continuo, y actualizarse durante la ejecución. En él, de contar con personal cualificado, debe profundizarse en el Análisis de Audiencias, esto se corresponde con lo que el AJP-10.1 llama Information Environment Assessment (IEA) (OTAN, 2023).

Asimismo, es un momento clave el analizar la misión recibida y entender los cometidos en el EI que se asignan en la orden del escalón superior. La Información relevante puede encontrarse tanto en el cuerpo de la orden (propósito, cometidos y medidas de coordinación) como en los anexos relacionados (STRATCOM, INFOOPS, PSYOPS, MILPA, CIMIC, Enlace, PPP, EW). Recibida la misión se continúa con el estudio de factores relacionados, extrayendo tareas, limitaciones o necesidades de información. De todo ello pueden salir elementos clave para continuar el planeamiento como RFIs[22], adaptaciones de los mensajes y temas para

[21] Político, Militar, Económico, Social, Información e Infraestrcutura. Se puede añadir los factores físicos y de tiempo.

[22] Solicitudes de Información / Request for Information (RFIs).

contrarrestar narrativas adversarias o incluso potenciales *Targets* para proponer en el proceso de *Targeting*. Finalmente, se elabora un Juicio Inicial, en el que se reflejará la Misión de Información, Objetivos y conclusión de estudio de los factores, con posibles Audiencias y *Targets*. Se deberá aclarar también los medios propios disponibles en caso de haber agregaciones de Unidades de Información.

Durante las siguientes etapas, como de todas las funciones, se desarrolla un Esquema de Apoyo de información. En este esquema se deben contemplar Efectos clave de Información, Situación Final Deseada en el ámbito de la Información y entidad de unidades para ejecutar las AI en apoyo a la Línea de Acción (LA). Por fases deben presentarse, deseablemente, Efectos/ Acciones / MoE, posibles Audiencias y *Targets*, medios a emplear y las prioridades de apoyo, sin olvidar las características del apoyo al Esfuerzo Principal. Finalmente, no deben olvidarse los Riesgos[23] asociados a la Información y su mitigación. El análisis de las LA se realiza, principalmente, a través del proceso de confrontación, en el que se debe tener en consideración una mirada de las AI tanto propias como adversarias.

A continuación, se le presentan las LAs al comandante para su decisión y, tras la decisión, se emitirá una Guía de Planeamiento final. Durante este proceso, ni el EPT para su recomendación, ni el comandante en la Guía de Planeamiento, deben dejar de lado la realidad del EI y del

[23] Esto se hará en colaboración con el elemento del CG encargado del análisis de riesgos.

AC, siempre que sea un factor relevante del EO (lo más habitual en los conflictos actuales). Esto se traduce en la introducción de elementos relacionados con este ámbito tanto en los criterios de comparación como en las ventajas o desventajas de cada LA, por parte del EPT y, por parte del comandante, en reflejar las directrices necesarias en la Guía, que permitan a las células del CG y a las unidades específicas continuar con el planeamiento. Al final de esta fase se emite una Orden Preparatoria que en ningún caso soslaya los aspectos relacionados con INFOOPS.

Finalmente, se desarrolla la OPORD, que debe contar en su cuerpo, como mínimo, con un párrafo específico relacionado con las AI en el Concepto de la Operación. Además, se elabora un Anexo[24] en el que se desarrollará el Concepto de Apoyo presentado en las etapas anteriores, dejando bien claros los Objetivos de Información, Audiencias autorizadas (con la mayor segmentación posible) y las Instrucciones de Coordinación[25] tanto para unidades subordinadas como para el resto de las funciones que interactúan con las AI. Se deben incluir como apéndices las matrices necesarias (ver apartado más abajo). Contar con una Matriz de Sincronización de AI no será óbice para la inclusión de las

[24] No es obligación limitarse a un solo anexo, si la entidad de la operación lo requiere se puede desglosar el apoyo en varios anexos como por ejemplo INFOOPS, PSYOPS, MILPA, CIMIC, Enlace, PPP. De hecho, es preferible que MILPA cuente con su anexo específico para asegurar su separación de actividades como PSYOPS o MILDEC.

[25] No deben faltar instrucciones sobre grupos de trabajo, reportes específicos que se solicitan a las unidades subordinadas de combate o específicas de información y, si se diera el caso, nivel de delegación de autoridades de aprobación de audiencias y mensajes (es muy raro que esto se delegue a Nivel Táctico, pero es un aspecto que debe estar en conocimiento de todo el personal involucrado)

tareas más relevantes dentro de la Matriz de Sincronización que desarrolle Operaciones.

Herramientas de Coordinación

IAWG (Info Activities Working Group / Grupo de trabajo AMI): Los tres niveles mencionados deben integrar en su ritmo de batalla una reunión que asegure la coordinación de todas las AMI (PSYOPS, OPSEC, EW, INFOSEC, KLE, PPP y MILPA), así como su sincronización con el resto actividades militares. La participación y su frecuencia dependerán de las directrices del comandante, tipo de misión y tempo del ciclo de decisión.

Como norma general, en cada ciclo de decisión (entre dos CB) debe haber un IAWG. Si el Ritmo de Batalla lo permite, o si las acciones en el AC tienen una relevancia considerable en el contexto de la operación, puede haber, además, una Junta/Board específica de AMI con el comandante, en la que tome decisiones relacionadas.

Los temas por tratar, sin agotarse en estos, son: Actualización STRATCOM / AMI superior, guía del jefe de AMI, Actualización de la situación entorno (social e info.) (G2), actualización AMI (acciones PSYOPS, CIMIC y MILPA últimas 24/48 horas y próximas 24/48 horas), Targets relacionados con AMI, Actualización KLE, Actualización Valoración campaña (relacionado con Información).

Las conclusiones posibles son: Resultado de Valoración de

Campañas de Información y acciones CIMIC en curso, propuesta de nuevos Planes de Acción AMI, guías o nominaciones para *Targets*, modificaciones a Matriz de Enlace, necesidades de Coordinación de AMI con otras con acciones tácticas.

La participación recomendada sería: Jefe célula AMI/G10, responsables de PSYOPS, CIMIC/G9, MILPA y Enlace (si hubiera específico), AMI/planes, AMI/IEA, AMI/*Targetint*, representantes G2, G3, G6 (CEMA/EW/CO), Targeting, OFEN EaEI, Aseores (jurídico, político, cultural, género). De forma puntual se puede requerir asistencia de representantes Logístico/G4, Financiero/G8, Protección/C-IED, Oficiales de Enlace (OFENs).

Si se desarrolla la Junta la presidirá el Comandante/COS/jefe DIVCOM, según la delegación designada por el comandante:

Reportes: Se pueden dar dos casos: solicitar mensajes específicos, como PSYREP o PIREP[26], o que las unidades incluyan la información relacionada con las interacciones y resto de AI en los Reportes de Situación (SITREPS) que remiten con el resto de los datos sobre el estado y las actividades de la unidad. No se debe descartar la posibilidad de solicitar informes Ad Hoc sobre estado de Audiencias o incidentes específicos. La periodicidad dependerá del ciclo de toma de decisiones del CG así como de la intensidad de las AI en curso.

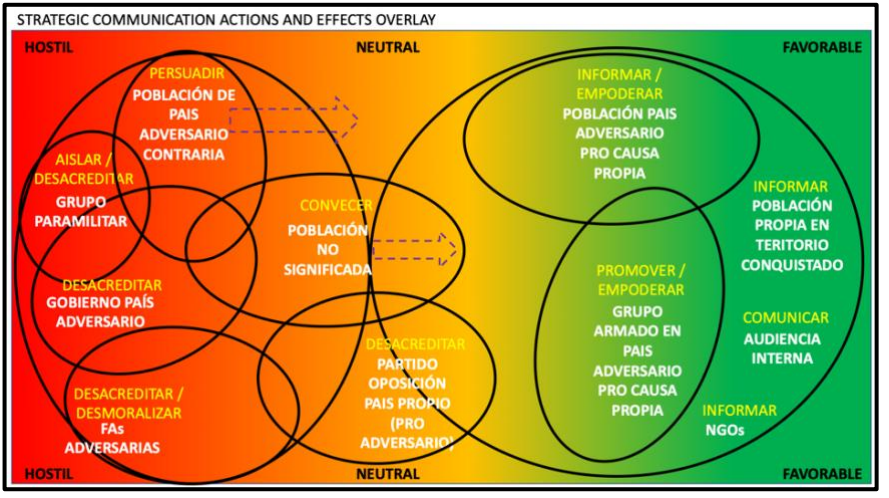
Matrices y Planes de Acción: Se presentan a continuación una serie

[26] Informe de PSYOPS / PSYOPS Report (PSYREP) e Informe de Comunicación Pública / Public Informarion Report (PIREP) (MADOC, 2005)

de herramientas, elaboradas sobre la base de manuales de referencia, y que han demostrado su utilidad para la coordinación de las AI a Nivel Táctico.

Figura 4

Matriz de audiencias y efectos



Nota: Elaboración propia según modelo AJP-10.1

Figura 5

Matriz de objetivos, efectos, tareas y medios

OBJETIVOS INFOOPS	OBJETIVOS ESPECÍFICOS	EFECTOS	COMETIDOS	MEDIOS
PROMOVER CAPACIDAD DE LAS FUERZAS LOCALES	Promocionar capacidades militares de Fuerzas locales.	Operatividad de las FAs locales y capacidad de actuación incrementada	Explotar éxitos Fuerzas locales	PSYOPS/ INFOOPS (IP)
			Apoyar la instrucción de las Fuerzas locales, PARTNERING. Mostrar resultados	PSYOPS/ INFOOPS (IP)
	Promover confianza de la población en FAs locales.	Percepción de seguridad de la población local implantada	Promover ante la población, el honor y honradez como valores de las fuerzas armadas locales	PSYOPS/ INFOOPS (IP)
PROMOVER LEGITIMIDAD DE LAS AUTORIDADES LOCALES	Promover capacidad y legitimidad de de las autoridades ante la población y fortalecer su imagen.	Confianza de la población en las autoridades locales y regionales del gobierno restablecida.	Convencer a la población de la eficacia de las autoridades locales.	PSYOPS/ INFOOPS (IP)
			Promover y resaltar esfuerzos del gobierno local para restablecer el orden y proporcionar los servicios. Apuntalar éxitos y promocionar proyectos.	PSYOPS/ INFOOPS (IP) /CIMIC
PROMOVER SENSACIÓN DE PROGRESO	Promover proyectos de desarrollo económico local.	Calidad de vida de la población mejorada	Impulsar contratación y espíritu emprendedor en las comunidades locales	KLE / CIMIC
			Campañas para mostrar beneficios del desarrollo económico legítimo (no actividades ilegales)	KLE/ PSYOPS / INFOPPS (IP)
	Impulsar avances sociales en las comunidades locales.	Servicios básicos implantados en buenas condiciones en todas las regiones de la ZA.	Proyectos colaboración con entidades educativas y sus líderes.	KLE / CIMIC
			Actividades para mejorar saneamiento y distribución de agua y electricidad	CIMIC
ROMPER LAZOS DE CONFIANZA/ COOPERACIÓN ENTRE POBLACIÓN E INSURGENTES Y CRIMEN ORGANIZADO	Disminuir influencia de OPFOR sobre Población local.	Apoyo población andaluza a OPFOR reducida	campaña en zonas despliegue inicial para ganar el apoyo popular para el Gobierno local	KLE/ PSYOPS / INFOPPS (IP)
			Trabajar sobre compromiso de líderes locales y medios de comunicación afines.	KLE
			Detectar células de reclutamiento grupos armados adversarios y anularlas.	EW
	Asegurar control zona fronteriza.	Población de etnia europea se siente integrada y asistida por autoridades GoA.	Fortalecer compromiso líderes locales en zonas fronterizas	KLE / CIMIC
			Realizar actividades conjuntas con Fuerzas y Autoridades locales en beneficio de la población etnia europea y darles visibilidad y propaganda	PSYOPS/ INFOOPS (IP) /CIMIC
	Disminuir capacidad de actuación de OPFOR	Oposición en el entorno informativo reducida	Localizar elementos hostiles (líderes grupos armados adversarios, crimen organizado, medios comunicación hostiles) actuar sobre ellos	EW / PSYOPS
			Apoyar operaciones ofensivas, explotando éxitos tácticos para reducir iniciativa del enemigo.	PSYOPS

Nota: Elaboración propia según modelo OR3-001

Figura 6

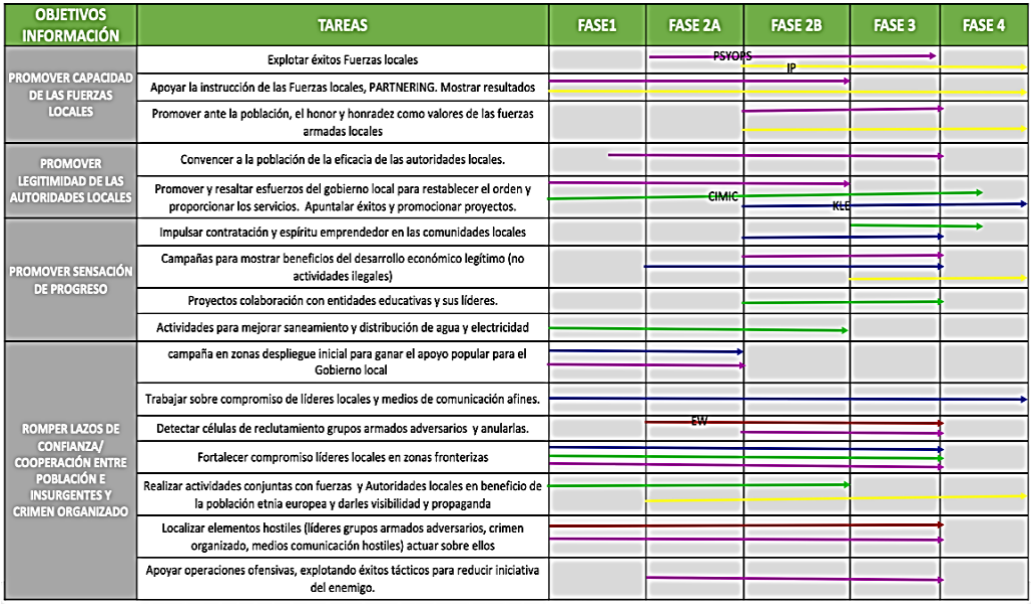
Matriz de objetivos y tareas

OBJETIVO OPERACIÓN: DISMINUIR EFICACIA FUERZAS ADVERSARIAS						
FASE (S) : 3A – PREPARACIÓN Y 3B - CONTRAOFENSIIVA						
OBJETIVOS ESPECÍFICOS (INFORMACIÓN)	GRUPOS DE OBJETIVOS / AUDIENCIAS	RFI ASOCIADAS	TAREAS	MEDIOS	EFECTOS DESAEDOS	MEDIDAS EFECTIVIDAD
Degradar C2 adversaria	Nodos comunicación adversario	¿cuáles son y dónde están los nodos C4 críticos adversarios?	-Neutralizar nodos C4 adversarios. -Neutralizar comunicaciones PC adversario con escalón superior y subordinados	EW / Art. / Apoyo aéreo	Fuerzas enemigas incapaces de conducir sus operaciones	Emisiones enemigas detectadas (no hay o disminuidas)
Disminuir capacidad de combate adversaria	Miembros FAs adversarias	Grado de preparación y moral de FAs adversarias	-Disminuir moral fuerza adversaria (directamente o a través de incrementar preocupación en familiares / población civil) -Crear dudas sobre posibilidad de éxito adversaria	PSYOPS	Rendición o deserción de miembros FAs Adversaria	Nº de rendiciones o deserciones (incremento)

Nota: Ejemplo del OR3-001

Figura 7

Matriz Sincronización INFOOPS



Nota: Elaboración propia según modelo OR3-001

Figura 8

Plan de Acción de Información (PAI)/ Military Information Activitiy Action Plan (MIAAP)

<table>
<tr><th colspan="3">PLAN DE ACCIÓN DE INFORMACIÓN: “LEGITIMIDAD”</th></tr>
<tr><td colspan="3"><u>Objetivo de información principal</u>: Legitimar el accionar de fuerzas propias.
<u>Objetivo de información secundario</u>: Influir positivamente en la población civil.</td></tr>
<tr><td colspan="3"><u>Antecedentes</u>: En el marco de las tensiones territoriales entre X e Y… Se ha decidido intervenir para asegurar sus intereses nacionales, así como para proteger a los civiles que confían en esta nación.</td></tr>
<tr><td>Efecto operacional</td><td>Efectos deseados</td><td>Efectos no deseados</td></tr>
<tr><td>CD 2 fuerza desplegada
CD 3 conflicto escalado
CD 9 Zona de compensación conquistada
CD 10 Administración territorial establecida
CD 11 transición al gobierno local ejecutada</td><td>• Legitimidad de las operaciones propias
• Presencia propia aceptada por la población
• Población protegida
• Administración territorial iniciada
• Servicios esenciales en funcionamiento</td><td>• Fuerzas propias vistas como invasoras
• Población civil masivamente afectada por las operaciones militares
• Nuevo gobierno visto como una imposición
• Intereses de terceros países afectados por las operaciones militares
• Operación rechazada por la comunidad internacional</td></tr>
<tr><td colspan="3">Mensajes claves:
• Unidos defenderemos nuestro país y somos más (patriotismo)
• Recuperamos lo que nos pertenece.
• Y es responsable de quebrantar los DDHH contra ciudadanos de X y sus intereses.
• Compromiso con la seguridad de todos los ciudadanos que tienen una vinculación con nuestro país.
• El avance es de carácter temporal para conformar una zona de seguridad (no antes de XXX) (OPSEC)
• X, en defensa de sus intereses, no ha tenido más remedio que actuar ante los abusos de Y.

Personal del Comando Conjunto debe tener siempre en cuenta:
• El respeto a las tradiciones propias de Y es crítico.
• Hasta el nivel más bajo deben conocerse las directrices comunicacionales impartidas a través de los órganos de comunicación respectivos.</td></tr>
<tr><td colspan="3">Asignación de tareas</td></tr>
<tr><td>Medio/responsable</td><td>Acción información</td><td>Audiencia</td></tr>
<tr><td>COM Comando Conjunto (IP)</td><td>Informar sobre estado de las operaciones
• Ruedas de prensa y comunicados
• Enlaces clave (Según plan de enlaces clave)</td><td>Población propia y Población territorios ocupados.</td></tr>
<tr><td>IP</td><td>Informar sobre operaciones (comunicados y ruedas de prensa)
• Apoyar difusión de Maniobras previas.</td><td>Población propia en TOCS/Población Austral territorios ocupados</td></tr>
</table>

	• Explotar Acción escalada • Explotar protección puente • Preparar procedimiento ante situaciones de crisis comunicacional y Preparar cartilla comunicacional.	
KLE (COM CC, JEM CC, ACAT, COM OMs)	Realizar interacción con líderes en los que se integrarán los mensajes de este plan (Según Plan de enlaces clave).	Autoridades, Líderes clave y creadores de opinión de zona conquistada
ACAT (CIMIC)	Integrar mensajes de este plan en: • Sus interacciones con responsables y gestores de la administración. • Sus interacciones con población a la hora de desarrollar proyectos (fase 4) promover sensación de seguridad	Autoridades locales/ Población propia en territorios ocupados
EW (OMT, OMN)	Perturbar y afectar sistemas de MyC	FAs contrarias
C-OPS (apoyo escalón superior)	Contribuir a: • Contrarrestar desinformación • Afectar la capacidad de Y para difundir sus mensajes a través de MCS. • Difundir mensajes de legitimidad entre población no afín operación propia.	Población en territorio conquistado contraria a presencia propia/ Población no significada /MCS contrarios en zona conquistada
TGT	A través del ciclo TGT contribuir a: • Afectar la capacidad adversaria para difundir sus mensajes a través de MCS (antenas y centro de emisión) • Anular capacidad de influencia de líderes civiles y para militares contrarios.	Población en territorio conquistado contraria a presencia propia/MCS adversarios
INTEL	Contribuir el IEA (Análisis del entorno de la Información) y al TAA (análisis de audiencias objetivo) a través del plan de colección y el apoyo de INTEL al TGT	

Nota: Elaboración propia

Unidades y capacidades para ejecución de AI

Regimiento de Operaciones de Información Nº1 (ROI 1)

Creado el 1 enero de 2019 por la Norma General 03/17 «Adaptaciones Orgánicas del ET para el año 2018» y alcanza FOC el 25 de junio de 2019. Unifica bajo el mismo mando el Batallón independiente de cooperación Cívico-Militar (CIMIC) Nº1 y el GROPS III/1. Proporciona las capacidades para llevar a cabo las AI y CIMIC en Operaciones de Proyección de la Fuerza (Expósito, 2020). Hasta finales del año 2020, el Regimiento dependía directamente de General Jefe de la Fuerza Terrestre. Con la implantación de la nueva organización del ET orientada a la misión, pasó a depender de la División San Marcial.

Su misión es proporcionar a los niveles Mando Componente Terrestre (MCT), DIV y BRI las capacidades para ejecutar AI (en especial PSYOPS y CIMIC) sobre Audiencias autorizadas, así como contribuir a la integración de estas con el resto de Actividades Militares para comprender y modelar el EI e influir en actitudes y comportamientos. Para ello constituye una UaEI / EaEI[27] . Además, se pueden reforzar los apoyos con elementos que operen desde retaguardia con capacidad de análisis de EI y de producción (imagen, video y audio).

Se compone de dos Grupos de Operaciones de Información (GOIs) y una Compañía de Plana Mayor y Servicios.

[27] El nombre de esta organización operativa se encuentra en proceso de cambio y por lo tanto puede encontrarse de las dos formas Unidad o Elemento de apoyo en el EI (UaEI o EaEI)

El GOI I, además de su elemento de mando, cuenta con una **unidad de Especialistas Funcionales**, otra **unidad de Generalistas** y personal formado en Comunicación Pública para apoyar a los órganos de comunicación de los CG que se determine.

Tiene las siguientes misiones:

- Establecer y mantener el **enlace con los elementos civiles** en ZO.
- Materializar actividades CIMIC.
- Identificar y desarrollar los proyectos de impacto inmediato en beneficio de población.
- Coordinar el apoyo de Autoridades Civiles a las operaciones.
- Difundir mensajes adecuados a la población civil y medios de comunicación para asegurar que el entorno civil donde se desarrollan las operaciones comprenda la misión de las Fuerzas propias.

El GOI II, al igual que el grupo hermano, cuenta con elemento de mando al que se le une una **Unidad de Planes**, con capacidad de planificar campañas y elaborar programas PSYOPS, analizar audiencias, desarrollar criterios de evaluación de campañas y reforzar con personal especializado, de manera limitada, el CG que se determine. Además, cuenta con una **Compañía de Producción y Diseño** con capacidad de producción gráfica, y de producción y difusión[28] de radio y video. También tiene una **Compañía de Difusión** que contribuye a la diseminación de los productos

[28] La difusión desarrollada por esta compañía puede ser coordinada con medios de comunicación tradicionales a través de las vías definidas oficialmente en los acuerdos o normas nacionales y de la operación o a través de RRSS y WEB.

mencionados, desarrollar relaciones humanas que faciliten la difusión de mensajes y el *feedback* de las campañas y con capacidad de Cámara Táctica (CAMTAC). Finalmente cuenta con un **Centro de Análisis del EI (CAEI)** que proporciona al mando datos sobre la situación del EI (Medios de Comunicación digitales y RRSS).

Tiene las siguientes misiones:

- Contribuir al planeamiento, coordinación y ejecución de PSYOPS, Campañas de Información y otras AMI que se definan en apoyo a una GU, realizando Análisis de Audiencias, elaboración de Programas y valoración de Efectos.
- Diseñar, producir y difundir productos gráficos y audiovisuales en apoyo a las campañas definidas en el planeamiento.
- Monitorizar los medios de comunicación y RRSS y analizar la Información Pública Disponible (PAI) en apoyo a las operaciones.
- Preparar y difundir mensajes adecuados:
  - Para asegurar que el entorno civil donde se desarrollan las operaciones comprende la misión de las Fuerzas propias.
  - Para que los posibles adversarios depongan su actitud o vean mermada su moral y voluntad.
  - Para contrarrestar la propaganda enemiga en la zona de operaciones y mantener la moral de las fuerzas propias.

El GOI II ha sido nombrado unidad de referencia de la preparación (URP) en CAMTAC, por lo que, a través de ejercicios anuales, contribuye al adiestramiento de equipos orgánicos de las BRI.

INFOOPS en la brigada

La brigada ejecuta AI, integradas con el planeamiento y ejecución de los escalones superiores, para causar efectos sobre Audiencias autorizadas. Para ello no cuentan con unidades orgánicas específicas para la ejecución de AMI. A lo largo de una operación, o durante un ejercicio, recibe la agregación de equipos tácticos de CIMIC, Información o CAMTAC, provenientes de ROI1. Además, en caso de considerarse adecuado por las características del entorno, se le puede asignar una UaEI[29] , además del que apoye a DIV.

Lo anterior no excluye la participación de personal de las brigadas en los ejercicios anuales que se desarrollan en el ROI1[30] para la instrucción de equipos tácticos (no especializados) propios de las brigadas. Este personal puede hacer funciones básicas de interacción y enlace, difusión de mensajes y toma de imágenes.

Capacidades en el Ciber Espacio (CE) y Guerra Electrónica (EW)

Estas capacidades, conocidas también como CEMA (Cyber and Electromagnetic Activities), se encuentran muy ligadas al Arma de Transmisiones. Como se relata en la introducción, en el ET se crearon dos REW a mitad de la década de los 90 del siglo pasado, aglutinadores de la

[29] Unidad de Apoyo en el EI, organización operativa generada por el ROI1 en apoyo a grandes unidades (BRI y DIV).

[30] Ejercicios Rubielos (GOI I / CIMIC) y Tridente (GOI II / Información).

capacidad de EW dentro de la Institución. Con los medios que cuenta[31] (Tomás, 2023, p. 785), la contribución a las AI es muy limitado.

El caso de las capacidades en el CE es diferente. A día de hoy, en el ámbito de las Fuerzas Armadas Españolas el núcleo de la capacidad se encuentra en Mando Conjunto del CE (MCCE), con el foco en la Ciberdefensa y desde el que el apoyo a las acciones en el AC es limitado. Además, el ET cuenta con una compañía de Ciberdefensa, dirigida a protección y defensa de redes propias, dotada del sistema SIMBA[32] (Tomás, 2023, p. 785). En un futuro cercano no se descarta la ampliación de estas capacidades del ET hasta la entidad de Batallón.

Conclusiones

Este capítulo se inicia con una revisión de la evolución histórica de las unidades y la doctrina relacionada con las AI. Le sigue una síntesis de los principales conceptos relacionados con INFOOPS con la finalidad de establecer un marco que facilite la comprensión de un campo de estudio complejo, destacando la fuerte influencia del modelo de OTAN, referencia para el desarrollo doctrinal español. En el corazón del documento se encuentra una descripción de las características de los CG de las GU para poder trabajar en el campo de INFOOPS. A este apartado se le añade un análisis sobre la relevancia de los aspectos de Información en el Proceso

[31] Principales sistemas son Gamo y GESTA (Guerra Electrónica Sistema Táctico), principalmente sensores de emisiones empleados en escucha electrónica y goniometría, ni perturbación ni emisión.

[32] Sistema Integrado de Monitorización, Búsqueda y Análisis de amenazas Ciber en redes propias.

de Planeamiento Táctico, así como una propuesta (a modo de ejemplo) de herramientas útiles de coordinación a emplear en los citados CGs. Se finaliza el escrito presentando una serie de unidades y capacidades propias del ET para la ejecución de INFOOPS.

De la evolución doctrinal se extrae la relevancia, para esta función, del orden en el desarrollo de la doctrina. Contar con un claro marco de STRATCOM e INFOOPS desde el Nivel Conjunto, como se tiene en OTAN, es fundamental para favorecer la definición de conceptos de AI e implementar INFOOPS en el Nivel Táctico. A ello se le suma la relevancia de la adecuada comprensión de lo que se entiende por Entorno y Ámbito específico para comprender cómo será la forma de actuación en éstos. Sin estas dos claves doctrinarias no se progresará de forma adecuada en la bajada hacia el Nivel Táctico de los conceptos relacionados con las AI e INFOOPS. Así mismo, resulta indispensable comprender la diferencia que, en el marco de la doctrina OTAN y española, existe entre INFOOPS, función de coordinación, y las AI (conjunto de actividades diseñadas para causar efectos en el EI y el AC).

No debe confundirse INFOOPS con las FC y FT, constructos teóricos que agrupan actividades y capacidades permitiendo al Comandante y su EM integrarlas, sincronizarlas y dirigirlas. En este sentido se destaca la reciente creación de la FT Información en el ET. Lo que se considera de gran utilidad para dar solidez doctrinal a este tipo de actividades. Incluir esta Función de Combate en la doctrina del Ejército de Chile, además del desarrollo de una Doctrina Conjunta adecuada, sería un avance importante para dar consistencia a las INFOOPS en el Nivel Táctico.

Una parte importante del capítulo se dedica a definir las estructuras relacionadas con INFOOPS de los CG de GU en el ET, ya que, según su definición, INFOOPS es una función de CG/EM. Es primordial contar con el adecuado personal (capacitado) y con procesos claros en estas células para que las INFOOPS funcionen de forma conveniente en el Nivel Táctico. Un proceso fundamental de estos CG, en el que se debe integrar la mirada desde la perspectiva de las AI, es el Planeamiento de las Operaciones, que deberá proveer a las unidades, desde el inicio de la ejecución, de las herramientas e instrucciones de coordinación necesarias para todas las AI (matrices, WG o reportes).

Finalmente, se presenta la forma en que el ET contempla la ejecución de las AI en el Nivel Táctico, coordinadas por INFOOPS. La Unidad de Operaciones de Información específica en el ET es el ROI 1, creada en 2019, con capacidades PSYOPS, CIMIC, enlace, análisis de redes y CAMTAC. Además, se potencia que las BRI cuenten con personal capacitado en el CG y algún Equipo Táctico con formación básica, recibida en ejercicios anuales organizados por el ROI.

Todo lo expuesto en el presente capítulo no limita la posibilidad de continuar ahondando en el tema, siendo posible profundizar, a partir de esta descripción, en conceptos tan relevantes como la capacitación del personal, integración de la capacidad en ejercicios, experiencia en despliegues o integración entre niveles de mando, en los que no se ha podido profundizar dada la limitación de extensión.

En conclusión, este artículo pretende, a través de la descripción del modelo español, ofrecer lineamientos que puedan ser empleados por el Ejército de Chile para el desarrollo doctrinal y orgánico asociado a INFOOPS en el Nivel Táctico.

Referencias Bibliográficas

Bolivar, J. P. (20 de mayo de 2024). Minerva Institute. Obtenido de Minerva Institute: https://www.minervainstitute.es/propaganda-decepcion-operaciones-psicologicas-conflictos-modernos/

Estado Mayor de la Defensa. (2018). *PDC-01: Dooctrina para el empleo de las FAS.* Ministerio de Defensa de España.

Estado Mayor de la Defensa . (2021). *PDC-10: Doctrina de Comunicación Estratégica.* Ministerio de Defensa de España.

Estado Mayor del Ejército de Tierra. (2023). *Concepto de Transformación Fuerza 35.* Ministerio de Defensa de España.

Estebaranz M. , L., & Muñoz-Manero F., A. (2007). Operaciones psicológicas: el mundo de las percepciones. *Revista Ejército*, 51 - 55.

Expósito, J. L. (2020). El arma de la Comunicación. *Revista Española de Defensa*, 36 - 39.

MADOC. (2005). *OR3-001 Orientaciones. Operaciones de Información* .

MADOC. (21 de julio de 2018). *Concepto Derivado 02/18: La Función de combate información.* Mando de Adiestramiento y Doctrina - MADOC.

MADOC. (2021). *PD1-001: Empleo de las Fuerzas Terrestres.*

MADOC. (2022). *PD4-026: Proceso de Planeamiento de las Operaciones. Nivel Táctico (2ª ed.).* Mando de Adiestramiento y Doctrina - MADOC.

MADOC. (2024). PD2-004 Las Funciones Táscticas.

NATO. (2023). *AJP-10 Allied Joint Doctrine for Stratcom.*

NATO. (2023). *AJP-10.1 Allied Joint Doctrine for Information Operations.*

Tomás, G. (2023). La Guerra Electrónica en el Ejército de Tierra. *Revista de Aeronáutica y Astronáutica*, 782 - 785.

Vazquez M., M. (1998). Las operaciones psicológicas y operaciones de información de campaña. *Boletín de información del Ministerio de Defensa de España*, 39 - 53.

CAPÍTULO 7

Contrarrestando las Operaciones de Información de la Amenaza

Teniente Coronel Nicolás Kaiser Onetto [1]

El arte de la guerra está basada en la decepción
Sun Tzu

Introducción

El engaño ha sido, a lo largo de la historia militar, un factor decisivo para asegurar la sorpresa táctica y el éxito en las operaciones. Ya en la antigüedad, en los siglos XI o XII a.C., los griegos lograron una victoria sobre Troya mediante el uso de la decepción.

En la época moderna, durante la Segunda Guerra Mundial, las medidas adoptadas por los Aliados para engañar a Alemania fueron claves para el éxito de la Operación *Overlord*. Medidas como la creación de unidades ficticias, maniobras de distracción y la difusión de información falsa mediante agentes dobles, lograron confundir al alto mando alemán, impidiendo que concentraran sus fuerzas en el punto de desembarco. Esto contribuyó al éxito de la operación.

[1] Oficial del Arma de Caballería Blindada. Posee la Especialidad Primaria de Estado Mayor y las especialidades secundarias de Inteligencia, Buzo Táctico Militar y Profesor Militar de Academia. Tiene el grado de Magister en Ciberseguridad de la Universidad Adolfo Ibáñez y de Planificación y Gestión Estratégica de la Academia de Guerra del Ejército de Chile.

Tras la Segunda Guerra Mundial, durante la Guerra Fría, los servicios de inteligencia utilizaron medidas activas[2] para influir en las decisiones o engañar sobre las capacidades reales de las principales potencias. Los servicios soviéticos, en particular, emplearon técnicas como la propaganda encubierta, falsificación de documentos, agentes encubiertos y operaciones militares para influir en sus adversarios.

A finales del siglo XX, tras la Guerra Fría la humanidad fue testigo de la Guerra del Golfo Pérsico en 1991, un conflicto que marcó un cambio en el carácter de la guerra. El Ejército de Iraq, considerado una potencia cuantitativa por las fuerzas de la coalición, fue superado cualitativamente por las tecnologías empleadas por el Ejército de EE.UU. y sus aliados, lo que resultó en una aplastante victoria.

La doctrina predominante en ese momento era la aeroterrestre, que contemplaba el uso combinado de medios para alcanzar un objetivo. Además, comenzaba a surgir la necesidad de contar con capacidades de mando y control para sincronizar, integrar y coordinar las múltiples capacidades disponibles. Este conflicto también representó un cambio en la manera en que la población se informaba. Los medios de comunicación transmitían prácticamente en directo el desarrollo de las operaciones, lo que impactó de manera global la percepción de la guerra.

Para contrarrestar las capacidades de mando y control del adversario

[2] Medidas Activas: describir una serie de técnicas abiertas y encubiertas para influir en los acontecimientos y el comportamiento en países extranjeros, así como en las acciones de éstos (Shultz & Godson, 1984).

y fortalecer las propias, se llevaron a cabo acciones en el ámbito de la "Guerra de Mando y Control", que incluyeron guerra electrónica, operaciones psicológicas, operaciones en redes y medidas de seguridad (OPSEC). El objetivo era neutralizar las capacidades del enemigo y proteger las propias. En conjunto, estas acciones formaron una estrategia integrada que debilitó la capacidad del enemigo para coordinar y ejecutar sus operaciones.

Con el tiempo, las tecnologías continuaron avanzando, transformando la forma en que nos comunicamos. Paralelamente, el uso de internet se masificó, junto con la aparición de las redes sociales. La irrupción de estas tecnologías creó condiciones para modificar la capa cognitiva del entorno informativo a través de diversos medios.

A pesar de los avances tecnológicos y su incorporación en las operaciones de información, la finalidad a lo largo de la historia ha sido siempre la misma: engañar e influir al adversario. Para ello, los ejércitos han desarrollado capacidades destinadas a proteger la información, ocultar sus intenciones y persuadir a una amenaza específica.

El presente trabajo tiene como objetivo describir cómo las capacidades relacionadas a las funciones operacionales contribuyen a contrarrestar los efectos de las Operaciones de Información (OI) de una amenaza. Para ello, se establecen tres premisas clave:

- ***Primera premisa***: la amenaza no solo intentará alterar el ciclo OODA de la fuerza propia, sino que también buscará influir en la población

para disminuir su apoyo o generar tensiones internas. Esto permitiría a la amenaza obtener una ventaja tanto sobre la fuerza propia como sobre la situación en general. Las acciones de la amenaza no se limitarán al teatro de operaciones, sino que abarcarán todo el teatro de guerra, incluyendo la Zona Interior.

- ***Segunda premisa***: la amenaza actuará en la denominada "Zona Gris", es decir, por debajo del umbral del conflicto, y empleará una amplia gama de capacidades, tanto estatales (tradicionales) como no estatales, pero patrocinadas por el Estado (no convencionales). De este modo, se intentará influir tanto las capacidades militares como a la población civil.

- ***Tercera premisa***: aunque podría pensarse que solo las funciones conjuntas de inteligencia y protección son relevantes para contrarrestar las OI de la amenaza, sin embargo, es fundamental una articulación integral de todas las funciones para asegurar una ventaja en el ambiente de la información.

Primera premisa: Operaciones de información, ambiente de información y configuración del campo de batalla

Las OI tienen como finalidad influir en el ambiente de la información (IE, por sus siglas en inglés), ya sea de fuerzas adversarias, propias o de la población en el contexto de una operación militar. Por lo tanto, es fundamental comprender el terreno sobre el cual se planifican y ejecutan las OI.

En tal sentido, la doctrina nacional conjunta, considera el IE como "el colectivo de individuos, organizaciones y sistemas que recopilan, procesan, difunden o se guían por la información. Este ambiente está compuesto por tres dimensiones (física, informativa y cognitiva) interrelacionadas, que continuamente interactúan en los individuos, organizaciones y sistemas" (Estado Mayor Conjunto, 2024, p. 73).

Por su parte, la doctrina de la OTAN lo define como "un entorno compuesto por la propia información, las personas, organizaciones y sistemas que reciben, procesan y transmiten la información, y el espacio cognitivo, virtual y físico en el que esto ocurre" (NATO, 2023, p. 155).

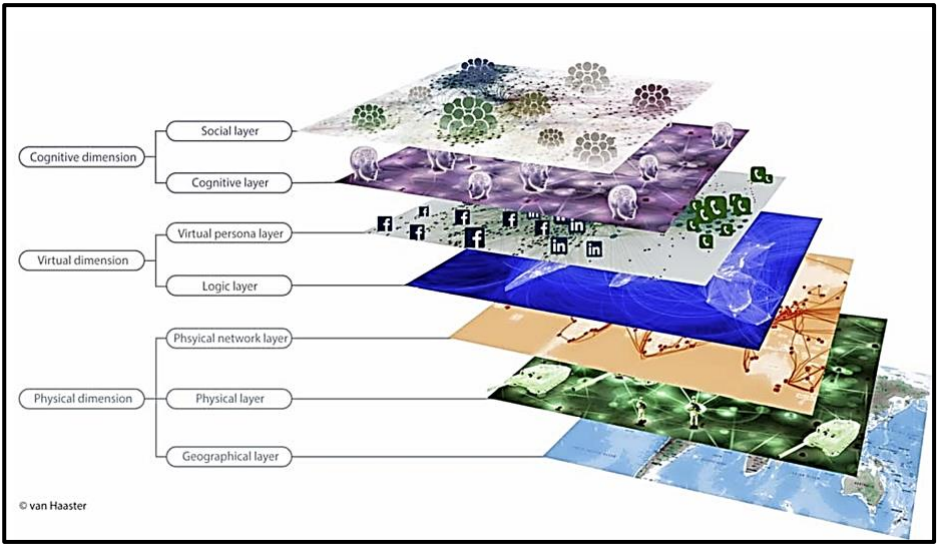
Adicionalmente, Ejército de EE.UU. ya no utiliza el término "Ambiente de Información" en su reglamentación, sino más bien incorpora el término *consideraciones informacionales*[3], definido como "aspectos de las dimensiones humana, física y de la información que afectan al modo en que las personas y los sistemas automatizados obtienen significado de la información, la utilizan, actúan en consecuencia y se ven afectados por ella" (Department of the Army, 2023, p. 128).

Pese a los matices entre las definiciones, se puede concluir que en el ambiente de información interactúan personas, organizaciones y/o sistemas con información en las capa o dimensión física, cognitiva

[3] Information Considerations.

(psicológica) e informativa (virtual)[4], las cuales están interrelacionadas entre sí.

Figura 1
Dimensiones del Ambiente de Información



Nota: Manoeuvring and Generating Effects in the Information Environment

Respecto a los dominios, Ducheine, Van Haaster, & Van Harskamp (2017), señalan que la dimensión física incluye los sistemas de mando y control (C2) y las infraestructuras de apoyo que generan efectos; la dimensión cognitiva (o psicológica) abarca las mentes de quienes reciben y actúan según la información; y la dimensión informativa (o virtual)

[4] La diferencia entre cognitiva o psicológica o informativa con virtual, depende del origen de la publicación.

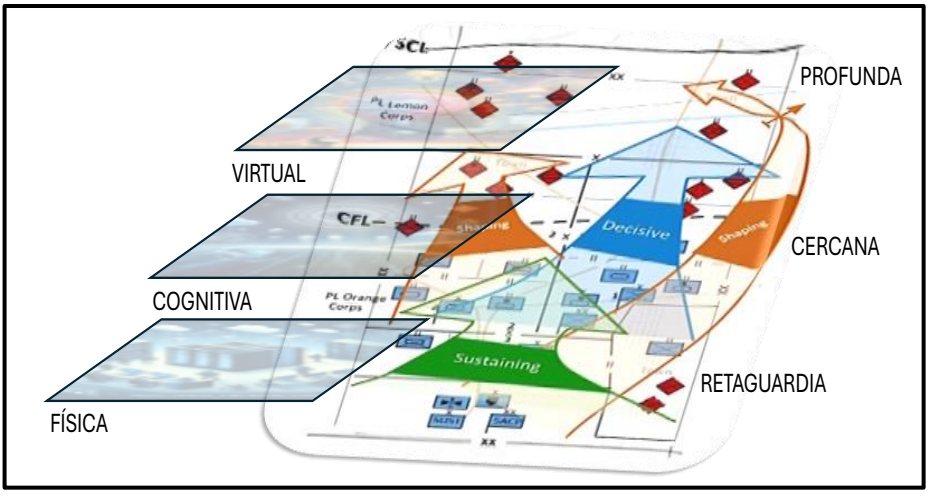
describe el proceso de recolección, almacenamiento, difusión y protección de la información. Esto demuestra que los efectos de las OI, independientemente de sus capacidades o dominios son transversales a todo el campo de batalla.

La doctrina institucional “Fuerza Terrestre” (Ejército de Chile, 2019. DD-10001: Fuerza Terrestre), clasifica la ejecución de las operaciones militares con el propósito de unificar los elementos en la organización del campo de batalla, logrando un enfoque común para todas las acciones. En este sentido, los comandantes organizan las fuerzas según el propósito, el estado final deseado y el área geográfica en la que se desplegarán.

Una forma de clasificar las operaciones es según la zona de empleo. En esta organización se consideran las operaciones en zonas profunda, cercana y en la retaguardia. Esta configuración requiere una sincronización continua y meticulosa para que la ejecución de una acción en profundidad esté conectada con la operación cercana que se esté realizando o que se llevará a cabo en el futuro próximo. Al mismo tiempo, se ejecutan operaciones en la retaguardia que buscan garantizar el éxito de las otras dos.

Figura 2

Relación entre Ambiente de Información y Zonas de Empleo



Nota: Elaboración propia

¿Por qué es importante esta descripción? Porque tanto las dimensiones (física, virtual o cognitiva) del ambiente de información como las zonas de empleo (cercana, profunda y retaguardia) son fundamentales para contrarrestar las OI de la amenaza. Las dimensiones son transversales a las zonas y, dependiendo de su ubicación en el campo de batalla, determinan cómo, cuándo y dónde se buscará afectar un objetivo (físico, virtual o cognitivo). Por lo tanto, es necesario desplegar las capacidades adecuadas para contrarrestar la acción de la amenaza.

El análisis de las OI desde la perspectiva de las fuerzas propias busca generar efectos que influyan en el proceso de toma de decisiones de la amenaza en función de la maniobra, ocultar las intenciones del

Comandante Operacional y mantener informados a los distintos grupos objetivo de la población local. Por otro lado, la amenaza intentará obtener una posición ventajosa y afectar nuestro proceso de toma de decisiones, utilizando diversas tácticas y procedimientos, y, como se mencionó en la introducción, operando en la *Zona Gris* mediante el empleo de diferentes capacidades.

Segunda premisa: Amenazas en el ambiente de información

Para comprender cómo actúa la amenaza, es fundamental entender cómo dos actores internacionales abordan las operaciones de influencia y cómo estas se despliegan desde el nivel político hasta el nivel táctico, trascendiendo el campo militar.

El primer modelo se asocia con la Federación Rusa y es conocido como Control Reflexivo. Este concepto unificador integra la guerra psicológica, la guerra de información y las operaciones de información (Bagge, 2019, p. 33). El modelo se basa en modelar los sistemas de toma de decisiones del adversario, entenderlos y eventualmente perturbarlos, con el objetivo principal de influir en el adversario para que tome decisiones favorables al engañador (Bagge, 2019, p. 35).

El segundo modelo es el desarrollado por la República Popular China, otro actor relevante en el contexto internacional. Según Livermore (2018), la teoría militar china ha valorado históricamente las estratagemas para socavar la moral del adversario, como lo señala Sun Tzu en "El arte de la guerra". En 2003, la Comisión Militar Central de la República Popular China introdujo el concepto de “Tres Guerras” (*san*

zhong zhanfa) en las directrices del Ejército Popular de Liberación, incorporando operaciones psicológicas estratégicas, manipulación abierta y encubierta de medios, y explotación de sistemas legales nacionales e internacionales para influir en el comportamiento del adversario y maximizar las ventajas de la RPC. Esta estrategia se centra en la dominación informativa para asegurar el control del Partido Comunista Chino (PCC) y minimizar la interferencia externa.

Es importante destacar que el Ejército de EE.UU. ha incorporado ambos conceptos en su nueva publicación sobre operaciones de información, el ADP 3-13 "*Information*" (2023). En esta publicación se subraya la importancia de identificar y clasificar la amenaza en el contexto de la guerra de información, definiéndola como "el uso orquestado de actividades de información (como operaciones en el ciberespacio, guerra electromagnética, guerra psicológica y operaciones de influencia) para lograr objetivos desde el nivel estratégico hasta el táctico.

A continuación, se describen los medios a través de los cuales se puede maniobrar en el ambiente de la información y los objetivos que se persiguen:

Tabla 1

Acciones, objetivos y efectos en el ambiente de la información

Acciones Ejecutadas	Objetivos	Efectos
- Operaciones en el ciberespacio. - Guerra psicológica. - Operaciones de influencia. - Movimiento y posicionamiento de fuerzas. - Decepción. - Guerra electrónica. - Destrucción física. - Guerra política y jurídica. - Medidas activas (espionaje, sabotaje y asesinatos). - El uso de representantes y agentes no estatales.	- Sensores de vigilancia y adquisición de objetivos - Centros y nodos C2. - Responsables de la toma de decisiones. - Datos e información. - Sistemas e infraestructuras de telecomunicaciones - Grupos de población y actores relevantes. - Enlaces de información, como receptores de radiofrecuencia, dispositivos de comunicación y protocolos de información.	- Destruir o perturbar el C2 amigo. - Destruir o engañar el reconocimiento, vigilancia y adquisición de objetivos amigos. - Negar la comprensión situacional amiga. - Aislar elementos clave de una fuerza amiga, particularmente aliados y socios. - Distorsionar o negar información a actores y audiencias relevantes.

Nota: ADP 3-13 "*Information*" (2023)

En resumen, el análisis de las operaciones de influencia de dos actores internacionales revela sus enfoques estratégicos distintivos. Tanto el modelo de "Control Reflexivo" de Rusia como la estrategia de las "Tres Guerras" de China buscan manipular al adversario y maximizar sus propias ventajas mediante el uso de diversas capacidades. La relevancia estratégica de estas acciones en el ambiente de la información se refleja en la reciente publicación del Ejército de los Estados Unidos, que subraya la necesidad de identificar y clasificar las amenazas en el contexto de la guerra de información. Queda claro que estas acciones tienen un impacto directo en el nivel táctico, lo que resalta la importancia

de comprender y abordar eficazmente este aspecto en el ámbito internacional contemporáneo.

Tercera Premisa: Funciones de conjuntas y sus efectos

La doctrina matriz "Fuerza Terrestre" del Ejército organiza el campo de batalla como un sistema donde interactúan personas, equipos, doctrina y procedimientos para asegurar el éxito de las operaciones. La agrupación de tareas, personas, organizaciones, información y procesos es denominada "Función de Combate" (FC) (Ejército de Chile, 2019. DD-10001: Fuerza Terrestre, p. 97). Estas funciones están presentes en los niveles estratégico, operacional y táctico.

En el nivel operacional, la Doctrina Operacional DNC 5-0: "Doctrina para la Planificación Conjunta" (2023), considera las "Funciones Conjuntas", como capacidades y actividades relacionadas entre sí, las cuales son claves para integrar y sincronizar las actividades operacionales en el entorno militar, como la maniobra, inteligencia, protección, informaciones, y mando y control, entre otras. Estas funciones orientan la toma de decisiones y permiten al comandante estructurar el mando y control para maximizar la efectividad operacional, detallando cómo se ejecutan las operaciones. La planificación funcional asegura que estas funciones apoyen de manera efectiva el proceso planificación operacional y contribuyan al éxito de la misión. Dado que las OI se articulan a nivel TO, para el presente trabajo se considerarán las funciones del Nivel Operacional, las cuales se detallan en tabla 2.

Tabla 2

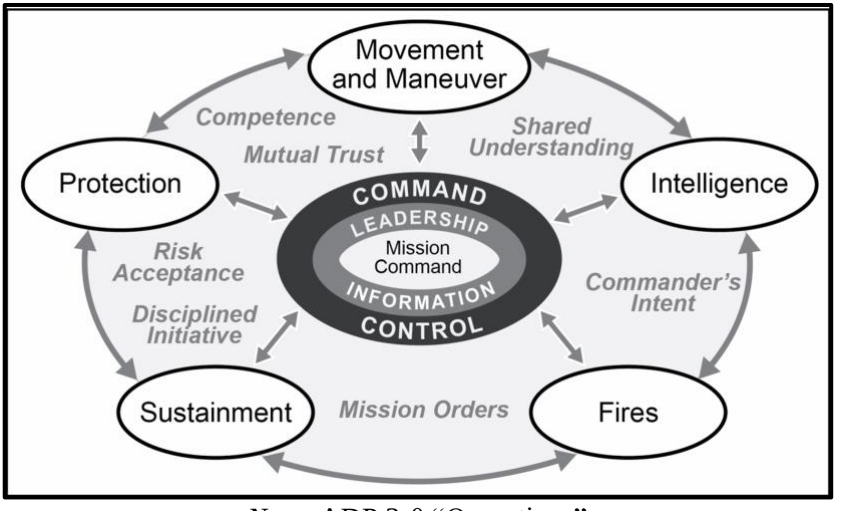
Funciones Conjuntas

Función	***Definición***
Maniobra	Conjunto de movimientos y acciones coordinadas en tiempo y espacio para crear situaciones favorables que permitan concentrar y emplear fuerzas propias en momentos clave, con el objetivo de quebrantar la voluntad del adversario mediante su dislocación y destrucción, preferiblemente de manera sorpresiva.
Fuegos	Buscan destruir o neutralizar las capacidades clave del adversario para debilitar su centro de gravedad y alcanzar los objetivos. Esto implica el uso coordinado de inteligencia, armas de apoyo, aviones de combate, fuego naval y otros medios, integrados con la maniobra para reducir la capacidad de combate del enemigo.
Mando y Control	Ejercicio de la autoridad de un comandante sobre una organización militar para cumplir una misión, apoyado por sistemas de información, telecomunicaciones y procedimientos que facilitan la planificación, conducción y seguimiento de operaciones. En el nivel operacional, es una actividad conjunta que requiere coordinación con elementos no militares, y es crucial para la toma de decisiones en todos los niveles, especialmente en funciones de protección, maniobras y fuegos.
Inteligencia	Se enfoca en analizar y comprender los elementos vitales del adversario, como los centros de gravedad, cuya neutralización, daño o destrucción podría debilitar su voluntad de conflicto. También se ocupa de los objetivos operacionales, el potencial militar y otros aspectos relevantes del adversario, incluyendo factores políticos, económicos, sociales y técnicos que puedan influir en sus operaciones.
Protección	Abarca actividades para evitar sorpresas y reducir la eficacia de las acciones ofensivas del adversario en todas las dimensiones, preservando la libertad de acción del comandante y la operatividad de las fuerzas. Está estrechamente vinculada a la inteligencia y a la protección de la fuerza antes y durante la maniobra, incluyendo la protección de objetivos estratégicos, bases, apoyo logístico, infraestructura crítica e información.
Sostenimiento	Asegura que una fuerza militar mantenga sus capacidades para alcanzar los objetivos operacionales a lo largo del tiempo necesario. Abarca tanto el apoyo de las Bases Generales como las coordinaciones estratégicas, y cubre todas las fases de la operación, incluyendo acciones previas y posteriores. Su alcance incluye logística, personal, técnica, finanzas, infraestructura, ingeniería, investigación y otros campos relacionados.
Informaciones	Implica el uso estratégico de la información para confundir al adversario y proteger las propias actividades, gestionando y aplicando la información para influir en percepciones y actitudes, así como para apoyar la toma de decisiones.
Administración Civil y Territorial	Actividades tendientes a asegurar que las operaciones propias no afecten a la población civil, a la vez que las acciones de los civiles no afecten a las operaciones propias.

Nota: Estado Mayor Conjunto, 2023, DNC-5-0. pp. 79-81

Además, el Ejército de Estados Unidos considera las funciones de combate como parte del Poder de Combate[5], aplicado a través del liderazgo y la información (ver Figura 3). La información permite a los comandantes en todos los niveles tomar decisiones basadas en datos sobre el uso del poder de combate y obtener resultados concretos. La gestión de la información es clave para identificar lo relevante dentro vasto volumen de datos disponibles (Department of the Army, 2019, p. 5-1 -5-2).

Figura 3
Elementos del Poder de Combate



Nota: ADP 3-0 "Operations"

[5] El poder de combate es el conjunto de medios de capacidades destructivas, constructivas y de información que una unidad o formación militar puede aplicar en un momento dado. El poder de combate tiene ocho elementos: liderazgo, información, mando y control, movimiento y maniobra, inteligencia, fuegos, sostenimiento y protección. (Department of the Army, 2019, p. 5-1)

En ambas doctrinas, la información se considera como un elemento clave de las funciones. En la primera, es un componente que, junto con otros elementos (tareas, procesos, etc) contribuye al éxito de una operación; en la segunda, es un facilitador que permite tomar decisiones para aplicar el poder de combate. Es esencial alcanzar una ventaja en el ambiente de información, ya sea afectando al adversario o protegiendo a la propia fuerza.

Para lograr una ventaja en el ambiente de información, una fuerza necesita capacidades que se traduzcan en actividades específicas. Para comprender mejor este concepto, es necesario establecer un marco sobre lo que es una capacidad. El Libro de la Defensa de Chile (2017) define capacidad como "la habilidad obtenida de la interdependencia y ponderación de factores de capacidad para cumplir las misiones asignadas a la Defensa Nacional" (Ministerio de Defensa, 2017, p. 113). Esta habilidad se logra mediante la articulación de los factores MERODISI (Material, Entrenamiento, Recursos Humanos, Organización, Doctrina, Infraestructura, Sostenibilidad e Información) (Ministerio de Defensa, 2017, p. 113).

En el contexto de las OI, esta habilidad sería la capaz de realizar acciones que modifiquen el ambiente de la información en beneficio de la operación En este sentido, la doctrina norteamericana desarrolla el concepto de Capacidades Relacionadas con Información (IRC por su sigla en inglés), que son herramientas, técnicas o actividades empleadas en el ambiente de la información y que son utilizadas para crear efectos y condiciones operacionales deseables (Department of Defense, 2016).

Para comprender cómo se logran estos efectos, es importante identificar qué actividades, capacidades y/o acciones se consideran en el ámbito de las OI.

Tabla 4

Comparación de ICR señaladas en distintas doctrinas

IRC	Chile	EEUU	OTAN (RU)[6]
Ciberoperaciones	X	X	X
Guerra Electrónica	X	X	X
Cooperación cívico – militar (CIMIC/CMO)	X	X	X
Destrucción física	X		X
Seguridad de las Operaciones (OPSEC)	X	X	X
Decepción	X	X	X
Key Leader Engagement (KLE)	X	X	X
Asuntos Públicos (PA)	X	X	
MISO (Military Information Support Operationss)	X	X	X

Nota: Elaboración propia a partir de la bibliografía empleada

La tabla precedente muestra que, aunque las acciones y actividades asociadas a las OI son conceptualmente similares, las capacidades varían según el país. Cabe destacar que, entre las doctrinas analizadas, la de EE.UU. es la más actualizada y desarrollada, por lo que en este artículo se considerarán las actividades incluidas en el ADP 3-13 “Information” para contrarrestar las OI de una amenaza.

En este sentido, la doctrina considera actividades de información que permiten obtener una ventaja informacional sobre una amenaza.

[6] Información extraída de la reglamentación de Reino Unido.

Estas actividades incluyen: habilitar, proteger, informar, influenciar y atacar, y en conjunto con las funciones conjuntas, buscan incrementar la efectividad del ciclo de decisiones propio y afectar el del adversario. A continuación, se describe cada actividad y las tareas que se ejecutan:

Tabla 5

Actividades de Información

Actividad	Descripción	Tareas
Habilitar	Esta actividad incluye tareas que mejoran el C2 propio. El objetivo de esta actividad es mejorar la comprensión de la situación, la toma de decisiones y las comunicaciones.	• Establecer, operar y mantener sistemas C2. • Ejecutar el proceso de operaciones y coordinar los distintos niveles. • Ejecutar los procesos de integración (preparación de inteligencia del ambiente operacional [IPOE], obtención de información, selección de objetivos, gestión de riesgos y gestión de conocimientos). • Mejorar la comprensión del ambiente operacional.
Proteger	Esta actividad incluye tareas que aseguran los datos, la información y las redes amigas. Esta actividad se centra en denegar el acceso de las amenazas a los datos y la información amigos, preservando al mismo tiempo las capacidades de comunicación amigas.	• Asegurar y ocultar información. • Realizar actividades de seguridad. • Defender la red, los datos y los sistemas.
Informar	La actividad incluye tareas que fomentan percepciones informadas de las operaciones y actividades militares entre diversos públicos. El objetivo de esta actividad es mantener la confianza de los públicos internos (miembros del Ejército, civiles y sus familiares) y externos (públicos nacionales e internacionales).	• Informar y educar a las audiencias del Ejército. • Informar al público nacional • Informar al público internacional.

Influenciar	Incluye tareas que afectan el pensamiento y, en última instancia, el comportamiento de las amenazas y otros públicos extranjeros. Esta actividad se centra en reforzar o cambiar la forma de pensar, sentir y actuar de individuos y grupos en apoyo de los objetivos.	• Influir en la percepción de las amenazas y en los comportamientos. • Influir en otros públicos extranjeros.
Atacar	Incluye tareas que afectan a la capacidad de la amenaza para ejercer el C2. El objetivo de esta actividad es afectar a los datos de la amenaza y a sus capacidades físicas para comunicarse y llevar a cabo una guerra de información.	• Degradar el C2 de la amenaza. • Afectar a las capacidades de guerra de información de la amenaza.

Nota: ADP 3-13 "Information" (2023)

De las actividades descritas en la tabla 5, habilitar, proteger e informar se consideran acciones defensivas, orientadas a potenciar la propia fuerza. Por otro lado, las acciones de informar, influenciar y atacar se emplean para degradar al adversario. Independientemente de si las actividades son defensivas u ofensivas, deben estar sincronizadas, integradas y coordinadas, ya que la amenaza utilizará todas sus capacidades para afectar a las fuerzas propias.

Contrarrestando las OI de la Amenaza

Después de describir las capacidades y actividades de información, así como sus efectos, es necesario analizar la relación que tienen con las funciones conjuntas para determinar cómo contribuyen a contrarrestar la amenaza.

Dado el propósito de la función de protección, podría considerarse inicialmente que las actividades asociadas a ella son las más relevantes

para contrarrestar la amenaza. Sin embargo, como se mencionó al inicio, el ambiente de información es transversal a todo el campo de batalla, lo que significa que se pueden ejecutar acciones en la zona profunda, cercana o en la retaguardia. Dado que la protección se centra en la retaguardia, sería un error enfocarse únicamente en esta función.

Asimismo, podría asumirse que las actividades de información que contribuyen a contrarrestar las OI de la amenaza son las que tienen un enfoque defensivo (habilitar, proteger e informar). Sin embargo, al igual que ocurre con la función de protección, sería engañoso considerar solo estas actividades.

Dado que el desarrollo de operaciones militares incluye tanto acciones ofensivas como defensivas en las diferentes áreas del campo de batalla, en el ámbito de las OI también es necesario considerar actividades de información que contrarresten las acciones del adversario, ya sea protegiendo las capacidades propias o actuando sobre las de la amenaza

A continuación, se presentan las relaciones entre las capacidades y actividades de información respecto de las funciones conjuntas (tabla 6). Estas funciones se priorizan según su incidencia en la protección de la fuerza frente a las OI de la amenaza[7].

[7] Para realizar la priorización de las funciones conjuntas y su relación con las capacidades y actividades de información, se realizó una encuesta a los alumnos del II y III Curso Regular de Estado Mayor, quienes durante los años 2023 y 2024 han venido estudiando las Operaciones de Información y ejercitándolas en distintos Juegos de Guerra.

La función de inteligencia exige el empleo de múltiples capacidades para analizar y comprender elementos cruciales de la amenaza. Entre las actividades de información, "habilitar" es fundamental, ya que permite obtener información de alta calidad, lo que facilita una comprensión holística del ambiente de batalla. Esta comprensión es esencial para que una fuerza pueda contrarrestar preventivamente las Operaciones de Información (OI) de la amenaza. Dado que se requiere información transversal de todo el teatro de operaciones, estas capacidades se emplean en todo el teatro de guerra, impactando de manera transversal en todas las capas del ambiente de información.

En la función de informaciones, las ciberoperaciones se consideran la capacidad principal. A través de ellas, es posible utilizar la información para confundir al adversario y proteger las propias actividades. Debido a que el ciberespacio, al igual que el ambiente de la información, está compuesto por diversas capas que permiten una transversalidad en el TO, impactando principalmente las capas cognitiva y virtual.

En lo que respecta a la función de protección, su esencia radica en evitar la sorpresa. Su esfuerzo se enfoca principalmente en las acciones de engaño a través de OPSEC y decepción, con el objetivo de reducir la eficacia de las acciones ofensivas del adversario en todas las dimensiones, preservando así la libertad de acción del comandante y la operacionalidad de la fuerza. Estas acciones se ejecutan en la capa física, mediante operaciones de engaño y OPSEC como parte de la maniobra operacional y en la capa cognitiva, a través de KLE y MISO,

especialmente en las zonas donde se llevan a cabo las acciones principales y de apoyo.

La función de Mando y Control se enfoca principalmente en actividades de información de carácter defensivo, facilitando así el desarrollo de las operaciones y el mantenimiento de los sistemas de mando y control. La capacidad clave para contrarrestar la amenaza en este ámbito es la Guerra Electrónica. Aunque su enfoque es predominantemente defensivo, no se deben ignorar los efectos ofensivos de la EW, especialmente dentro de la función de fuegos. Dado que esta es transversal a todos los niveles, se estima que está presente en todo el campo de batalla, impactando en las tres capas del ambiente de información.

La función Maniobra es, en esencia, ofensiva. Sin embargo, sus capacidades complementan las acciones de la función de protección al coordinar los movimientos y acciones de la fuerza en tiempo y espacio, en función de los objetivos establecidos. Además, mediante la actividad de atacar, se busca afectar las capacidades de información del adversario. Debido a su naturaleza ofensiva, las acciones se concentran en las áreas donde se desarrollan las operaciones principales, y su impacto se manifiesta principalmente en las capas física y cognitiva.

A diferencia de la función maniobra, que busca contrarrestar las OI mediante el despliegue de medios, la función fuegos buscan efectos a través del empleo de capacidades cinéticas y no cinéticas. Dependiendo de la capacidad a emplear, podría generar efectos en la capa física

(destrucción de nodos, antenas, etc), virtual afectando redes y sistemas de información y la dimensión cognitiva, producto de los efectos de las acciones.

Por último, la función de Administración Civil y Territorial centra sus acciones en evitar que las operaciones militares perjudiquen a la población civil. En este contexto, la actividad de informar es fundamental para mantener a la población al tanto de las acciones que realiza la fuerza, y así prevenir o contrarrestar posibles intentos de desinformación.

Tabla 6

Relación de la Funciones Conjuntas respecto de las Capacidades y Actividades de Información

Función Conjunta	**Capacidades de Información**	**Actividades de Información**	**Zona de Empleo**	**Capa que Impacta**
Inteligencia	Ciberoperaciones Guerra Electrónica CIMIC OSPEC Decepción MISO KLE	Habilitar Informar Influenciar	Profunda Cercana Retaguardia	Física Cognitiva Informacional
Informaciones	Ciberoperaciones CIMIC Asuntos Públicos MISO	Proteger Informar Influenciar	Profunda Cercana Retaguardia	Cognitiva Virtual
Protección	KLE OPSEC Decepción MISO	Proteger Informar Influenciar	Cercana Retaguardia	Física Cognitiva
Manado y Control	Guerra Electrónica Asuntos Públicos KLE	Habilitar Proteger Informar	Profunda Cercana Retaguardia	Física Cognitiva Virtual
Maniobra	Destrucción Física OPSEC Decepción	Habilitar Proteger Atacar	Profunda Cercana	Física Cognitiva

Fuegos	Ciberoperaciones Guerra Electrónica Destrucción Física	Proteger Influenciar Atacar	Profunda Cercana	Física Cognitiva Virtual
Administración Civil y Territorial	CIMIC Asuntos Públicos KLE	Habilitar Informar Influenciar	Profunda Cercana Retaguardia	Cognitiva

Nota: Elaboración propia

Consideraciones finales

El presente trabajo, tuvo como finalidad determinar de qué forma se pueden ejecutar medidas para evidenciar la presencia de OI de la amenaza, y cómo las diferentes funciones de combate aportan para la protección. Para ello, en primera instancia se establecieron premisas que tienen relación con el alcance de las OI en el campo de batalla, de *Zona Gris* y que se requiere la integración de todas las capacidades para contrarrestar la amenaza.

Respecto de la primera premisa, las dimensiones del ambiente de información son transversales a todas las zonas de empleo (profunda, cercana y retaguardia). Las actividades para contrarrestar las OI de la amenaza deben estar sincronizadas, integradas y coordinadas en todas las zonas, utilizando una combinación de capacidades de información y funciones conjuntas. De esta forma, se asegura que los efectos deseados sean efectivos en todos los niveles, minimizando de esta forma la influencia adversaria y contribuyendo a la libertad de acción propia.

En cuanto a la segunda premisa, es relevante continuar evaluando la evolución de las tácticas, técnicas y procedimientos empleados por las grandes potencias. Los actuales conflictos, en donde es complejo separar

en el ambiente de la información los objetivos militares y civiles, dan cuenta de la complejidad de las tácticas de influencia y de la constante evolución de las OI por parte de la amenaza, por lo que se requiere que las fuerzas militares no solo entiendan las tácticas actuales, sino que también anticipen y preparen capacidades para contrarrestar futuras amenazas.

En relación con las funciones de combate, el rol de estas es fundamental para contrarrestar las OI, ya que permiten una integración eficaz de capacidades. Cada función conjunta, al ser coordinada adecuadamente, contribuye a minimizar los efectos de las acciones adversarias. La inteligencia proporciona la información necesaria para anticipar y mitigar amenazas, la protección asegura que las operaciones críticas no sean comprometidas, y las informaciones permiten gestionar la percepción tanto de la población como del enemigo. Esta sinergia entre las funciones conjuntas no solo protege a la fuerza propia, sino que también permite tomar la iniciativa en el ambiente de información y con ello consolidar una posición ventajosa.

Finalmente, tener en consideración que las operaciones de información han demostrado ser un componente crucial en la planificación y ejecución de operaciones militares. La evolución de las tecnologías y la creciente influencia de la información en la toma de decisiones subrayan la necesidad de integrar las OI en todos los niveles de operación, desde lo estratégico hasta lo táctico. Las capacidades relacionadas con la información permiten a las fuerzas militares no solo proteger sus propios sistemas y redes, sino también influir en la

percepción y el comportamiento del adversario y otros actores relevantes. Este enfoque integral es esencial para mantener la superioridad operativa en un entorno cada vez más complejo e interconectado.

Referencias Bibliográficas

Bagge, D. P. (2019). *Unmasking Maskirovka: Russia's Cyber Influence Operantios.* New York: Defense Press.

Clark, R. M., & Mitchell, W. L. (2019). *Deception: counterdeception and counterintelligence.* Washington DC, Estados Unidos: CQ Press.

Department of Defense. (2016). *Department of Defense Dictionary of Military and Associated Terms.* Retrieved Agosto 21, 2024, from https://irp.fas.org/doddir/dod/jp1_02.pdf

Department of the Army. (2019). *ADP 3-0 "Operations".* Washington DC: Departmet of the Army.

Department of the Army. (2023). *ADP 3-13 INFORMATION.* Washington DC: Department fo the Army.

Ducheine, P., Van Haaster, J., & Van Harskamp, R. (2017). Manoeuvring and Generating Effects in the Information Environment. En N. A. Studies, *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in* (p. 155-179). Amsterdam: Springer.

Ejército de Chile. (2017). D-10001 "El Ejército". Santiago, Chile: DIVDOC.

Ejército de Chile. (2019). DD-10001 "La Fuerza Terrestre". Santiago, Chile: DIVDOC.

Estado Mayor Conjunto. (2023). *DNC-5-0 "Doctrina para la Planficación Conjunta".* Santiago: Estado Mayor Conjunto.

Estado Mayor Conjunto. (2024). DNC 3-7 "Operaciones de Información" (2do Borrador). Santaigo, Chile: Estado Mayor Conjunto.

Friedman, B. (2017). *On Tactics.* Annapolis, MD, Estados Unidos: Naval Institute.

Heuer , R. J., & Pherson, R. H. (2015). *Técnicas Analíticas Estructuradas para el análisis de inteligencia.* (R. Ardanaz, C. Arribas, & R. Arcos, Trads.) Madrid, España: Plaza y Valdes.

Livermore, D. (2018, Marzo 25). *Georgetown Security Studies Review.* Retrieved Mayo 20, 2024, from China's "Three Warfares" In Theory and Practice in the South China Sea: https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/

Ministerio de Defensa. (2017). *Libro de la Defensa Nacional de Chile.* Santiago: MDN.

NATO. (2023). *Allied Joint Publication-10.1 Information Operations.* (P. e. autor, Trans.) NATO.

Shultz, R. H., & Godson, R. (1984). *Desinformatsia: Active Measures in Soviet Strategy.* New York, NY, Estados Unidos: Pergamon-Brassey's International Defense Publishers.

Stenson, R. (23, Noviembre 2023). *US Army.* Retrieved Mayo 5, 2024, from Army publishes first doctrinal manual dedicated to

information: https://www.army.mil/article/271932/army_publishes_first_doctrinal_manual_dedicated_to_information

Wade, N. M. (2021). INFO1 Smartbook. *Information Operations & Capabilities: Guide to Informations Operations & the IRC*. Lakland, Florida, Estados Unidos: The Lightning Press.

REFLEXIONES FINALES

Teniente Coronel Branko Versalovic Serrano
Jefe del Centro de Estudios Estratégicos (CEEAG)

Luego de haber abordado diferentes dimensiones de las operaciones de información (INFOOPS), a lo largo de este Tema Central de Investigación de la Academia de Guerra 2024, es factible de evidenciar los alcances que tienen este tipo de operaciones en beneficio de cualquier empresa bélica que sea emprendida.

Desde el análisis de dos casos de guerras ocurridas durante el siglo pasado, en el capítulo 1, se puede apreciar de qué forma la correcta aplicación y consideración de lo que hoy se conoce como capacidades relativas a la información (IRCs) en la planificación y conducción de operaciones militares, genera resultados que surgen de la alteración de la toma de decisiones del adversario. Al respecto, si bien se abordan sólo dos casos históricos, el empleo de las INFOOPS se encuentra reflejado a lo largo de toda la historia militar. Así, a partir de la afirmación de Sun Tzu de que "el arte de la guerra se basa en el engaño" se encuentran casos que lo confirman y que, por citar algunos, se hacen carne en el engaño causado por el caballo de Troya para sortear los muros de la ciudad, pasando a través del modo de empleo que visualizó Alejandro Magno en la batalla de Gaugamela para desconcertar a su enemigo, así como también en los episodios relatados para la II Guerra Mundial y el Yom Kipur dentro del mismo capítulo, pudiendo incluso llegar a casos

contemporáneos como el del empleo de ejercicios militares rusos en la frontera con Ucrania previo a la ofensiva de 2022.

Por otra parte, a partir de los capítulos 2 y 5, se puede evidenciar de qué forma se comporta el ambiente de la información y, paralelamente, la mente humana como un verdadero escenario dentro del cual se desarrollan las INFOOPS, logrando potenciar sus efectos a partir del conocimiento y uso de ambos elementos. En tal sentido, es clave que los planificadores consideren ambas variables al momento de planificar las operaciones de información, las cuales se deben concebir y coordinar desde los más altos niveles de la conducción militar, para ser ejecutadas en los niveles inferiores, sin restringir esto que todos los comandantes consideren sus propias opciones de engaño desde el nivel táctico.

En la actualidad, lo anterior cobra vida bajo una estructura doctrinaria y conceptual robusta, que se ha ido forjando en base a la experiencia de quienes han ido aplicando las INFOOPS durante las guerras que han enfrentado en el siglo pasado y el presente, como es el caso de los EE.UU. analizado en el capítulo 3, o la propia experiencia del Ejército de Tierra de España para el nivel táctico, abordado en el capítulo 6. Todo esto, se debe comprender en un contexto evolutivo de diversos aspectos que han modificado el carácter de la guerra y que se logra evidenciar en el análisis profundo desarrollado en el capítulo 4, donde se traslapan incluso las INFOOPS con el empleo del instrumento del poder nacional de la información. Por ende, la consideración del campo de batalla cognitivo se expande no tan solo a los tomadores de decisiones de una fuerza militar, sino que se expande hacia actores como

líderes políticos, organizaciones internacionales y la propia población que, como parte constitutiva de la trinidad de Clausewitz, tendrán una gran injerencia en los resultados de una guerra.

Es así que, luego de analizar a lo largo de esta investigación las diversas particularidades de las INFOOPS y sus gravitantes alcances, se quiso abordar en el capítulo 7 algunas consideraciones para intentar contrarrestar las que pueda plantear un posible adversario, toda vez que una toma de decisiones errónea durante un conflicto bélico puede llevar a resultados catastróficos. Siendo muy relevante este último punto, es necesario de mantener la conciencia de los diferentes comandantes y sus estados mayores por proteger, últimamente, a las fuerzas que se verán comprometidas en combate, siendo de importancia vital el mantener medios de obtención suficientes para monitorear el ambiente de la información, así como parámetros de evaluación adecuados, y una firme disciplina información de no tan solo los líderes militares, sino que también de las diversas tropas que se encuentren en el campo de batalla.

Últimamente y como corolario a esta apasionante investigación, es menester mencionar que, si bien, las INFOOPS corresponden a una temática que se arrastra de una prolongada data histórica, se debe mantener una conciencia permanente y adecuada preparación a nivel militar para poder aplicarlas en los diferentes niveles y aspectos de la guerra, situación que puede incluso revertir ámbitos físicos de la aplicación del poder de combate, como es una diferencia desfavorable de potenciales o una posición perjudicial de una fuerza en el terreno, por citar solo algunas.

Por tanto, se invita a nuestros lectores, siendo principalmente relevante para quienes efectúan sus estudios como alumnos de la Academia de Guerra, a mantener la constante investigación y actualización de un tema tan apasionante como el abordado en el presente texto, ya que como futuros comandantes serán capaces de incorporar a las INFOOPS en distintas opciones que se estructuren para solucionar un problema militar determinado.