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:

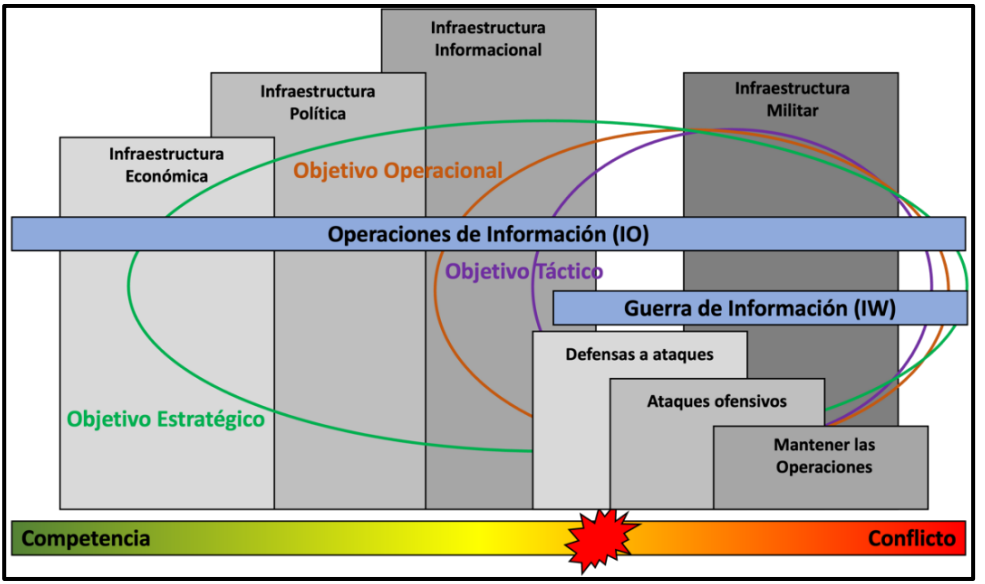
- Destrucción
- Decepción
- Operaciones psicológicas
- Seguridad de las operaciones
- Guerra electrónica

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?

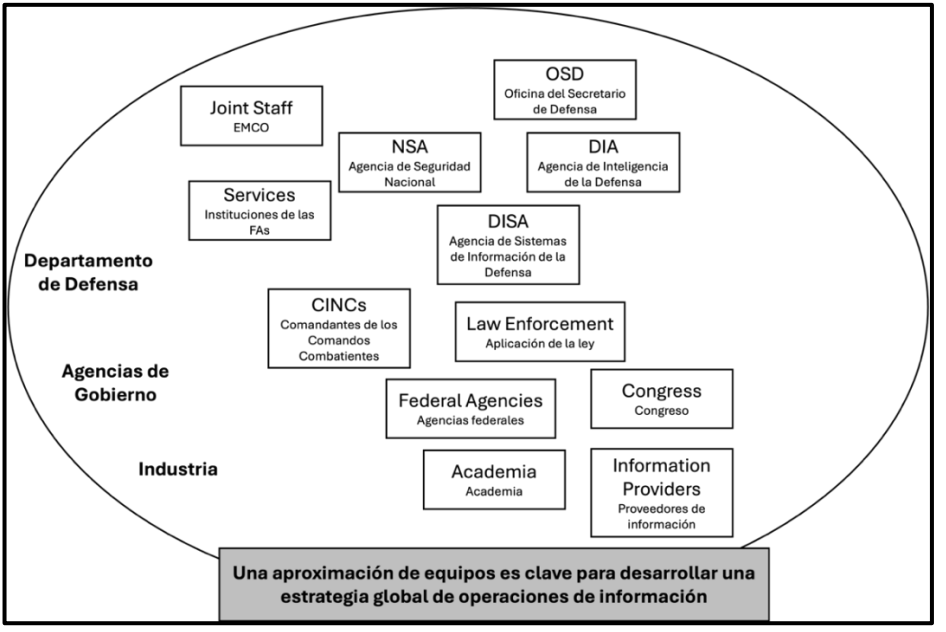
Países referentes de la OTAN y particularmente EE.UU. tienen una sólida experiencia al respecto. Por lo tanto, para dar respuesta a esta pregunta, nuevamente la doctrina norteamericana es pertinente de revisar, para luego reflexionar respecto algunos desafíos doctrinarios que tendría Chile, en términos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

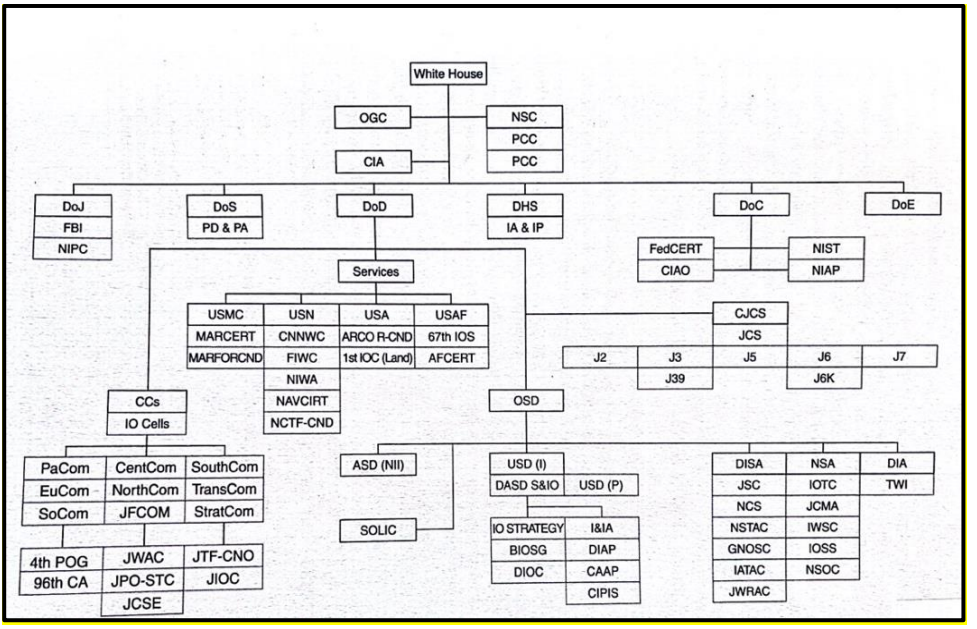
Un aspecto relevante por mencionar desde la perspectiva de los desafíos de integración es que, en el caso de EE.UU., las INFOOPS son lideradas por el poder político, siendo el presidente de los Estados Unidos quien aprueba la directiva de este tipo de operaciones, y junto al Secretario de Defensa conforman 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.