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).

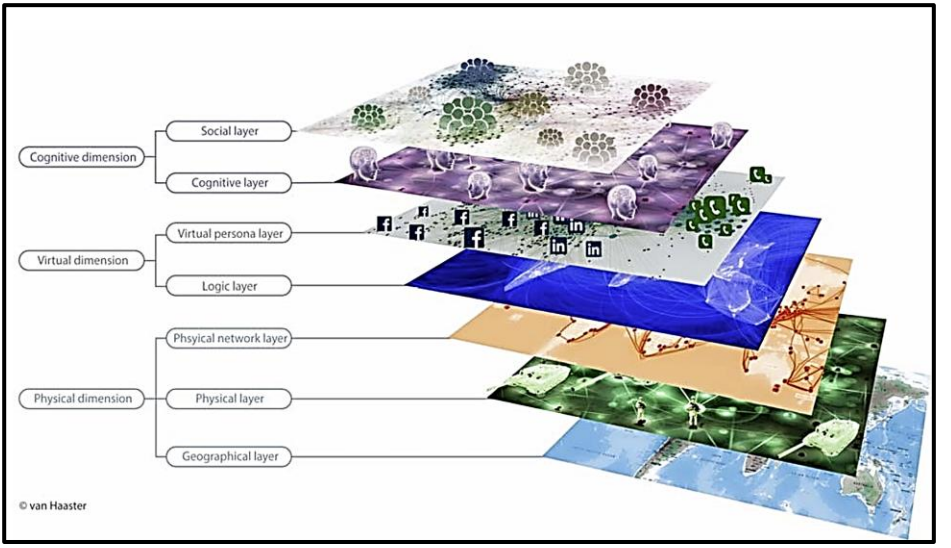
Adicionalmente, Ejército de EE.UU. ya no utiliza el término "Ambiente de Información" en su reglamentación, sino más bien incorpora el término *consideraciones informacionales*[3], definido como "aspectos de las dimensiones humana, física y de la información que afectan al modo en que las personas y 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)

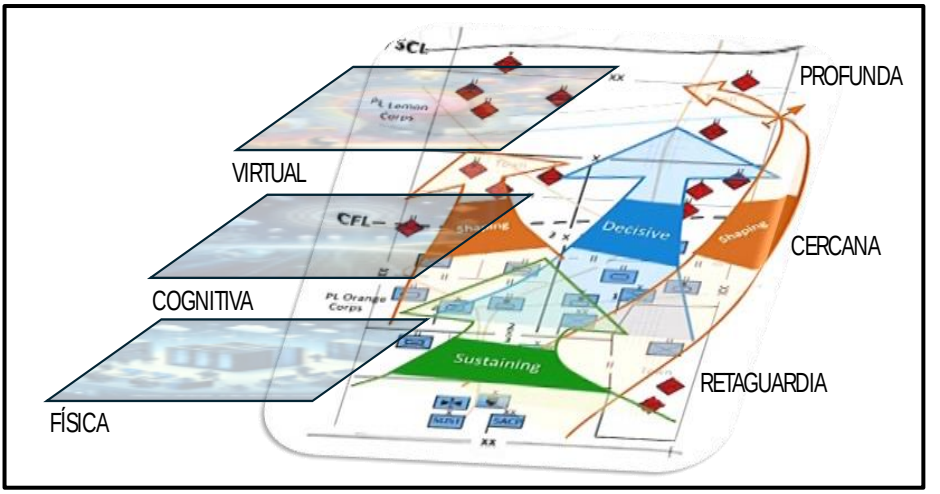
[4] La diferencia entre cognitiva o psicológica o informativa con virtual, depende del origen de la publicación.

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

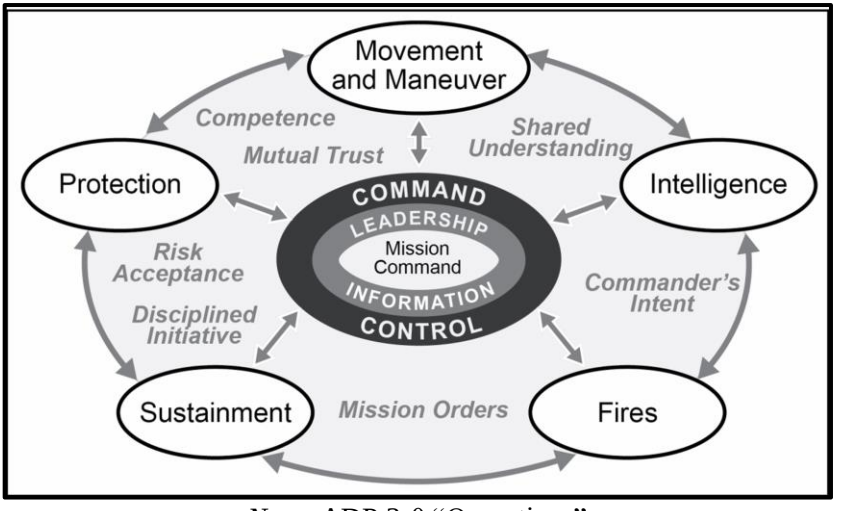
Funciones Conjuntas

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.