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

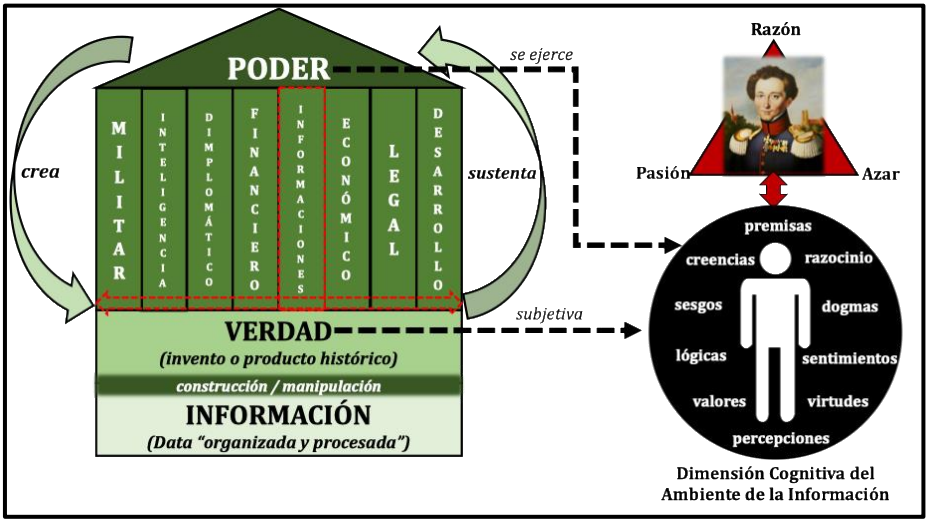
Basado en los postulados de Michel Foucault la información es la base fundamental para la construcción de la verdad, y sobre ésta, el ejercicio del verdadero poder. Según Vásquez (2011), Foucault define el poder como "la capacidad que tiene un determinado sujeto de imponer su verdad, como la verdad para 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



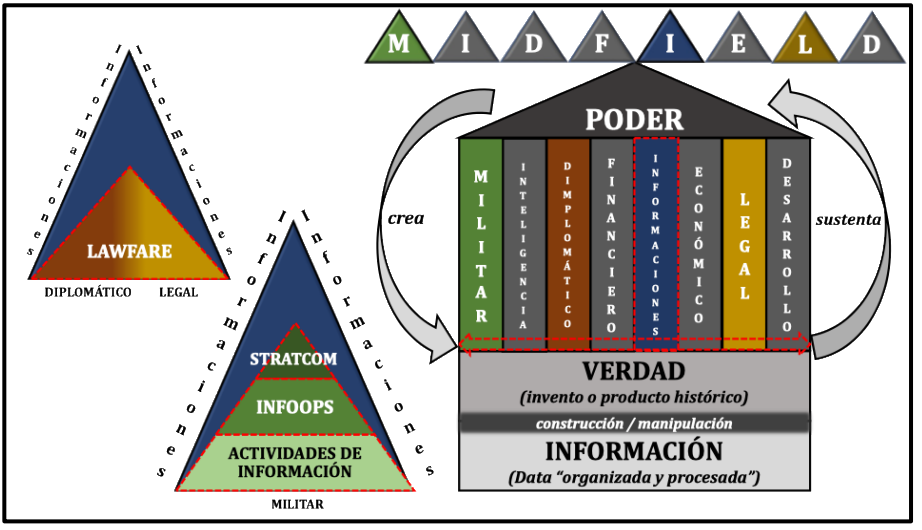
Nota: Elaboración propia

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.

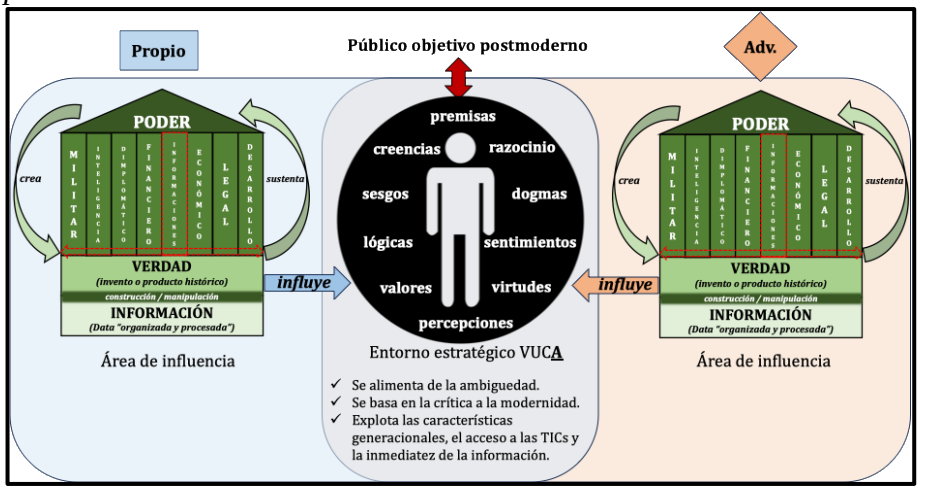
Algunas reflexiones que aporten para una posible solución

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.

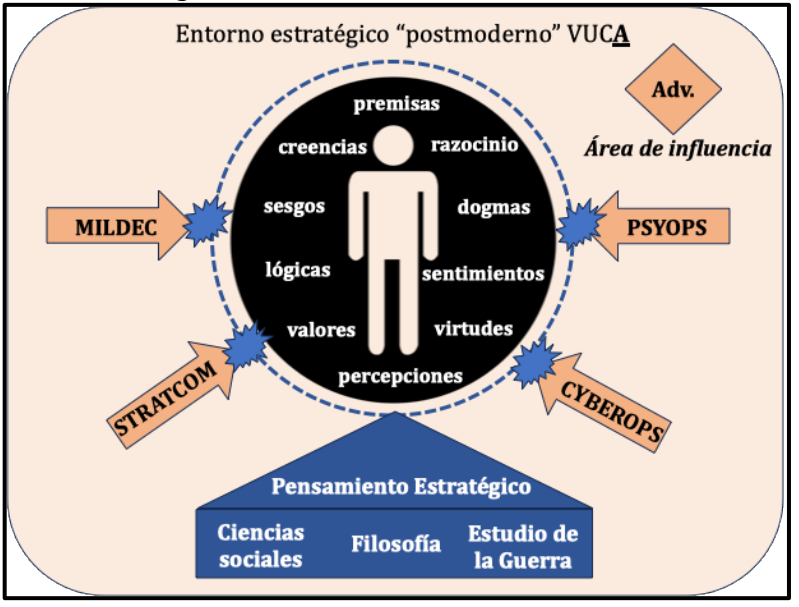
Una de las formas de poder asumir, conscientemente, las diversas verdades impuestas en esta lucha señalada por Foucault, es que el tomador de decisiones -ya sea político o militar en el contexto del conflicto- debe contar con una sólida formación en las ciencias sociales, particularmente, en filosofía. 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